Nasjonal kommunikasjons-myndighet

Internett i Norge – Årsrapport 2026

Juni 2026

Sammendrag

Utbredelsen av internettaksesstjenesten

Ved utgangen av 2025 hadde henholdsvis 99,3% og 96,3% av alle husstander tilbud om internettilgang med minst 100 Mbit/s og 1000 Mbit/s i nedlastingshastighet. På samme tidspunkt var basisdekningen for 4G og 5G beregnet til hhv. 100% og 99.8% av husstander i Norge[1].

Utbredelse av aksesser med IPv6 og trafikkandel IPv6

Det siste året har andelen av IPv6-trafikk i Norge – basert på ulike internasjonale målekilder - gått opp med 16 prosentpoeng, til 48% per mars 2026. Norge er med det på førsteplass blant de nordiske land når det gjelder bruk av IPv6. På europeisk nivå har Norge gått opp fra 15. til 7. plass.
Norske internettilbydere har det siste året fortsatt økt aktiveringen av IPv6 for sine abonnenter.
Fast trådløst bredbånd, som i år for første gang i år er tatt med i IPv6-statistikken for fast bredbånd, trekker imidlertid andelen av aksesser som er aktivert for IPv6 noe ned. Det er også betydelig variasjon i andelen IPv6-aktiverte aksesser mellom tilbyderne. Nkom følger utviklingen og vil igjen understreke viktigheten av at aktørene i det norske markedet legger til rette for bruk av IPv6 i størst mulig grad. Nkom anser likevel at det er tilstrekkelig med årlig rapportering framover.

Sikkerhet i internettilgangstjenester

Sikkerhet et av Nkoms mest sentrale ansvarsområder - også mht. internettilgangstjenester. Dette feltet er ikke hovedfokus i denne rapporten. I kapittel 2 beskrives likevel kort de viktigste områdene knyttet til arbeid med sikkerhet i internettilgangstjenester og Nkoms rolle i denne sammenheng.

Nettnøytralitet og åpent internett

Nkoms oppfølging av norske internettilbydere viser at norske internettbrukere nyter godt av åpen tilgang til internett via sine abonnement i fastnett og mobilnett. Internettilbydernes innrapportering indikerer at trafikkstyringen som benyttes er i tråd med nettnøytralitetsforordningen.
Nkoms gjennomgang av internettilbydernes nettsider viser at tilbyderne generelt opplyser tilfredsstillende om trafikkstyringstiltak. På enkelte nettsider kan det imidlertid være utfordrende å finne den relevante informasjonen, særlig når det gjelder ulike hastighetsparametere for fast internettilgang.

Kvalitet på internettilgangstjenesten

Resultater fra måletjenesten Nettfart viser at hastighet for fast internettilgang fortsetter den gode trenden fra forrige rapporteringsperiode. Gjennomsnittlig hastighet for nedlasting og opplasting for fast internettilgang i 2026 er henholdsvis 173 Mbit/s og 149 Mbit/s.
Med utgangspunkt i tall fra Nettfart observerer vi at gjennomsnittlig nedlastingshastighet, opplastingshastighet og forsinkelse for 5G-nettene i Norge i 2026 var henholdsvis 198 Mbit/s, 36 Mbit/s og 39 millisekunder (ms). Dette er forsiktig ned sammenlignet med 2025.

Digital Services Act (DSA)

Digital Services Act (DSA) regulerer formidlingstjenester og formålet er å skape et tryggere og mer ansvarlig digitalt rom i EU/EØS-området. Forordningen er foreløpig ikke inntatt i norsk rett. Regelverket skal blant annet redusere risiko for mindreårige, og beskytte brukere mot ulovlig innhold og manipulasjon, på digitale tjenester. De største nettbaserte plattformene pålegges ekstra strenge krav. Nkom er utpekt som koordinerende myndighet for regelverket i Norge, mens Medietilsynet, Forbrukertilsynet og Datatilsynet vil bli tildelt tilsynsansvar innenfor sine respektive ansvarsområder.

[1] Grunnet en metodeforbedring hos en av tilbyderne i 2025-rapporteringen, bør ikke tallene for mobilnettbasert dekning sammenliknes direkte med tallene rapportert tidligere år.

KI-forordningen

KI-forordningen, som foreløpig ikke er inntatt i norsk rett, etablerer et felles regelverk for utvikling og bruk av kunstig intelligens i EU/EØS med mål om å sikre trygg og ansvarlig KI. Regelverket bygger på en risikobasert tilnærming med strenge krav til KI-systemer med høy risiko, mens visse KI-praksiser er forbudt. Det innføres også egne regler for de kraftigste KI-modellene, som også kan gi plikter for norske virksomheter som tar dem i bruk. Nkom er koordinerende markedstilsynsmyndighet og felles kontaktpunkt for KI-forordningen i Norge.

Dataregulering

Dataforvaltningsforordningen (DGA) er foreslått innført i Norge som ny dataforvaltningslov. Lovproposisjon ble sendt til Stortinget våren 2026 og det er ikke besluttet hvem som får tilsynskompetanse etter den nye loven. Dataforordningen (Data Act/DA) er gjeldende i EU, og er nå til vurdering i EØS-EFTA-landene. DA er ment å bidra til datadeling mellom aktørene i det europeiske datamarkedet.
Digital Omnibus ble lagt frem av Europakommisjonen 19. november 2025. Formålet med Digital Omnibus er å forenkle og samordne eksisterende digitale regelverk.

Antisvindelarbeid på internettområdet

Omfanget av digital svindel og svindelforsøk på internett er betydelig. Dette utfordrer tilliten til internett som tjeneste og samfunnskritisk infrastruktur og kan påføre enkeltmennesker og bedrifter store økonomisk tap. Redusert tillit til internett kan bremse digitaliseringen og digital inkludering i samfunnet. Nkom bidrar til å møte disse utfordringene blant annet gjennom sitt antisvindelarbeid og gjennom tilsyn med domenenavnsforvaltningen for '.no'. Nasjonal ekspertgruppe mot digital svindel består av offentlig og private aktører og ledes av Nkom i partnerskap med Økokrim. Gruppen har hatt fokus på tale og SMS, men fikk i desember 2025 fornyet mandat til også å se på svindel over internettbaserte tjenester

Internasjonal internettforvaltning

Internasjonal internettforvaltning har ved overgangen fra 2025 til 2026 passert en viktig milepæl. Norge var arrangør for det 20. årlige internasjonale møtet innen internettforvaltning i juni 2025 (IGF 2025), og FN vedtok på generalforsamlingen i desember 2025 å videreføre det internasjonale samarbeidet innen internettforvaltning (WSIS+20).
I 2026 vil to parallelle prosesser innen internasjonal internettforvaltning bidra til videreutvikling av fagområdet. Ved utgangen av april åpnet en ny søkerunde for generiske toppdomener innen DNS, organisert av forvaltningsorganet ICANN. Og i oktober gjennomføres fullmaktskonferansen til FN-organisasjonen ITU med sentrale internettema på agendaen.

Innholdsfortegnelse

1 Status for internett i Norge 5

1.1 Innledning og bakgrunn 5
1.2 Utbredelse av internettilgangstjenesten 5
1.3 Volumutvikling for datatrafikk i mobilnett i Norge, gjesting i utlandet og for internett samtrafikk 6
1.4 Utbredelse av aksesser med IPv6 og trafikkandel IPv6 7

2 Sikkerhet i internettilgangstjenester 12

3 Status for nettnøytralitet i Norge 12

3.1 Innledning og bakgrunn 12
3.2 Tilgang til et åpent internett 12
3.3 Informasjon om internettilgangstjenesten 13
3.4 Kvalitet på internettilgangstjenesten 15

4 Digital Services Act (DSA) og Nkoms rolle som DSA-koordinator 22

4.1 Bakgrunn og formål - Nkoms nye temasider om DSA 22
4.2 Nkom som DSA-koordinator 23
4.3 Plattformenes plikter og brukernes rettigheter 23
4.4 Pliktsubjekter etter DSA 25
4.5 DSA og regjeringens forslag om aldersgrense på sosiale medier 26

5 KI-forordningen og Nkoms rolle som KI-myndighet 26

5.1 Bakgrunn og formål – Nkoms nye fagsider om KI-forordningen 26
5.2 Risikobasert tilnærming til regulering av KI 27
5.3 Egne regler for de kraftigste KI-modellene 28
5.4 Roller og aktører 29
5.5 Krav og forpliktelser for høyrisiko KI-systemer 29
5.6 Sanksjoner ved brudd på KI-forordningen 30
5.7 Samspillet med annet regelverk 30

6 Dataregulering 31

6.1 Bakgrunn: En europeisk strategi for data 31
6.2 Dataforvaltningsforordningen 31
6.3 Dataforordningen 32
6.4 Digital Omnibus 32

7 Antisvindelarbeid på internettområdet 33

7.1 Bakgrunn og omfang 33
7.2 Internasjonale aktører og EU har økt fokus på digital svindel 34
7.3 Den nasjonale innsatsen mot digital svindel på internett 35

8 Internasjonal internettforvaltning 37

8.1 Bakgrunn 37
8.2 IGF 2025 i Norge 38
8.3 WSIS – 20 års milepæl passert 39
8.4 ICANN starter søkerunde for nye toppdomener 40
8.5 ITU på vei mot Plenipot 26 41

1 Status for internett i Norge

1.1 Innledning og bakgrunn

Internett utgjør en grunnleggende infrastruktur i det norske samfunn som gir store muligheter for innovasjon og vekst på mange samfunnsområder. Internettilgang er gradvis blitt den mest brukte ekomtjenesten i Norge og er nå blitt tilnærmet uunnværlig: Internettilgang av høy kvalitet og sikkerhet og med effektivt regulatorisk rammeverk nasjonalt og internasjonalt er en helt nødvendig forutsetning for gjennomføring av den nye nasjonale digitaliseringsstrategien[2]. Vår visjon peker på Nkoms rolle i dette: «*Vi sikrer en trygg og tilgjengelig digital hverdag for alle*».

Kapittel 1 i denne rapporten beskriver status for internett i Norge, basert på oppdrag gitt av departementet til Nkom gjennom «*Stortingsmelding 28 (2020-2021) Vår felles digitale grunnmur – Mobil-, bredbånds- og internettjenester*».

Internett fungerer som en åpen plattform for kommunikasjon og innholdsdistribusjon. Både forbrukere, virksomhetskunder og innholdstilbydere kobler seg til plattformen via sine respektive internettilbydere, og basert på dette kan forbrukere og innholdstilbydere kommunisere fritt over internett. Dette bidrar til å opprettholde insentivene til innovasjon, som igjen bidrar til økt etterspørsel etter innhold.

Sikkerhet er ikke et hovedtema i denne rapporten. I kapittel 2 gis likevel en kort oversikt over Nkoms rolle ifm. sikkerhet og pålitelighet for internettilgangstjenester, datasentre og annen kritisk digital infrastruktur.

Kapittel 3 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[3].

I kapittel 4 beskrives status for Digital Services Act (DSA) og Nkoms rolle som DSA-koordinator. I kapittel 5 beskrives status for KI-forordningen og Nkoms rolle som KI-myndighet. Kapittel 6 omhandler dataregulering, mens kapittel 7 omhandler på internettområdet. Til slutt beskrives status for internasjonal internettforvaltning i kapittel 0.

1.2 Utbredelse av internettilgangstjenesten[4]

Ved utgangen av 2025 hadde henholdsvis 99,3 % og 96,3 % av alle husstander tilbud om fast internettilgang med minst 100 Mbit/s og 1000 Mbit/s i nedlastingshastighet. På samme tidspunkt var basisdekningen for 4G og 5G beregnet til hhv. 100% og 99,8 % av husstander i Norge[5].

Utbredelse av internettilgangstjenesten samsvarer i stor grad med utbredelsen av bredbånd. Nkoms dekningsundersøkelse for 2025 viser at 99,3 % og 96,3 % av alle husstander hadde tilbud om fast bredbånd med henholdsvis minst 100 Mbit/s og minst 1000 Mbit/s i nedlastingshastighet[6]. Dette er i

[2] "Fremtidens digitale Norge", DFD, sept 2024

[3] EU-forordning 2015/2120: https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02015R2120-20181220

[4] Den siste publiseringen er å betrakte som midlertidige tall, og tallene betraktes som midlertidige inntil året etter når ny undersøkelse publiseres, jf. kap. 5.8 i Metodedokumentet for ekomstatistikken.

[5] Grunnet en metodeforbedring hos en av tilbyderne i 2025-rapporteringen, bør ikke tallene for mobilnettbasert dekning sammenliknes direkte med tallene rapportert tidligere år.

[6] https://nkom.no/statistikk/nokkeltall-og-interaktive-dashbord/dekningsunders%C3%B8kelsen

hovedsak basert på fiber- eller hybrid fiber-koaksial-nett[7], men også fast trådløst bredbånd bidrar til dekningstallene.

I Norge har 98 % av husstandene tilbud om alternative tilknytninger, og alternativene inkluderer fast trådløst bredbånd i tillegg til fiber og HFC. Det er geografiske ulikheter, men sett under ett har de fleste norske husstander gode muligheter for å koble seg til internett.

Utbygging av 5G-nettet startet i 2020. Nkoms dekningsundersøkelse ved utgangen av 2025 viser at basisdekningen for 5G (husstandsdekning) samlet for alle mobiloperatørene er beregnet til 99,8 %. Ved samme tidspunkt året før ble beregnet til om lag 99,7 %[8]. De fleste fylkene har en dekning på mer enn 95 %, og for de fleste fylkene er dekningen nærmere 100 %.[9]

Ekomstatistikken for 2025[10] viser at Telenor, Altibox[11], Telia, GlobalConnect og NextGenTel samlet hadde hånd om anslagsvis 86 % av markedet for fast internettilgangstjeneste basert på aksessvolum, når en slår sammen privat- og bedriftsmarkedet. I markedet for mobil internettilgang er konsentrasjonen enda høyere. Samlet har Telenor, Telia og Ice om lag 90 % av mobilmarkedet målt i abonnement, marginalt ned fra 2024.

Mot slutten av 2022 ble internettilgang via lavbanesatellitter (LEO) fra Starlink tilgjengelig over hele Norge [12]. Eutelsat-Oneweb tilbyr en lignende tjeneste i et noe mer begrenset omfang. Det er også forventet at andre aktører vil tilby internettilgang via LEO-satellitt i de kommende årene til både private og profesjonelle brukere, f.eks. Amazon LEO. Det jobbes også med å gjøre slike konstellasjoner i stand til å kommunisere direkte mot ordinære mobiltelefoner for enkel tale/tekst/data i områder uten dekning fra bakkenett. Starlink, Amazon LEO og AST-space mobile er eksempler på aktører som jobber med disse løsningene for kommersiell lansering i Europa i fremtiden.

1.3 Volumutvikling for datatrafikk i mobilnett i Norge, gjesting i utlandet og for internett samtrafikk

I 2025 var summen av datatrafikk i norske mobilnett og trafikk fra norske kunders gjesting i utenlandske nett 1160 Petabytes (PB), en økning på 10 % fra 2024.

I januar 2026 var maksimalt nivå på innkommende internettsamtrafikk («peak throughput») til de største fastnettilbyderne og de største mobiloperatørene i travel time («peak hour») i området mellom 0,3 Tbit/s og 3 Tbit/s.

Fordelingen av internettrafikken mellom ulike applikasjoner er relativt lik i mobilnettene og fastnettene med unntak for strømmetjenester som er mye større i fastnett.

Datatrafikk i mobilnettene

Trafikkutviklingen påvirkes av den teknologiske utviklingen og medfølgende økning i nettverkskapasitet, samt vekst i antall kunder og økte datakvoter.

[7] Hybrid fiber, som også kalles HFC (Hybrid Fiber-Coaxial), refererer til måten fiber og koaksialkabler brukes i kombinasjon innen et kabelnettverk.

[8] Grunnet en metodeforbedring hos en av tilbyderne i 2025-rapporteringen, bør ikke tallene for mobilnettbasert dekning sammenliknes direkte med tallene rapportert tidligere år.

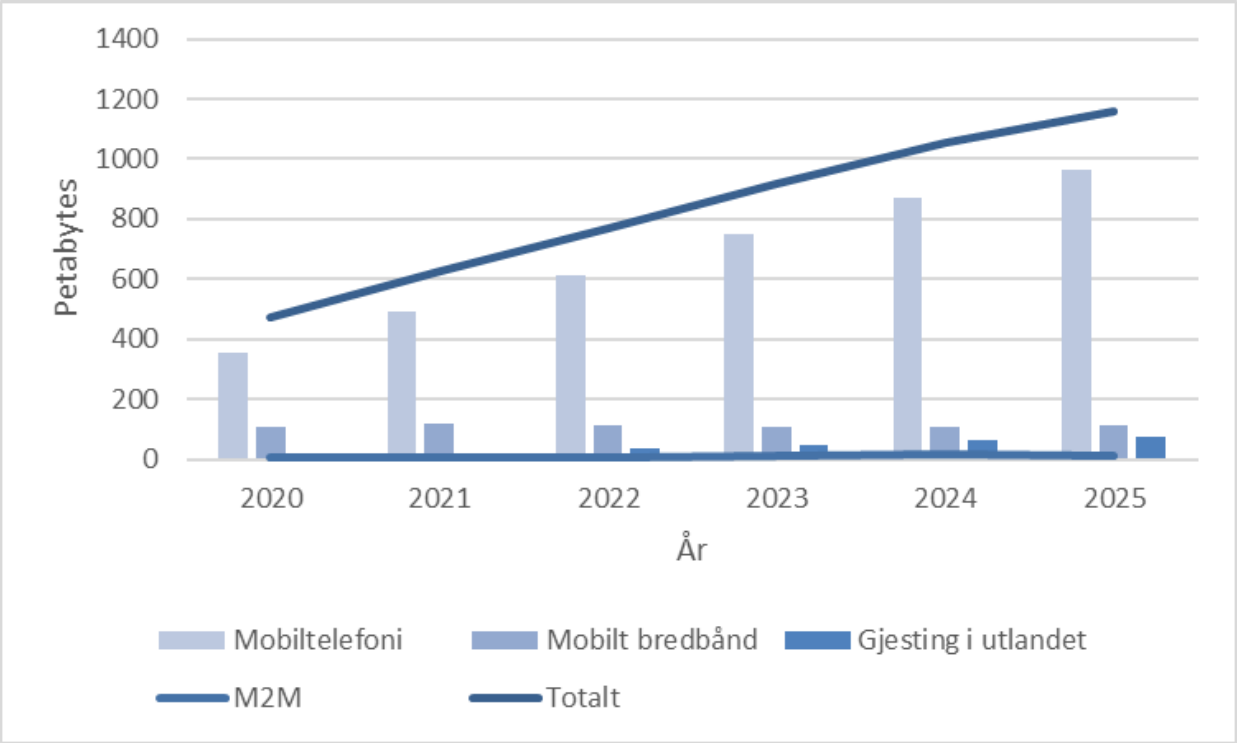
[9] https://nkom.no/statistikk/nokkeltall-og-interaktive-dashbord/dekningsunders%C3%B8kelsen

[10] Ekomstatistikken 2025

[11] Altibox refererer her til Altibox-partnerskapet som omfatter Lyse og et trettitalls andre regionale fibertilbydere.

[12] https://www.starlink.com/map

Figur 1 viser utviklingen i datatrafikk fordelt på vanlige mobilabonnement, dedikerte internettabonnement[13], gjesting i utlandet og M2M. Det er vanlige mobilabonnement som skaper mesteparten av datatrafikken i mobilnettene (over 80 %). I 2025 var datatrafikken i mobilnettene totalt 1160 Petabyte (PB)[14], en økning på 10 % fra 2024. Volumet av datatrafikk via mobilnettene i 2025 er nesten dobbelt så høyt som det var i 2021.



Figur 1 - Internettrafikk for ulike kategorier mobilabonnement (Kilde: Ekomstatistikken 2025)

Datatrafikken for gjesting i utlandet i 2025 var 72 Petabyte (PB), dette representerer en økning på 17 % sammenlignet med året før.

1.4 Utbredelse av aksesser med IPv6 og trafikkandel IPv6

Det siste året har andelen av IPv6-trafikk i Norge – basert på ulike internasjonale målekilder - gått opp med 16 prosentpoeng, til 48% per mars 2026. Norge er med det på førsteplass blant de nordiske land når det gjelder bruk av IPv6. På europeisk nivå har Norge gått opp fra 15. til 7. plass.

Norske internettilbydere har det siste året fortsatt økt aktiveringen av IPv6 for sine abonnenter.

Fast trådløst bredbånd, som i år for første gang i år er tatt med i IPv6-statistikken for fast bredbånd, trekker imidlertid andelen av aksesser som er aktivert for IPv6 noe ned. Det er også betydelig variasjon i andelen IPv6-aktiverte aksesser mellom tilbyderne. Nkom følger utviklingen og vil igjen understreke viktigheten av at aktørene i det norske markedet legger til rette for bruk av IPv6 i størst mulig grad. Nkom anser likevel at det er tilstrekkelig med årlig rapportering framover.

[13] Dedikerte internettabonnement omfatter 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.

[14] Petabyte (PB) er 1000 Terabyte eller 1000 000 Gigabyte.

1.4.1 Om overgangen fra IPv4 til IPv6

IP (Internet Protocol) er den grunnleggende protokollen som brukes for å overføre trafikk på internett. IP-protokollen finnes i to versjoner, IPv4 og IPv6. Offentlige IP-adresser er globalt unike identifikatorer for datamaskiner som kobles til internett.

Det er behov for å øke bruken av IPv6 på internett. Årsaken er mangel på ledige IPv4-adresser. Kompleksiteten til dagens internett medfører at overgangen fra IPv4 til IPv6 må gjøres gradvis, og starter med en periode av sameksistens med IPv4.

IPv6 bidrar til at det blir nok IP-adresser til et stort antall nye enheter som blant annet gir grunnlag for vekst og utvikling for IoT-løsninger. Dette bidrar igjen til et mer åpent og skalerbart internett og til grunnlag for innovasjon og vekst.

1.4.2 IPv6-utbredelsen i Norge og sammenliknet med andre land

Figurene nedenfor viser status for IPv6-utbredelsen i Norge sammenliknet med andre land. Datagrunnlaget er hentet fra de tre hovedkildene med offentlig tilgjengelig informasjon rundt IPv6-utbredelse (Google[15], Facebook[16] og Apnic[17]), og datainnsamlingen ble utført i mars 2026.

Både Google og Facebook gjør målinger basert på trafikkfordelingen mot egne tjenester fra ulike brukere, mens APNIC er basert på at brukere går inn på annonser som tilrettelegger for måling av IP-versjon. Disse forholdene kan gi en skjevhet. Det ble derfor i 2025 inntatt en ny statistikk-kilde, Cloudflare, som gjør målinger av trafikkfordelingen mellom IPv4 og IPv6 på sentrale målepunkter i IP-nett i de fleste land. Hovedbildet er at målingene fra Google, Facebook og APNIC synes å ha relativt små variasjoner innbyrdes, mens Cloudflare i de fleste land viser lavere IPv6-andel fra målepunktene sentralt i nettet. Nkom har valgt å videreføre de samme datakildene som i fjor for å få sammenliknbare tall over tid og mellom land.

I løpet av ett år har IPv6-utbredelsen i Norge gått opp med 15,9 prosentpoeng, til 47,8 % i mars 2026. Figur 2 nedenfor viser at Norge nå er på førsteplass blant de nordiske land når det gjelder bruk av IPv6. Av Figur 3 nedenfor framgår at Norge nå er på 7. plass på europeisk nivå, opp åtte plasser fra i fjor.

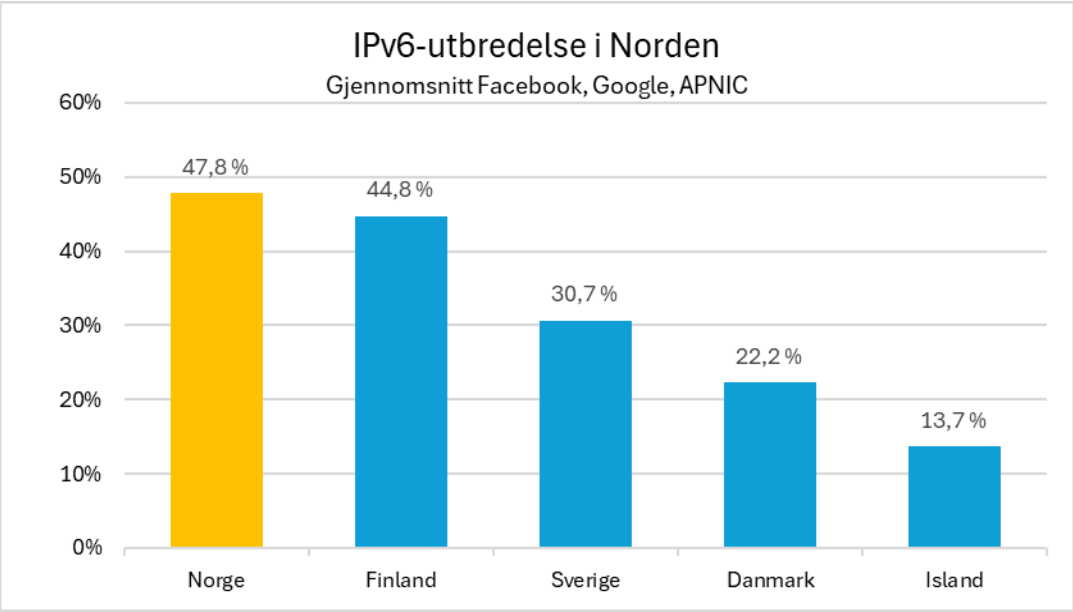
På listen over landene med høyest utbredelse av IPv6 på verdensbasis[18], beveget Norge seg vesentlig opp fra 44. plass til 21. plass.

[15] Andel av Google-brukere som aksesserer tjenestene over IPv6: Kartbasert presentasjon av data fra Google, samt tabelloppstilling av samme datagrunnlag

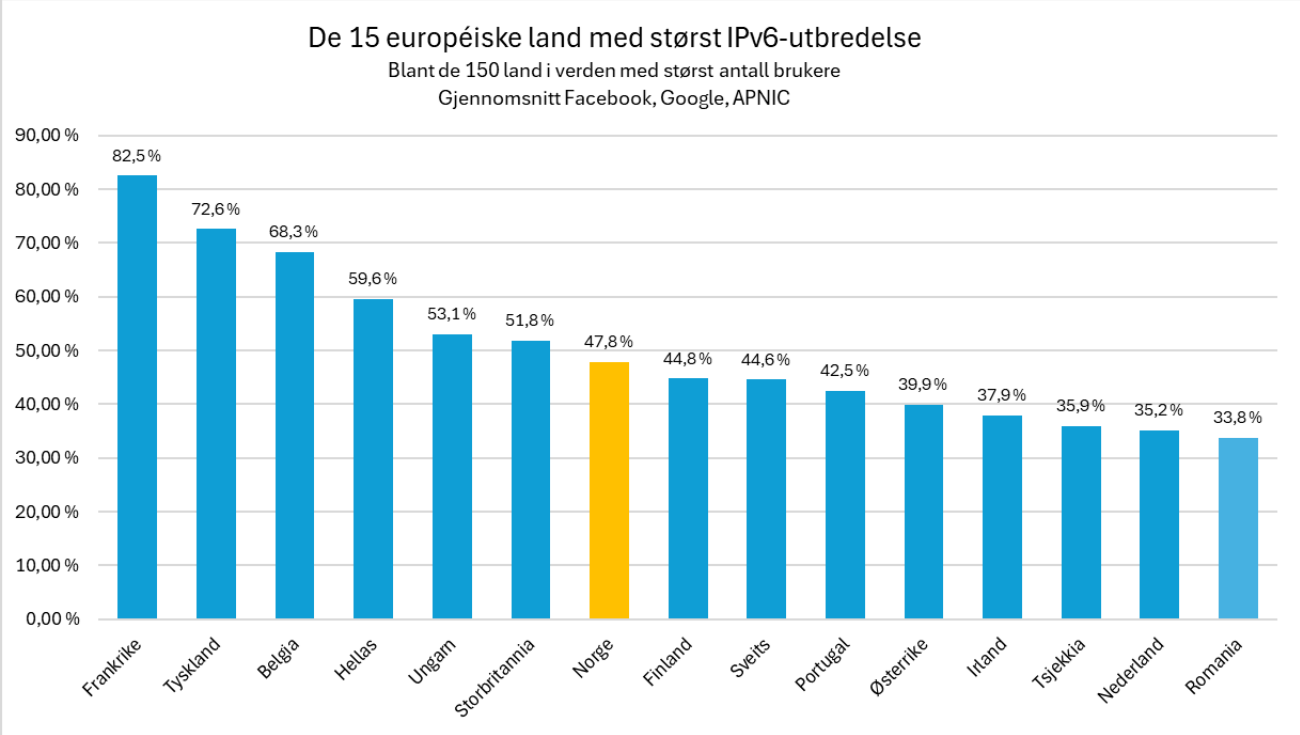
[16] https://www.facebook.com/ipv6/?tab=ipv6_country

[17] https://stats.labs.apnic.net/ipv6 – Målemetodikk

[18] Kun de 150 landene i verden med størst antall internettaksesser inngår i denne sammenlikningen.



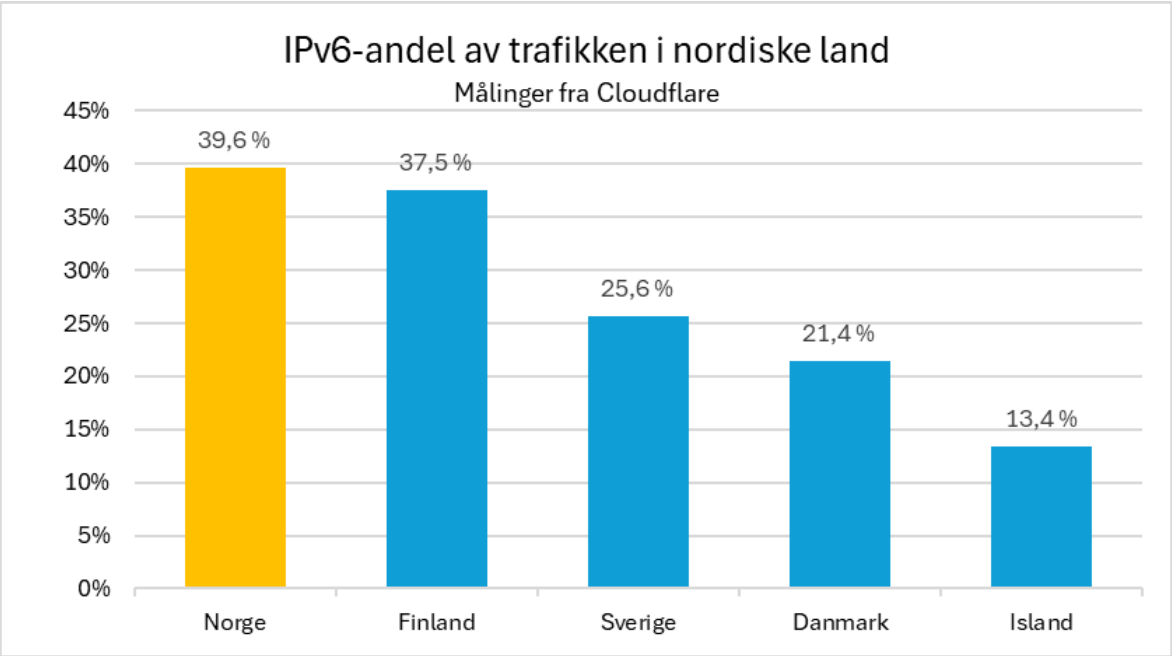
Figur 2 - IPv6-utbredelse i nordiske land



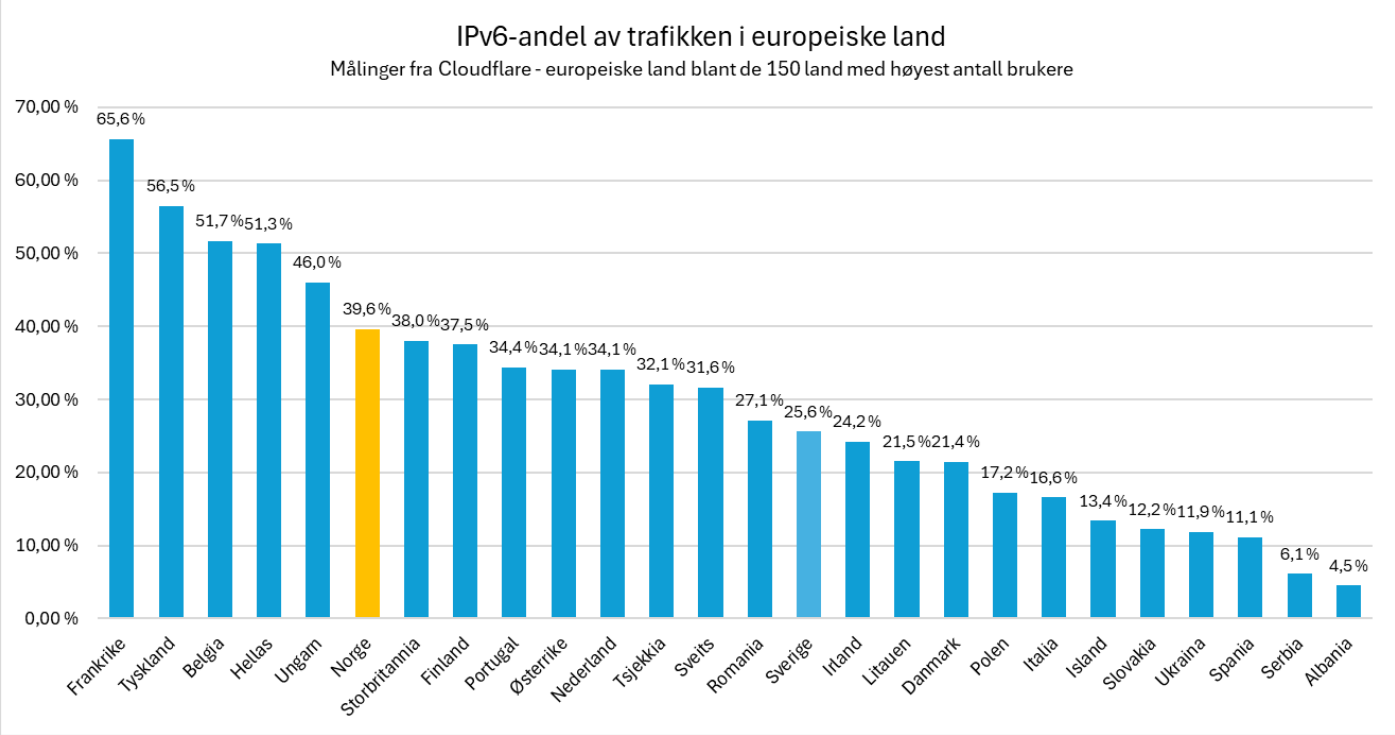
Figur 3 - IPv6-utbredelse i topp 15 land i Europa

I Figur 4 og Figur 5 nedenfor vises målinger fra Cloudflare av andelen IPv6-trafikk i målenoder sentralt i nettene for hhv. de nordiske land og for de 21 land i Europa som har størst IPv6 andel av trafikken og som også er blant de 150 land i verden med størst antall internettbrukere[19].

[19] https://radar.cloudflare.com/adoption-and-usage - Uttrekk pr. mars 26



Figur 4 Andel av internett-trafikken som er IPv6 - Norden



Figur 5 Europeiske land med høyest andel IPv6-trafikk blant de 150 land med høyest antall brukere

1.4.3 IPv6 aktiveringsandel hos norske tilbydere

I Figur 6 og Figur 7 nedenfor vises aktiveringsandel for IPv6 for henholdsvis fastnett og mobilnett for de største tilbyderne i Norge samlet, basert på opplysninger fra tilbyderne[20]. For mobilnettene vises også andel av IPv4- og IPv6-trafikk i nettene.

[20] Tallene ble hentet fra fastnettilbydere og mobilnettoperatørene i mars 2026

Største leverandører av fast bredbånd samlet - inkluderer FTB fra 2025	31.12.23	31.12.24	31.12.25
%-vis aksesser med IP V6-aktivering	63 %	78 %	79 %
Prosentandel eksisterende IPv6-kompatible, operatørutplasserte CPE'er	86 %	97 %	94 %
Prosentvis CPE'er som må byttes ut for FTB og fastnettbaserte tjenester	14 %	3 %	6 %

Figur 6 - Aktivering av IPv6 og andel CPE-utstyr som er IPv6-kompatibelt hos de største tilbyderne av fast bredbånd

Største mobilvirksomheter samlet	31.12.23	31.12.24	31.12.25
Andel abonnement i mobilnettene som kan få IPv6 - %	85 %	91 %	97 %
Internettrafikk volumet via IPv6 i mobilnett - %	42 %	40 %	45 %
Internettrafikk volumet via IPv4 i mobilnett - %	58 %	60 %	55 %

Figur 7 - Aktivering av IPv6 og andel av IPv4/IPv6 av trafikkvolumet hos de største mobiloperatørene

1.4.4 Regulatorisk oppfølging

Nkom gjennomførte i april 2023 dialogmøter om IPv6 med de største internettilbyderne i det norske markedet for å stimulere overgangen fra IPv4 til IPv6. Nkom presenterte følgende målsetning for opptrappingsplan for IPv6 de neste 2-3 årene, og de norske internettilbyderne (ISPene) ga uttrykk for at de på mange måter er på linje med forslaget[21]:

1. *Innen 30. april 2024 aktiverer norske ISPer IPv6 for alle sine internettabonnenter, eventuelt med unntak av abonnement som krever fysisk utskifting av hjemmeruter.*
2. *Innen 30. april 2025 har norske ISPer aktivert IPv6 for alle sine internettabonnenter, samt skiftet ut eventuelle hjemmerutere som ikke kunne oppgraderes via programvare.*
3. *Hjemmerutere basert på DSL-teknologi knyttet til kobbernettet trenger imidlertid ikke byttes ut før saneringen av kobbernettet er gjennomført.*

Nkom vil følge utviklingen av IPv6-bruken i det norske markedet tett i overgangsperioden.

- *Nkom vil publisere tertialvis statistikk over aktiv tilgjengeliggjøring av IPv6 hos norske ISPer, samt statistikk over bruk av IPv6 i det norske markedet som er tilgjengelig fra eksterne kilder.*
- *Nkom vil basert på den trinnvise utviklingen (innen utgangen av 2025) vurdere om det er behov for å innføre nasjonal regulering for å gjøre IPv6 obligatorisk blant norske ISPer.*

De største ISPene sender Nkom nå årlig oversikt over IPv6-aktivering i sine nett, og for aktørene samlet går utviklingen i riktig retning. Utfra målsettingene ovenfor og den rapporterte aktiveringsgraden for IPv6 sammenholdt med andelen av IPv6-trafikk, er det etter Nkoms syn behov for å følge opp både videre aktivering av aksesser og utskiftning av sluttbrukerutstyr. Utfra den positive utviklingen, anser Nkom at det likevel vil være tilstrekkelig med årlig rapportering.

Nkom oppfordrer norske ISPer til å forsterke innsatsen med å øke bruken av IPv6 for internettilgangstjenestene som tilbys. Denne innsatsen kommer i parallell med trenden fra utstyrstilbydere og programvaretilbydere med å innføre IPv6 i sluttbrukerutstyr.

[21] Jf. *Internett i Norge – Årsrapport 2023*, s. 21

2 Sikkerhet i internettilgangstjenester

Sikkerhet i internettilgangstjenester er en forutsetning for samfunnets, virksomheters og enkeltpersoners bruk. Nkom arbeider for et trygt og robust internett gjennom regulering, tilsyn og tett samarbeid med bransje og myndigheter. Gjennom bl.a. hendelsesoppfølging og krav til forsvarlig sikkerhet bidrar Nkom til å forebygge og håndtere digitale trusler. Arbeidet omfatter både sikring av elektroniske kommunikasjonsnett, datasentre og sentral digital infrastruktur. Nkom samarbeider aktivt med nasjonale og internasjonale aktører for å møte et mer komplekst og sammensatt trusselbilde. Samlet bidrar dette til økt tillit til internett og digitale tjenester. Målet er å sikre at befolkning, næringsliv og myndigheter har tilgang til trygge og tilgjengelige digitale tjenester i hele landet.

Ekomloven oppstiller krav om at tilbydere av internettilgangstjenester skal tilby elektroniske kommunikasjonstjenester med forsvarlig sikkerhet for brukerne i fred, krise og krig. Digitalsikkerhetsloven og -forskriften trådte i kraft 1. oktober 2025, og oppstiller krav til sikkerhet for sentralt register over norske toppnivådomener (.no), rekursive navnetjenester som i gjennomsnitt per 30 dager besvarer flere enn 15 000 domenenavnsystemforespørsler per sekund og samtrafikkpunkter for internett. Sammen bidrar de to regelverkene til at internettilgangstjenester skal være sikre og trygge for brukerne.

3 Status for nettnøytralitet i Norge

Tilstanden for nettnøytralitet i det norske markedet er fortsatt generelt god. Arbeidet med årets rapport har ikke avdekket større endringer eller avvik sammenlignet med fjorårets vurdering.

3.1 Innledning og bakgrunn

Nettnøytralitet er prinsippet om at all internettrafikk skal likebehandles, uavhengig av avsender, mottaker, utstyr, applikasjon, tjeneste eller innhold. Et felleseuropeisk regelverk om nettnøytralitet ble innført i 2015, og inntatt i norsk rett i 2017[22]. Hovedformålet med regelverket 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 garantere at internetts økosystem fortsetter å fungere som en motor for innovasjon*». [23]

Nkom regulerer nettnøytralitet i Norge basert på dette regelverket og på BERECs retningslinjer om nettnøytralitet, utformet med hjemmel i Forordning 2015/2120, artikkel 5 (3). Ifølge fortalens punkt 19 skal regulatører legge til grunn («*take utmost account of*») BERECs retningslinjer ved anvendelse av forordningen.

Denne rapporten dekker perioden 1. mai 2025 til 30. april 2026.

3.2 Tilgang til et åpent internett

Nkoms oppfølging av norske internettilbydere viser at norske internettbrukere nyter godt av åpen tilgang til internett via sine abonnement i fastnett og mobilnett. Internettilbydernes innrapportering indikerer at trafikkstyringen som benyttes er i tråd med nettnøytralitetsforordningen.

[22] Jf. Ekomforskriften, §1-11

[23] Forordning 2015/2120, fortalens første avsnitt

3.2.1 Retten til en åpen internettilgang

Sluttbrukerne har rett til en åpen internettilgang hvor man selv kan bestemme hva tilgangen brukes til, både hvilket innhold som hentes eller leveres, og hvilke applikasjoner som brukes eller tilbys, basert på forordningens artikkel 3(1). Internettilbyderen skal overføre trafikken i nettet på en ikke-diskriminerende måte, men har anledning til visse former for trafikkstyring som for eksempel å blokkere trafikk av sikkerhetsmessige grunner.

Internettilbyderen har også anledning til å tilby spesialiserte tjenester, for eksempel IPTV, i parallell med internettilgangen dersom disse har kvalitetskrav som ikke kan tilbys over internett. Videre kan spesialiserte tjenester bare tilbys hvis nettverkskapasiteten er tilstrekkelig til at det ikke går på bekostning av tilgjengeligheten og den generelle kvaliteten på internettilgangstjenester for sluttbrukerne.

3.2.2 Trafikkstyring av internettilgangen

Nkom har innhentet informasjon om trafikkstyring av internettilgangen fra norske internettilbydere. Årets resultater viser ingen signifikant forskjell fra fjorårets resultater.

Ifølge innhentet informasjon, er typiske trafikkstyringstiltak blokkering av domenenavn i DNS etter rettslig pålegg, Kripos Child Abuse Filter og blokkering av TCP/UDP-porter ved spesifikke sikkerhetstiltak (f.eks. for å forhindre DDoS og andre former for dataangrep).

I det norske markedet tilbys hastighetsdifferensiert mobil internettilgang. 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.

3.2.3 Spesialiserte tjenester

Nkom har også innhentet informasjon om spesialiserte tjenester, det vil si andre tjenester som tilbys i parallell med internettilgangstjenesten som oppfyller spesifikke kriterier i forordningen. En typisk spesialisert tjeneste i fastnett er IPTV. Tilsvarende er VoLTE vanlig å tilby som spesialisert tjeneste i mobilnett.

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 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.

3.3 Informasjon om internettilgangstjenesten

Nkoms gjennomgang av internettilbydernes nettsider viser at tilbyderne generelt opplyser tilfredsstillende om trafikkstyringstiltak. På enkelte nettsider kan det imidlertid være utfordrende å finne den relevante informasjonen, særlig når det gjelder ulike hastighetsparametere for fast internettilgang.

3.3.1 Krav til informasjon

Forordningen artikkel 4 fastsetter krav til informasjon om internettilgangstjenesten som tilbydere skal gjøre tilgjengelig for sine sluttbrukere. 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.

3.3.2 Informasjon om trafikkstyring

Tilbydere av internettilgangstjenester plikter å informere om hvilke trafikkstyringstiltak som brukes.

Aktuelle trafikkstyringstiltak er beskrevet i delkapittel 3.2.2. 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 viser at tilbyderne har en varierende, men generelt tilfredsstillende fremstilling av trafikkstyringstiltak. Det kan være utfordrende å finne den relevante informasjonen på enkelte nettsider. Noen 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 mening i overenstemmelse med regelverket.

3.3.3 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
- Normal tilgjengelig hastighet
- Maksimumshastighet
- Markedsført hastighet

Med «normal tilgjengelig hastighet» menes hastigheten som en sluttbruker kan forvente å oppnå mesteparten av tiden ved bruk av 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», på norsk ofte omtalt som «Fast Trådløs Bredbånd», FTB) som fast internettilgang. Dette omfatter for eksempel tilfeller der trådløs teknologi (inkludert mobilnett) 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.

For fast internettilgang ser Nkom at tilbyderne i varierende grad opplyser om de ulike hastighetsparameterne som forordningen krever. Markedsført og maksimal hastighet er som regel tydelig på tilbydernes nettsider. Informasjon om minimums- og normalt tilgjengelig hastighet er på enkelte tilbyderes nettsider mer uensartet og til dels mangelfull.

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 det 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 i abonnementene.

For mobil internettilgang anser Nkom at tilbyderne generelt opplyser om de ulike hastighetsparameterne som forordningen krever.

Konklusjon

Nkoms gjennomgang viser at tilbyderne i varierende grad presenterer informasjonen om internettilgangstjenesten. På enkelte nettsider kan det være utfordrende å finne den relevante informasjonen, og i noen tilfeller ser det ut som det mangler informasjon. Sluttbrukere bør derfor være bevisst hvilken informasjon man leter etter, eller kontakte sin tilbyder for å få spesifikk veiledning om hvor informasjonen er tilgjengelig. Nkom har ifm. årets rapportering valgt å følge nærmere opp enkelte aktører som ikke synes å ha offentliggjort informasjon om hastighet i tråd med nettnøytralitetskravene.

3.4 Kvalitet på internettilgangstjenesten

Resultater fra måletjenesten Nettfart viser at hastighet for fast internettilgang fortsetter den gode trenden fra forrige rapporteringsperiode. Gjennomsnittlig hastighet for nedlasting og opplasting for fast internettilgang i 2026 er henholdsvis 173 Mbit/s og 149 Mbit/s.

Med utgangspunkt i tall fra Nettfart observerer vi at gjennomsnittlig nedlastingshastighet, opplastingshastighet og forsinkelse for 5G-nettene i Norge i 2026 var henholdsvis 198 Mbit/s, 36 Mbit/s og 39 millisekunder (ms). Dette er forsiktig ned sammenlignet med 2025.

3.4.1 Krav til kvalitet på internettilgangstjenesten

Artikkel 5 i forordningen sier at nasjonale ekomregulatører har overvåkings- og rapporteringsforpliktelser som skal sikre at tilbydere av internettilgangstjenester oppfyller sine forpliktelser vedrørende åpen internettilgang. Videre skal regulatøren fremme ikke-diskriminerende internettilgang med kvalitetsnivå som gjenspeiler teknologiutviklingen.

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.

3.4.2 Regulatorisk oppfølging

Et regulatorisk 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

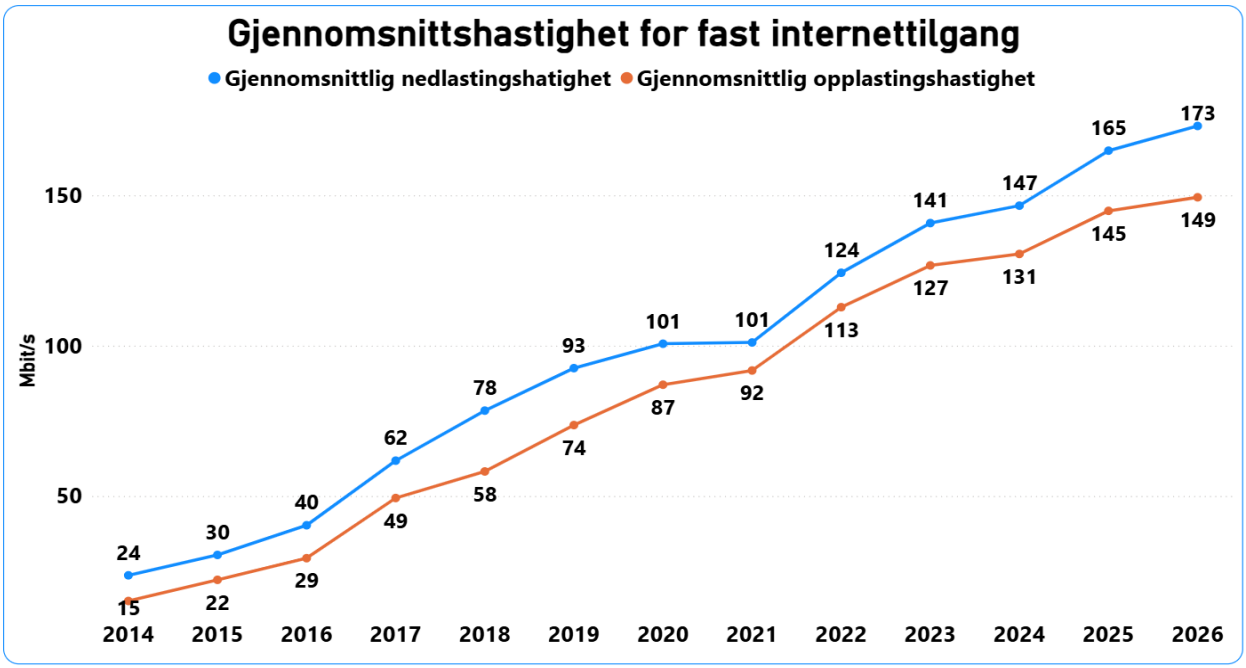
nettdugnad (crowd-sourcing) ved at det er brukerne selv som aktivt gjør målinger og dermed produserer datagrunnlaget som Nkom analyserer.

Som ved alle former for nettdugnad, kan det være noe begrenset hvor representativt det statistiske grunnlag 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.

3.4.3 Måleresultater

Måleresultater fra nettfart.no

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

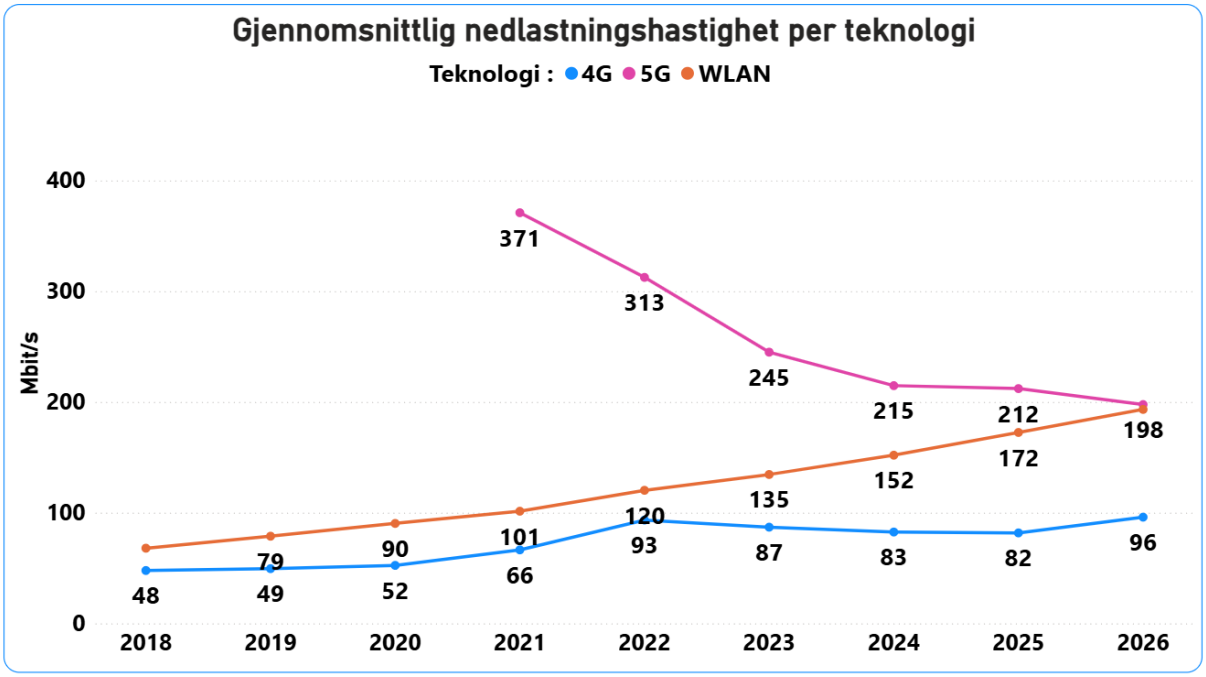


Figur 8 - Gjennomsnittshastighet for fast internettilgang (kilde: nettfart.no)

Figur 8 viser at gjennomsnittlig målt nedlastningshastighet på tvers av sluttbrukernes ulike abonnement, hittil i 2026 er om lag 70 % høyere enn verdiene var for fem år siden (2021). Trenden med årlig vekst på 10-20 Mbit/s per år ser ut til å flate noe ut sammenlignet med verdiene fra de forrige årene.

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 i 2025.

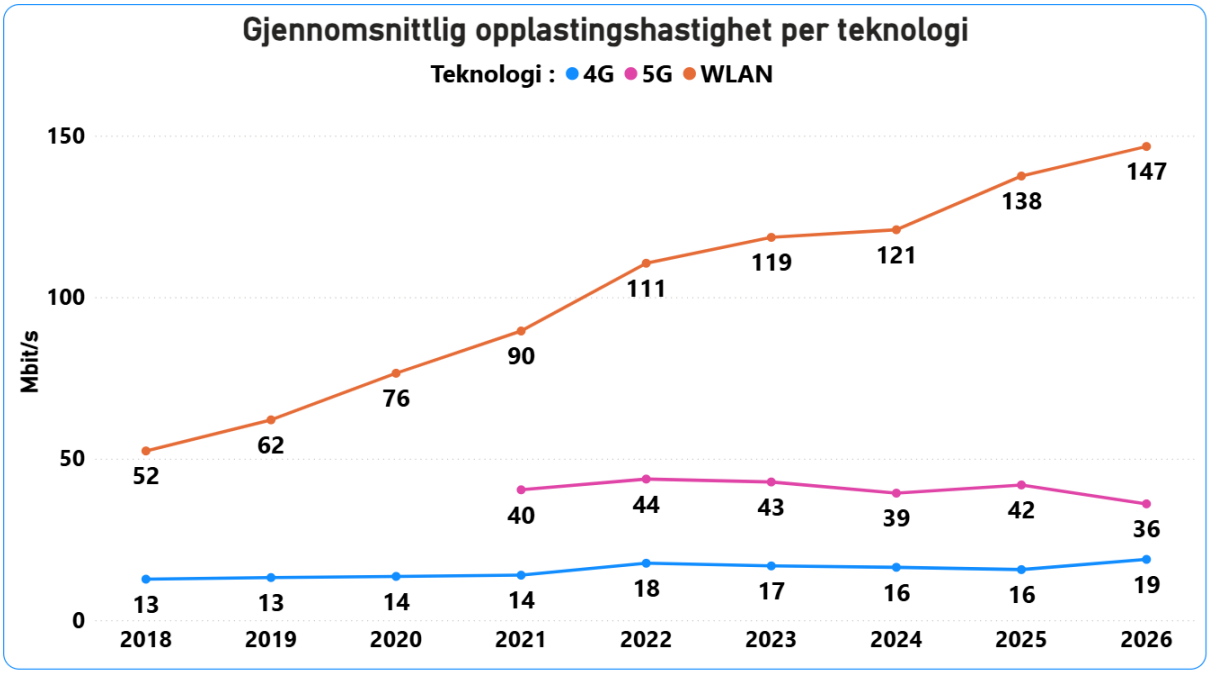


Figur 9 - Gjennomsnittlig nedlastningshastighet per teknologi (kilde: Nettfart mobilapp)

Figur 9 viser gjennomsnittlig 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. Nytt dette året er imidlertid at målinger gjort via WLAN oppnår samme gjennomsnittshastighet som målinger gjort via 5G. For mobilteknologiene 5G og 4G viser figuren at 4G har løftet seg noe sammenlignet med forrige år, men at 5G på sin side har en reduksjon.

Sett samlet er gjennomsnittlig nedlastingshastighet for [4G + 5G] i 2026 identisk med verdiene for 2025. Vi vet at totalt trafikkvolum i mobilnettene har økt det siste året og det kan så langt se ut til at mobiloperatørene fortsatt bygger kapasitet for å holde tritt med denne utviklingen.

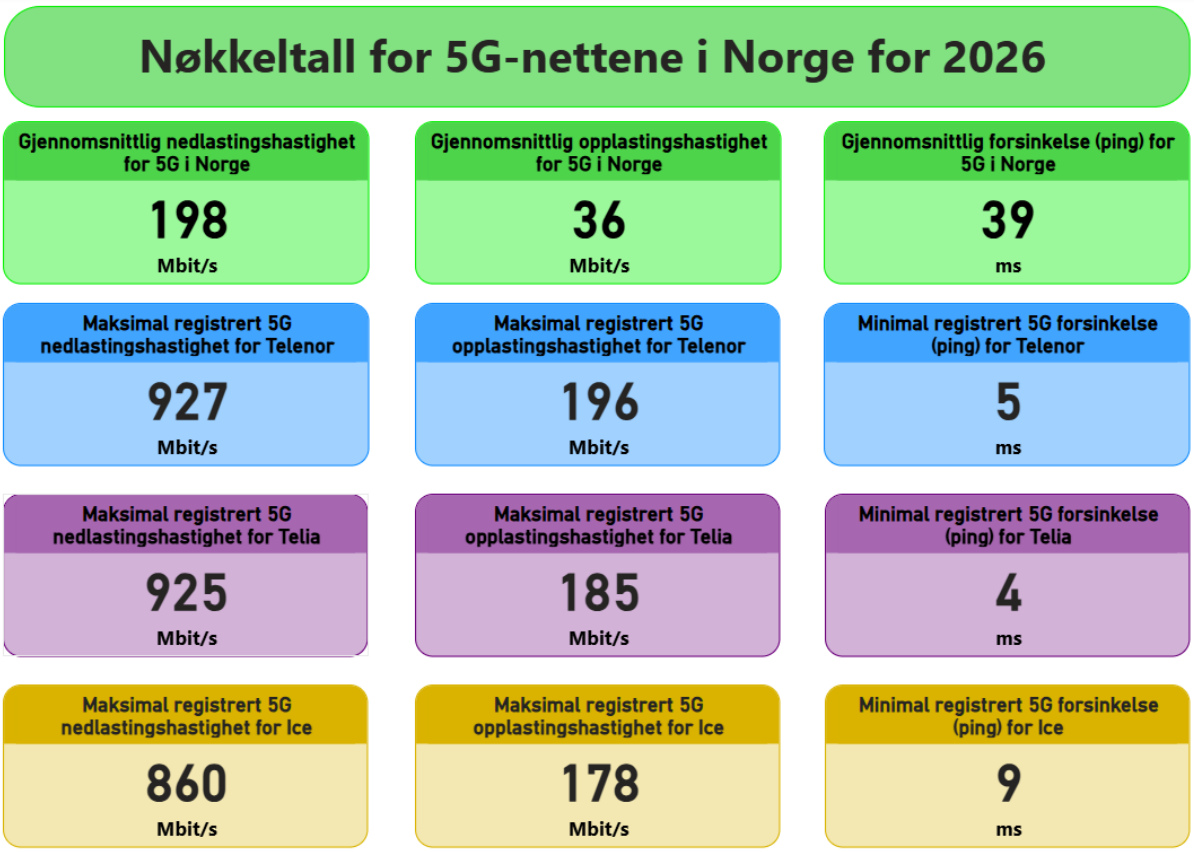
Gjennomsnittlig nedlastingshastighet for WLAN øker fortsatt og i løpet av det siste året har den økt med 15 %. For WLAN-målinger er det imidlertid usikkert hvilket transmisjonsmedium som benyttes til og fra stedet der målingen ble gjort. Det kan være fiber, hybridkabel eller fast trådløst bredbånd.



Figur 10 - Gjennomsnittlig opplastingshastighet per teknologi (kilde: Nettfart mobilapp)

Figur 10 viser at mobilteknologier (4G og 5G) har til dels betydelig lavere opplastingshastighet 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, jf. Figur 9. Forklaringen er sannsynligvis at mobilnettene reserverer en større del av det tilgjengelige frekvensspektrumet (og/eller tidsdelingen i 5G) til nedlasting, ettersom en antar at dette er den dominerende retningen for trafikk mellom internett og den enkelte bruker. Nkom observerer at gjennomsnittlig opplastingskapasitet for 5G pr mai 2026 er lavere enn for fem år siden, da rapporteringene startet.



Figur 11 - Nøkkeltall for 5G-nettene i Norge for 2026 (kilde: Nettfart mobilapp)

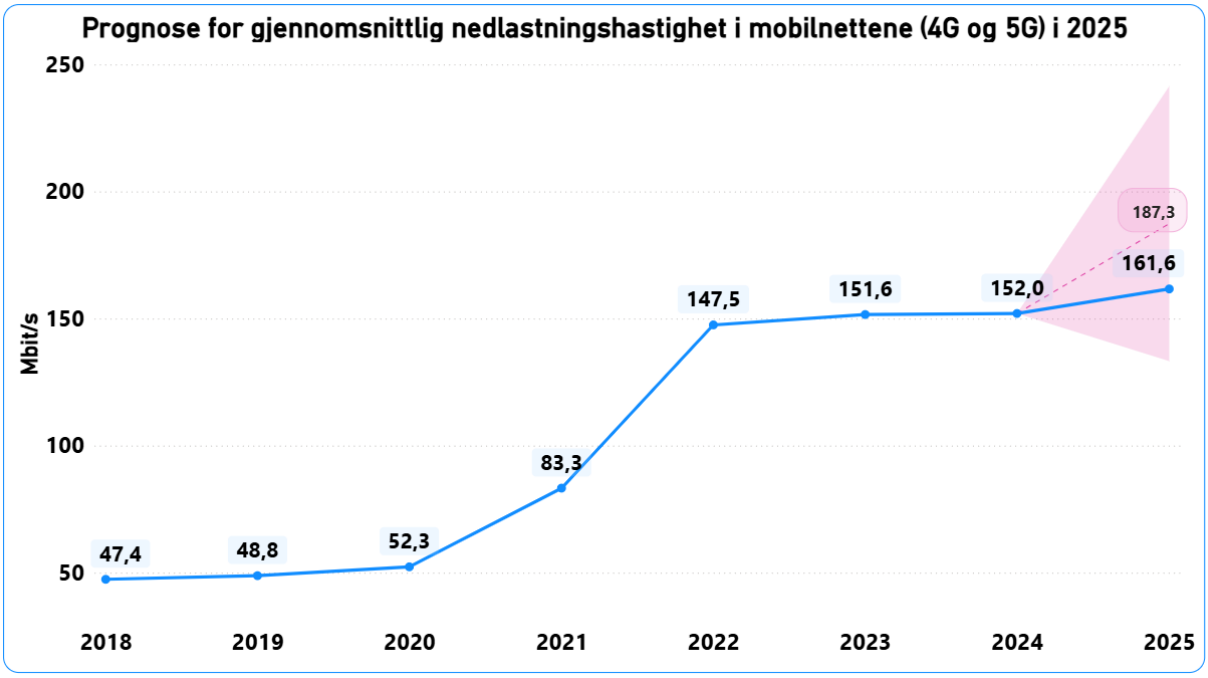
Figur 11 viser utvalgte nøkkeltall for 5G-målinger i mobilnettene i 2026. Gjennomsnittlig nedlastingshastighet, opplastingshastighet og forsinkelse for 5G-nettene i Norge i 2025 var henholdsvis 198 Mbit/s, 36 Mbit/s og 39 millisekunder (ms). Målinger fra Nettfart mobilapp viser at 5G-nettene i Norge tilbyr internettilgang med høye hastigheter og lav forsinkelse. Det blir ellers interessant å se hvordan en fremtidig aktivering av 5G Stand Alone for smarttelefoner kommer til å påvirke nøkkeltallene.

3.4.4 Generell kvalitet på internettilgangstjenesten

Nkom har anvendt BERECs metode for evaluering av generell kvalitet på internettilgangstjenesten på målingene gjort i mobilnettene. Metoden benytter en prognosefunksjon basert på gjennomsnittlig nedlastingshastighet, opplastingshastighet 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.

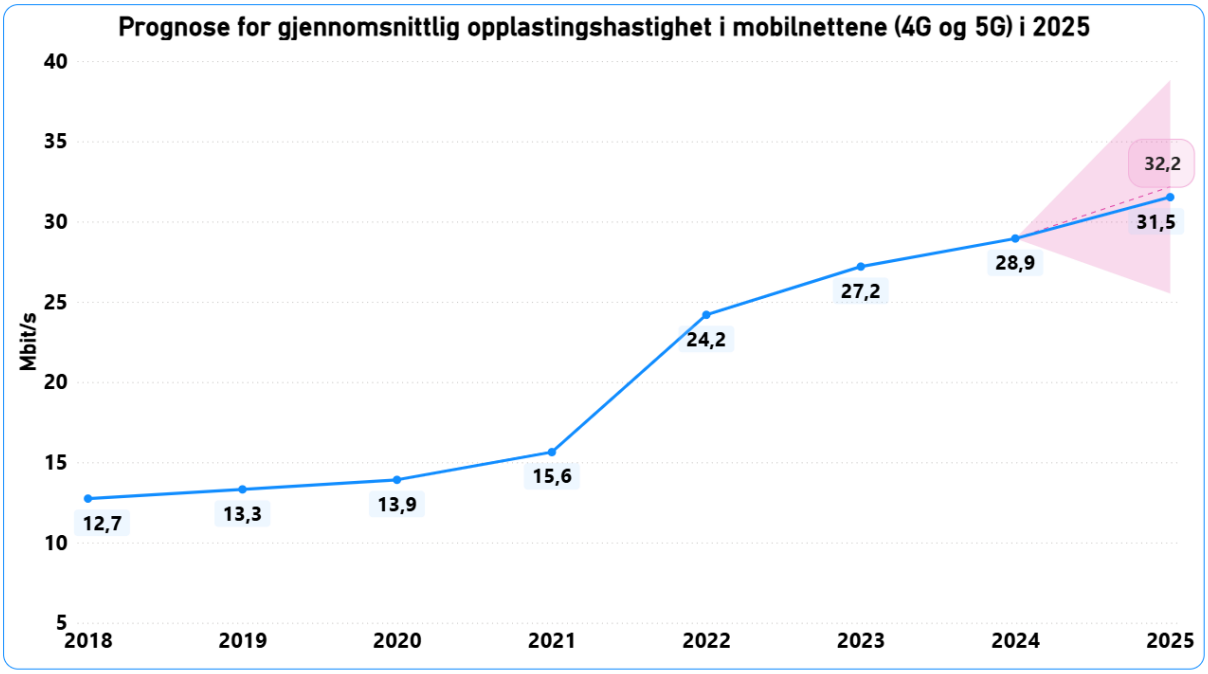
Figurene nedenfor viser prognoser[24] for nedlasting- og opplastingshastighet samt forsinkelse for målinger gjort i mobilnettene i Norge, aggregert for alle mobiloperatørene. Blå linje viser de målte verdiene og rosa stiplet linje viser prognosen for 2025.

[24] Prognoser for 2025 bygger på historiske data fra 2018-2024.



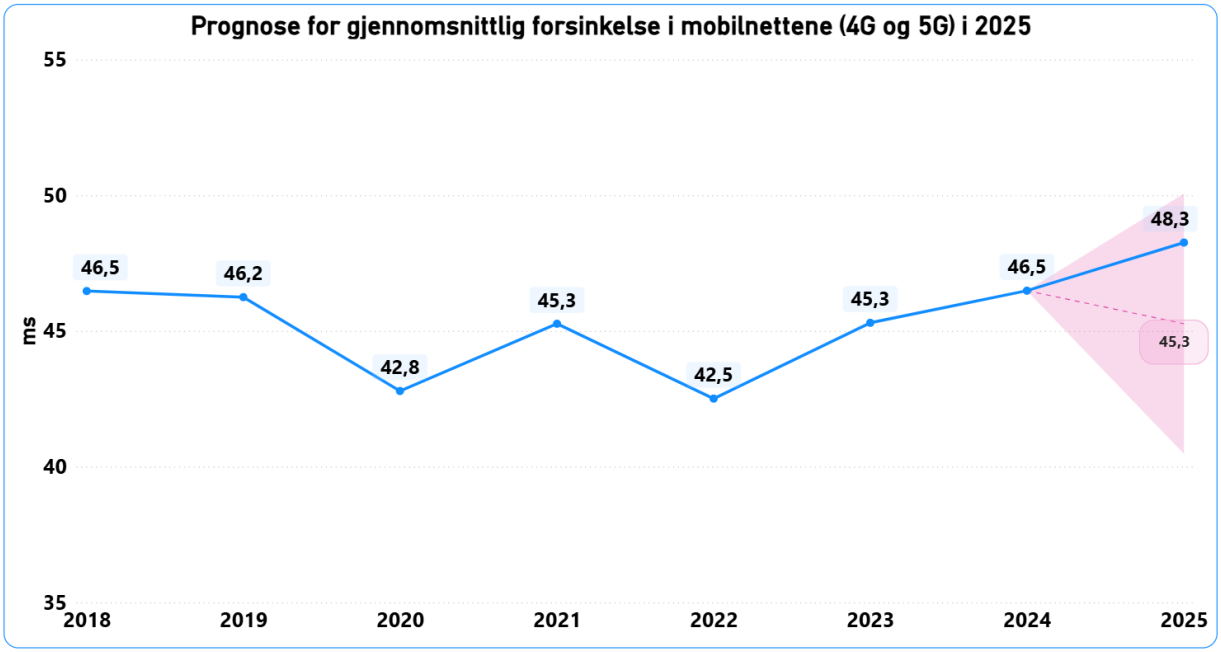
Figur 12 - Prognose for gjennomsnittlig nedlastningshastighet i mobilnettene i 2025

Figur 12 viser prognosen for gjennomsnittlig nedlastingshastighet for 2025 på 187 Mbit/s, samtidig som den målte gjennomsnittsverdien var om lag 162 Mbit/s. Dette viser at utviklingen for nedlastingshastighet i mobilnettene i 2025 ikke har møtt den matematiske forventningen basert på verdiene fra tidligere år. Likevel er avviket mellom målt og predikert verdi på et akseptabelt nivå.



Figur 13 - Prognose for gjennomsnittlig opplastingshastighet i mobilnettene i 2025

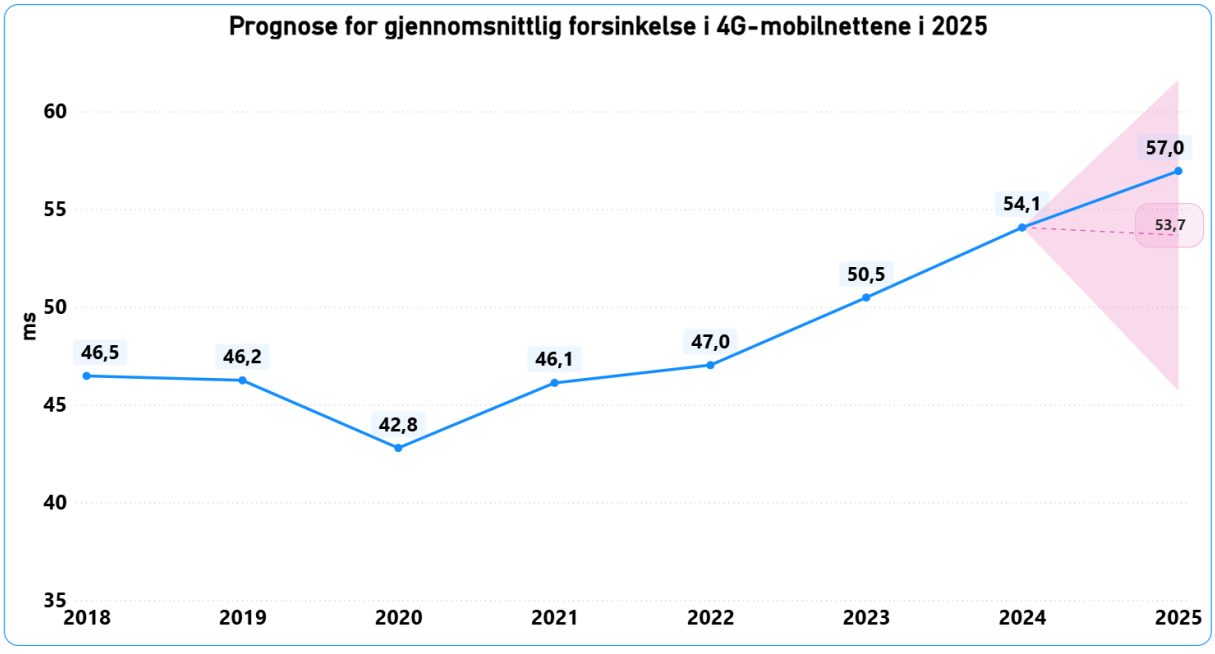
Figur 13 viser prognosen for gjennomsnittlig opplastingshastighet for 2025 på ca. 32 Mbit/s, samtidig som den målte gjennomsnittsverdien var 31,5 Mbit/s. Dette viser at utviklingen for opplastingshastighet i mobilnettene var svært tett på prognosen.



Figur 14 - Prognose for gjennomsnittlig forsinkelse i mobilnettene i 2025

Figur 14 viser at prognosen for gjennomsnittlig forsinkelse kombinert for 4G og 5G i 2025 var 45 ms, og at den målte gjennomsnittsverdien var om lag 48 ms. Dette viser at utviklingen for forsinkelse i mobilnettene har vært noe dårligere enn prognosen skulle tilsi. Vi har imidlertid analysert dette nærmere og sett på verdiene for 4G og 5G hver for seg. Som de neste figurene viser er det måleresultater fra 4G-teknologien som i stor grad preger den overordnede trenden.

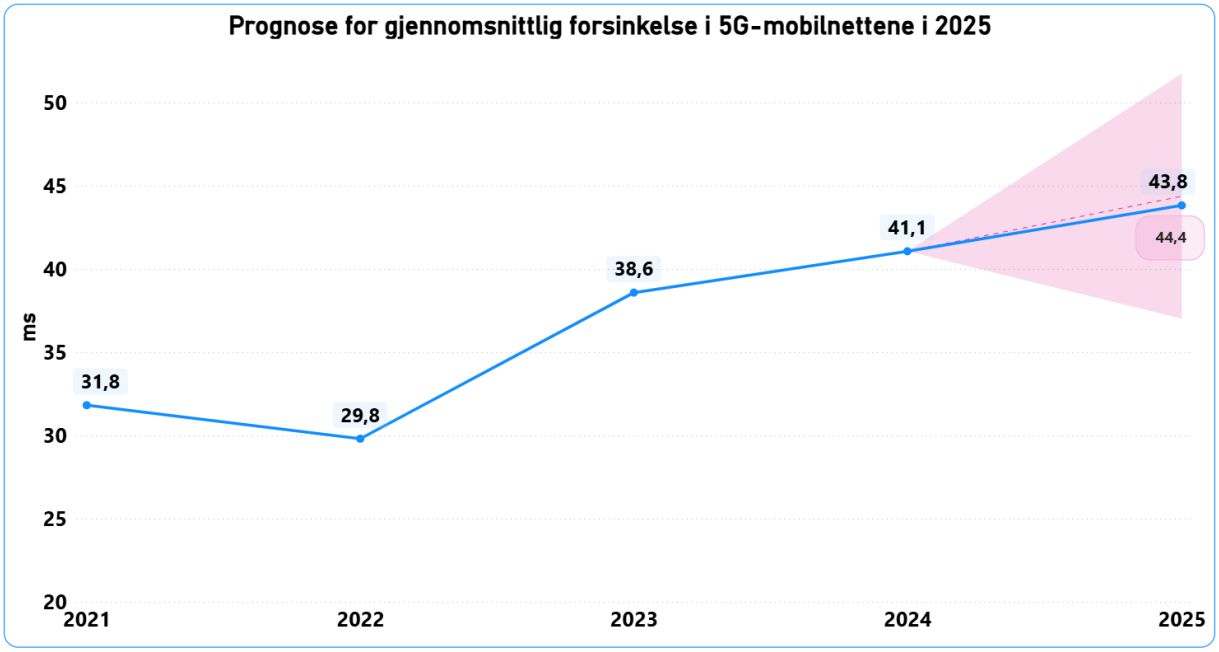
Figur 15 viser verdiene når 4G-målingene betraktes for seg selv:



Figur 15 - Prognose for gjennomsnittlig forsinkelse i 4G for 2025

For 4G viser resultatene at utviklingen i forsinkelse avviker tydeligere fra forventningene.

For 5G er trenden en annen og her kommer teknologiforskjellene klarere til syne:



Figur 16 - Prognose for gjennomsnittlig forsinkelse i 5G for 2025

Måleresultatet som angitt i Figur 16 er her tett på den matematiske forventningen.

Konklusjon

Nkoms analyse av måleresultatene fra Nettfart, både fra bruk av nettsiden og mobilappen, avdekker to trender: for det første fortsetter målt kapasitet i fastnettene å øke, og for det andre reflekteres ikke den samme trenden like sterkt for målinger utført i mobilnettene. Gitt antatt fortsatt økning av datatrafikk blir det viktig å følge med på om mobilnettnetteierne kan svare på dette med å fortsette utbygging av kapasitet i sine nett. De kommende årene forventes det at 5G SA blir tatt i bruk for vanlige smarttelefoner og det knytter seg forventninger til hva denne teknologien kan bidra med når det kommer til kundenes opplevelse av kvalitet.

4 Digital Services Act (DSA) og Nkoms rolle som DSA-koordinator

Digital Services Act (DSA) regulerer internettbaserte tjenester og plattformer og formålet er å skape et tryggere og mer ansvarlig digitalt rom i EU. Regelverket skal blant annet beskytte brukere mot ulovlig innhold og manipulasjon, samt verne mindreårige på digitale tjenester. De største nettbaserte plattformene pålegges ekstra strenge krav. Nkom er utpekt som koordinerende myndighet for regelverket i Norge, mens Medietilsynet, Forbrukertilsynet og Datatilsynet vil bli tildelt tilsynsansvar innenfor sine respektive ansvarsområder.

4.1 Bakgrunn og formål - Nkoms nye temasider om DSA

Det er en omfattende regulatorisk utvikling i Norge og EU som i stor grad vil påvirke fremtidens internett. En viktig europeisk rettsakt er forordningen om digitale tjenester (Digital Services Act, DSA), som ble vedtatt i EU oktober 2022 og trådte i kraft i november 2022. Implementeringen av regelverket i norsk rett er under arbeid.

Formålet med DSA er å sikre et tryggere og mer transparent internett for brukere av internettbaserte tjenester og plattformer, og å styrke beskyttelsen av brukernes grunnleggende rettigheter. Blant annet skal globale aktører i større grad godtgjøre hvordan plattformene deres fungerer og hvordan de leverer tjenester til brukerne, hvordan de bruker og behandler opplysninger om brukerne, og hvilke systemrisikoer tjenestene kan medføre – herunder risiko for ytringsfrihet, demokratiske prosesser og brukernes sikkerhet og rettigheter.

Les mer på Nkoms sider om trygt internett og DSA.

4.2 Nkom som DSA-koordinator

DSA skal håndheves både på nasjonalt og europeisk nivå. På nasjonalt nivå har det blitt utpekt flere kompetente myndigheter som vil få tilsynskompetanse på sine respektive ansvarsområder, samt en koordinerende myndighet som vil ha det overordnede ansvaret for oppfølgning av DSA på nasjonalt nivå. På europeisk nivå har EU-kommisjonen myndighet til å føre tilsyn med de største plattformene og søkemotorene (VLOP-er og VLOSE-er), selskaper som individuelt når ut til mer enn 10 prosent av EUs befolkning, omtrent 45 millioner mennesker.[25] Det vil også være samhandling mellom DSA-koordinatorer på tvers av landegrenser.

Digitaliserings- og forvaltningsdepartementet (DFD) har utpekt Nkom som nasjonal DSA-koordinator i Norge. Det betyr blant annet at Nkom får hovedansvaret for at digitale tjenester og plattformer overholder regelverket, og ansvaret for koordinering av tilsyn. Medietilsynet, Forbrukertilsynet og Datatilsynet er utpekt som vedkommende myndigheter, og vil bli tildelt tilsynsansvar innenfor sine kompetanseområder. Nkom og de øvrige myndighetene vil utgjøre det nasjonale DSA-nettverket, som vil sikre samarbeid og samhandling ved håndhevelse av DSA i Norge.

I tilfeller hvor det er grunnlag for mistanke om at tilbyder i Norge bryter pliktene i DSA, vil Nkom eller de øvrige vedkommende myndigheter kunne benytte de undersøkelses- og håndhevingsvirkemidlene som følger av regelverket. Dette kan for eksempel omfatte pålegg om informasjon, krav om medvirkning til kontrollundersøkelse og/eller be representanter for virksomheten redegjøre for informasjon og opplysninger om saken. Dersom det på bakgrunn av informasjonsinnhentingen eller andre undersøkelser avdekkes brudd på DSA kan både Nkom og øvrige utpekte vedkommende myndigheter innenfor sine ansvarsområder treffe vedtak om nødvendige tiltak og sanksjoner, for eksempel pålegg om opphør eller endring, overtredelsesgebyr og/eller begrensning av tilgang til tjenesten.

Nkom er underlagt DFD og utfører sine forvaltningsoppgaver i henhold til departementets tildelingsbrev og øvrige instrukser og bestillinger. Ifølge DSA artikkel 50 nr. 2 skal imidlertid DSA-koordinatoren og vedkommende myndigheter opptre med full uavhengighet fra andre myndigheter og private parter. Departementet kan dermed for eksempel ikke pålegge Nkom som DSA-koordinator å treffe en bestemt konklusjon i klagesaker, utforme den årlige aktivitetsrapporten på en gitt måte, eller prioritere utvalgte tilsynsområder.

Nkom plikter å utarbeide en årlig aktivitetsrapport, i henhold til DSA artikkel 55. Rapporten skal blant annet inneholde en oversikt over antall klager og hvordan klagene er behandlet, og den skal dekke aktiviteter hos både DSA-koordinatoren og andre utpekte kompetente myndigheter i Norge. Rapporten skal oversendes Europakommisjonen og det europeiske DSA-rådet.

4.3 Plattformenes plikter og brukernes rettigheter

DSA fastsetter en rekke krav til internettbaserte tjenester og plattformer, også kalt formidlingstjenester. Pliktene varierer avhengig av hvilken type tjeneste det er snakk om og hvor store plattformene er. Regelverket gjelder også for tjenester som tilbys fra land utenfor Europa, så lenge de er rettet mot europeiske brukere.

[25] Forordning om digitale tjenester (Digital Services Act - DSA) - regjeringen.no. Jf. også kap. 4.4.

Forordningen innebærer at nettbaserte plattformer, og særlig de aller største, får omfattende plikter. Alle nettbaserte plattformer må bl.a.:

- Utvikle effektive systemer som gjør det enklere å identifisere, melde fra om og fjerne ulovlig innhold.
- Gi brukerne begrunnelse når innhold eller brukere fjernes
- Tilby mulighet for å klage.
- Rapportere om omfanget av fjernet og redigert innhold.
- Sørge for at selgere på handelsplattformer kan identifiseres og spores.

I tillegg pålegges de største plattformene å gjennomføre risikovurderinger knyttet til systemiske samfunnstrusler, samt gi innsyn i relevante data med myndigheter og forskningsmiljøer.

For at ansvaret som DSA medfører for tilbydere av formidlingstjenester skal overholdes, blir det viktig at aktørene har åpenhet og publiserer tydelige kriterier for hvordan innholdet blir håndtert av tilbyderen. Dette er en forutsetning for at brukerne skal forstå hvordan deres informasjon og innhold vil bli behandlet.

Når en bruker er uenig i en beslutning tatt av en nettbasert plattform knyttet til moderering, for eksempel fjerning av innhold eller stenging av en konto, gir DSA brukeren rett til å klage til tilbyderen. Plattformene er forpliktet til å tilby effektive klagemuligheter og transparente klageprosesser som skal være tilgjengelige og gratis for alle brukere.

Dersom en bruker er uenig i plattformens beslutning etter intern klagebehandling, kan saken bringes inn for et sertifisert uavhengig tvisteløsningsorgan. Tvisteløsningen skal være utenrettslig og gi en kostnads- og tidseffektiv behandling av saken. Tvisten kan gjelde både beslutninger om fjerning eller begrensning av innhold, manglende fjerning etter varsel eller innhold som anses å være uforenlig med generelle vilkår og betingelser for bruk av plattformen. Tvisteløsningsorganet vurderer om plattformen har håndtert saken i tråd med regelverket og egne vilkår. Ordningen skal være rimelig for brukeren, og plattformen skal normalt dekke kostnadene dersom brukeren får medhold. Tvisteløsningsorganet kan være en eksisterende aktør, eller medlemsstaten kan opprette et slikt organ. Organet skal være upartisk og uavhengig, herunder også økonomisk uavhengig, av tilbydere av plattformene og mottakerne av tjenestene. Organisasjoner som ønsker å være utenrettslig tvisteløsningsorgan etter DSA, må sertifiseres av DSA koordinatoren i sitt etableringsland. En sertifisering er gyldig i alle medlemsstatene. En tjenestemottaker kan bringe saken sin inn for domstolene, selv om vedkommende har tatt saken til et utenrettslig tvisteløsningsorgan. [26]

Videre gir DSA tjenestemottakere og andre aktører som handler på deres vegne rett til å kontakte myndighetene dersom de mener at en tilbyder av formidlingstjenester har overtrådt forordningen. Klage skal sendes til koordinatoren eller tilsynsmyndigheten for sitt kompetanseområde i den medlemsstaten hvor tjenestemottakeren befinner seg eller er etablert. Tilsynsmyndigheten skal vurdere klagen, men har et skjønn med hensyn til hvordan og i hvilken grad klagen skal følges opp. Dersom saken egentlig hører inn under en annen relevant myndighet i samme medlemsstat, skal klagen videreformidles dit. Gjelder klagen en formidlingstjeneste som er etablert i en annen medlemsstat, kan klagen, hvis relevant, sendes videre til koordinatoren i etableringsstaten. En slik oversendelse kan også inneholde en uttalelse fra den opprinnelige koordinatoren.

Det er viktig å merke seg at koordinator eller vedkommende tilsynsmyndigheter ikke fungerer som en generell klageinstans for plattformenes innholdsvurderinger. Når koordinator eller vedkommende myndigheter vurderer en klage fra en tjenestemottaker, skal det vurderes hvorvidt plattformen har overholdt sine plikter etter DSA. Det kan for eksempel bety å vurdere hvorvidt tilbydere oppfyller krav om internt klagebehandlingssystem etter artikkel 20 eller om tilbyderen har gitt tilstrekkelig begrunnelse etter artikkel 17. Koordinator eller vedkommende myndigheter vil ikke vurdere om for eksempel selve

[26] Høringsnotat om digitaltjenesteloven - regjeringen.no, side 19 punkt 5.4.3

innholdsavgjørelsen etter en intern klagebehandling hos plattformen er riktig eller ikke, men om beslutningen og prosessen i forkant er i samsvar med kravene i DSA.

4.4 Pliktsubjekter etter DSA

Forordningen gjelder uansett hvor tjenestetilbyderen er etablert, så lenge tjenesten retter seg mot brukere i EU. Regelverket vil omfatte norske brukere når regelverket blir implementert i Norge. Tilbydere som ikke er etablert i EU må utpeke en juridisk representant i et av medlemslandene hvor tjenesten tilbys. Denne representanten skal blant annet ivareta kommunikasjonen med vedkommende myndigheter, Europakommisjonen og det europeiske DSA-rådet i saker som gjelder mottak, etterlevelse og håndheving av beslutninger.

Tjenestemottakere kan klage til DSA-koordinatoren eller tilsynsmyndigheten i medlemsstaten der brukeren holder til, dersom de mener en tilbyder har brutt forordningen. Hvis tilbyderen er etablert i et annet EU/EØS-land, skal koordinatoren videresende klagen til rette DSA-koordinator, eventuelt med en egen vurdering av klagen.

DSA gjelder for alle typer tilbydere av formidlingstjenester, ikke bare de største aktørene. Hvor omfattende plikter de pålegges, avhenger imidlertid av hvilken kategori tjenestetilbyderen tilhører. Regelverket skiller mellom flere typer formidlingstjenester/«intermediary services»:

1) Ren videreformidling («mere conduit»), for eksempel internettilbydere (ISP-er)
2) Mellomlagring («caching»)
3) Vertstjenester («hosting»)
    a) Nettbaserte plattformer («online platforms») er **en** underkategori av vertstjenester. For eksempel nettmarkedsplasser som bringer sammen selgere og forbrukere, appbutikker, og sosiale medieplattformer. Mikro- og små virksomheter som driver nettbaserte plattformer er i hovedsak unntatt fra de mest tyngende administrative forpliktelsene under DSA.
        i) Veldig store nettbaserte plattformer ("very large online platforms – VLOPs") er **en** underkategori av nettbaserte plattformer med utvidede forpliktelser.[27]
4) Veldig store nettbaserte søkemotorer («very large online search engines – VLOSEs») er en egen kategori formidlingstjenester etter DSA. De er ikke nettbaserte plattformer, men er underlagt mange av de samme utvidede forpliktelsene som VLOPs.

På nasjonalt nivå er det i hovedsak tilbydere som tilhører de to første kategoriene av formidlingstjenester, samt tilbydere av nettbaserte plattformer bortsett fra VLOPs, som Nkom og andre tilsynsmyndigheter på nasjonalt nivå vil føre tilsyn med. Pliktene som pålegges tilbyderne etter DSA er dels generelle og dels avhengig av hvilken type tjeneste(r) som tilbys. Hensikten med å oppstille pliktene på denne måten er at tilbydere pålegges en mer aktiv rolle i håndtering og organisering av innhold – for eksempel lagring, tilrettelegging eller formidling til brukere – og pålegges flere og mer omfattende forpliktelser enn tilbydere som kun videreformidler informasjon.[28]

På europeisk nivå vil Europakommisjonen føre tilsyn med de veldig store nettbaserte plattformene og veldig store nettbaserte søkemotorene. Tilbyderne av disse plattformene og søkemotorer er underlagt særlig omfattende og strenge regulatoriske forpliktelser, blant annet knyttet til risikovurdering, risikoreduserende tiltak og økt transparens.

Disse pliktsubjektene (VLOPs og VLOSEs) har et gjennomsnittlig antall månedlige aktive brukere i EU på 45 millioner eller mer. Så høye brukertall innebærer en særlig systemisk risiko. Europakommisjonen har kompetanse til å føre tilsyn med og håndheve de særskilte forpliktelsene som gjelder for disse aktørene. Nasjonale koordinatorer kan ikke selv håndheve disse særskilte forpliktelsene, men kan bistå Europakommisjonen med informasjon og anmode Kommisjonen om å undersøke mulige brudd på regelverket. Når Europakommisjonen innleder en sak mot en VLOP eller VLOPSE varsles samtidig alle

[27] Forordning om digitale tjenester (Digital Services Act - DSA) - regjeringen.no

[28] Tilbydernes plikter - Nkom

DSA-koordinatorene, som deretter skal oversende relevante opplysninger de måtte besitte i relasjon til saken.

Kommisjonen har per 26. mars 2026 utpekt følgende aktører som VLOPSEs:[29]

AliExpress	Instagram	TikTok
Amazon Store	LinkedIn	WhatsApp
Apple AppStore	Microsoft Bing	Wikipedia
Booking.com	Pinterest	X (Twitter)
Facebook	Pornhub	XNXX
Google Maps	Shein	XVideos
Google Play	Snapchat	YouTube
Google Search	Stripchat	Zalando
Google Shopping	Temu	

4.5 DSA og regjeringens forslag om aldersgrense på sosiale medier

Et eksempel på en lovbestemmelse som vil fremme formålene bak DSA er kravet om særlig beskyttelse av mindreårige. Alle tilbydere av digitale plattformer som er tilgjengelige for mindreårige skal iverksette tiltak for å sikre et høyt nivå av både personvern, sikkerhet og trygghet for unge brukere.

Som et tillegg til kravet om særlig beskyttelse av mindreårige i DSA har regjeringen uttalt at de vil legge frem et nytt lovforslag om aldersgrense for barn i sosiale medier for Stortinget i år. Statsminister Støre uttalte i den forbindelse at «*[d]ette er et viktig grep for å trygge barns digitale hverdag*», og Norge vil være blant de første til å innføre lovfestet aldersgrense på sosiale medier. Regjeringen har lagt til grunn at DSA gir et rettslig rammeverk som gjør det mulig å pålegge plattformene ansvar for å håndheve en nasjonal aldersgrense, blant annet gjennom krav til aldersgrense og beskyttelse av mindreårige.[30]

5 KI-forordningen og Nkoms rolle som KI-myndighet

KI-forordningen etablerer et felles regelverk for utvikling og bruk av kunstig intelligens i EU/EØS med mål om å sikre trygg og ansvarlig KI. Regelverket bygger på en risikobasert tilnærming med strenge krav til KI-systemer med høy risiko, mens visse KI-praksiser er forbudt. Det innføres også egne regler for de kraftigste KI-modellene, som også kan gi plikter for norske virksomheter som tar dem i bruk. Nkom er koordinerende markedstilsynsmyndighet og felles kontaktpunkt for KI-forordningen i Norge.

5.1 Bakgrunn og formål – Nkoms nye fagsider om KI-forordningen

Kunstig intelligens (KI) blir stadig en større del av hverdagen, i alt fra digitale tjenester til helsehjelp og offentlig forvaltning. For å møte de mulighetene og utfordringene som KI fører med seg har EU vedtatt KI-forordningen (AI Act). Dette er det første helhetlige regelverket som fastsetter bindende regler for kunstig intelligens. Forordningen skal skape rettslig forutsigbarhet for alle berørte aktører i både privat og offentlig sektor, blant annet leverandører og brukere av KI-systemer. Samtidig skal den legge til

[29] Supervision of the designated very large online platforms and search engines under DSA

[30] Loven kommer etter planen i år – slik blir aldersgrensen for sosiale medier - regjeringen.no

rette for innovasjon og teknologisk utvikling, innenfor rammer som ivaretar grunnleggende samfunnsverdier og rettigheter.

KI-forordningen er en EU-forordning som fastsetter bindende regler i EUs medlemsland. For at dette regelverket skal få virkning i Norge, må det tas inn i EØS-avtalen gjennom den nye norske loven om kunstig intelligens (KI-loven). Den norske KI-loven vil i hovedsak vise til KI-forordningen, og utfylle forordningen der det er nasjonalt handlingsrom til å fastsette egne regler, blant annet ved å fastsette nasjonale myndigheters ansvar knyttet til tilsyn og håndhevelse. Regjeringen har utpekt Nkom som koordinerende markedstilsynsmyndighet, og de får ansvaret for å være felles kontaktpunkt («single point of contact») for KI-forordningen i Norge.

På Nkoms nye fagsider om KI og regulering av kunstig intelligens finnes utfyllende informasjon om KI-forordningen, herunder definisjonen av et KI-system, forpliktelsene og tilsynsstrukturen både nasjonalt og på EU-nivå. Informasjonen på fagsidene vil bli løpende oppdatert, og det er ventet at det kommer endringer i KI-forordningen som følge av EUs Digitale Omnibus.

Les mer på Nkoms fagsider om Kunstig intelligens (KI).

5.2 Risikobasert tilnærming til regulering av KI

KI-forordningen bygger på en risikobasert tilnærming hvor reguleringen differensieres etter hvilken risiko KI-systemet innebærer. Det stilles opp fire risikokategorier: uakseptabel risiko, høy risiko, begrenset risiko og minimal/ingen risiko.

1. **Systemer med uakseptabel risiko**
   Noen KI-systemer anses å utgjøre en uakseptabel risiko for menneskerettigheter, sikkerhet eller andre grunnleggende verdier, og er derfor forbudt å utvikle og bruke i EU/EØS. De forbudte KI-praksisene er listet opp i KI-forordningens artikkel 5. Begrunnelsen for disse forbudene er at skaden, og de etiske overtrampene ved å bruke disse KI-systemene, er så alvorlig at ingen risikoreduserende tiltak vil gjøre dem akseptable å bruke. Forbudene omfatter blant annet KI-systemer som manipulerer og bruker subliminale/villedende teknikker, utnyttelse av sårbare grupper, «social scoring», visse former for forutseende politivirksomhet, masseinnsamling av ansikter via «masseskraping», følelsesgjenkjenning på arbeidsplasser og skoler (med noen unntak), biometrisk kategorisering basert på sensitive forhold, og politiets bruk av biometriske fjernidentifisering i sanntid på offentlig sted (med noen unntak).

2. **Høyrisikosystemer**
   De fleste kravene og forpliktelsene i KI-forordningen gjelder KI-systemer som blir plassert i kategorien høyrisiko etter artikkel 6. Disse KI-systemene utgjør en høy risiko fordi feil, skjevheter eller misbruk kan få alvorlige konsekvenser for enkeltpersoners liv, helse eller grunnleggende rettigheter. KI-systemer med høy risiko er ikke forbudt i seg selv, men utvikling, omsetning og bruk er kun tillatt dersom KI-systemet oppfyller de strenge kravene i KI-forordningen. Her bygger KI-forordningen på de samme prinsippene som annet produktsikkerhetsregelverk, hvor hensikten er å sikre at de KI-systemene som kommer på markedet i EU/EØS er trygge å bruke.

   KI-systemer med høy risiko er plassert i to ulike vedlegg (I og III) til KI-forordningen, avhengig av om KI-systemet er integrert i et sikkerhetskritisk produkt, for eksempel maskiner, ekomutstyr eller leketøy (vedlegg I), eller om KI-systemet har bestemte bruksområder som angitt i vedlegg III. KI-systemene som er høyrisiko etter vedlegg III er «frittstående» i den forstand at de ikke er integrert i et fysisk produkt. Bruksområdene angitt i vedlegg III er:

   - Biometri
   - Kritisk infrastruktur
   - Utdanning og yrkesopplæring
   - Sysselsetting, arbeidsliv og tilgang til selvstendig næringsvirksomhet

- Essensielle private og offentlige tjenester og ytelser
- Rettshåndhevelse
- Migrasjon, asyl og grensekontroll
- Rettspleie og demokratiske prosesser

Det finnes imidlertid nyanser og unntak fra kategoriseringen som høyrisiko. Dersom et KI-system på listen i vedlegg III likevel ikke medfører en betydelig risiko for skade på fysiske personers helse, sikkerhet eller grunnleggende rettigheter, kan leverandøren argumentere for at KI-systemet ikke skal anses som høyrisiko etter KI-forordningen. I så fall må leverandøren dokumentere dette før KI-systemet lanseres på markedet.

3. **Systemer med begrenset risiko**
   Det neste nivået i «risikopyramiden» er KI-systemer med såkalt «begrenset risiko». Etter artikkel 50 pålegges leverandører og idriftsettere av slike KI-systemer særskilte krav til åpenhet og merking av KI-generert eller manipulert innhold. Dette er ikke en egen risikokategori, fordi reglene i artikkel 50 kan få anvendelse både på KI-systemer med høy risiko, og KI-systemer uten høy risiko. Bestemmelsen omfatter tre hovedtyper av KI-systemer:

   - KI-systemer som samhandler direkte med mennesker
   - KI-systemer for analyse av følelses eller biometrisk kategorisering
   - KI-generert eller manipulert innhold («deepfakes»)

4. **Systemer med minimal eller ingen risiko**
   Alle KI-systemer som ikke faller i noen av kategoriene over regnes som KI-systemer med minimal eller ingen risiko. For slike systemer stiller ikke KI-forordningen krav til verken tillatelser, samsvarsvurdering eller merking. Disse kan fritt utvikles og tas i bruk, så lenge det skjer i tråd med annet teknologinøytralt regelverk.

   Eksempler på KI-systemer med minimal eller ingen risiko kan for eksempel være KI-drevne stavekontroller, anbefalingsalgoritmer for musikk/film eller KI brukt i visse typer spill. Slike KI-systemer anses å ha så begrenset skadepotensial at spesifikk KI-regulering ikke er nødvendig. For mange virksomheter betyr dette at mange KI-verktøy de utvikler og tar i bruk ikke vil utløse juridiske plikter etter KI-forordningen. Alle bør likevel ha et bevisst forhold til etikk og mulige konsekvenser, og gjøre seg kjent med det som finnes av beste bransjepraksis.

5.3 Egne regler for de kraftigste KI-modellene

Disse store KI-modellene fungerer ofte som «råvaren» i ulike KI-systemer, fordi de er trent på bredt datagrunnlag og kan brukes til mange ulike oppgaver. KI-forordningen inneholder et eget regelsett for de kraftigste modellene, som kalles «KI-modeller for allmenne formål» («General-Purpose AI» eller «GPAI»). Disse reglene ble lagt til i KI-forordningen underveis i lovprosessen på EU-nivå, da lanseringen av ChatGPT i november 2022 bidro til at EU så et behov for å ha egne regler for de kraftigste KI-modellene. Disse reglene begynte å gjelde i EU fra 2. august 2025.

For norske virksomheter er det viktig å være klar over at selv om forpliktelsene i kapittel V i KI-forordningen retter seg mot leverandører av KI-modeller for allmenne formål (GPAI) kan også bruken av slike modeller utløse omfattende plikter. Dette gjelder blant annet dersom en virksomhet tar i bruk en KI-modell for allmenne formål og bygger denne inn i en egen løsning. Dersom virksomheten endrer KI-systemets tiltenkte formål på en slik måte at det klassifiseres som et høyrisiko KI-system anses virksomheten/aktøren som «leverandør av et KI-system». Dette innebærer at en virksomhet som i utgangspunktet kun er en bruker eller integrator av en KI-modell, likevel kan få fulle leverandørforpliktelser etter KI-forordningen. Norske virksomheter må derfor vurdere ikke bare hvilken KI-modell de bruker, men også hvordan og i hvilken kontekst den brukes. Det er særlig viktig å

være oppmerksom på om løsningen kan falle inn under høyrisikokategoriene, eller om bruken innebærer en endring av formålet som utløser strengere krav.

Selv der virksomheten ikke blir å anse som leverandør av et høyrisiko KI-system, kan bruken av KI-modeller for allmenne formål utløse andre plikter etter KI-forordningen. For leverandører av KI-systemer som genererer syntetisk tekst, bilde, lyd eller video, skal uttaket merkes slik at det kan identifisere som KI-generert eller -manipulert. I tillegg må idriftsettere opplyse om bruk av såkalte «deepfakes», med mindre det foreligger unntak, for eksempel av hensyn til ytringsfrihet eller kunstnerisk uttrykk. Disse kravene vil i mange tilfeller være direkte relevante for norske virksomheter som tar i bruk generative KI-løsninger i sine tjenester, markedsføring, kundedialog eller beslutningsstøtte.

Reglene om KI-modeller for allmenne formål erstatter ikke pliktene som gjelder for KI-systemer. Når en slik modell integreres i en konkret anvendelse eller tjeneste, vil den inngå som en del av et KI-system. En virksomhet som bygger en tjeneste på en slik modell, opptrer da som leverandør av et KI-system overfor sluttbrukere, og må forholde seg til regelverket basert på hvordan KI-systemet klassifiseres og brukes. Dette innebærer at virksomheten må vurdere om bruken er forbudt, om KI-systemet klassifiseres som høyrisiko, og om det gjelder krav til åpenhet og merking.

Håndhevingen av reglene for KI-modellene er i stor grad sentralisert til EU-organene. Kommisjonen har såkalte «enekompetanse» til å føre tilsyn med og håndheve reglene, og det er KI-kontoret (AI Office) hos Kommisjonen som skal utføre oppgavene.

5.4 Roller og aktører

KI-forordningen omfatter alle som utvikler, tilbyr eller bruker visse typer KI-systemer i EU/EØS, uavhengig av om virksomheten er etablert i EU/EØS eller ikke. Det betyr at også virksomheter utenfor EU, herunder USA og Kina, må følge regelverket dersom KI-systemene deres bringes inn på det europeiske markedet.

KI-forordningen er i stor grad utformet som et produktsikkerhetsregelverk der hovedansvaret ligger hos leverandøren. Det er leverandøren som skal sørge for at KI-systemet oppfyller kravene i KI-forordningen før det omsettes og tas i bruk. Samtidig pålegger KI-forordningen også forpliktelser på blant annet importører, distributører og idriftsettere av KI-systemer.

Leverandøren er den som utvikler, eller tar initiativ til å utvikle, et KI-system eller en KI-modell for allmenne formål under sitt eget navn eller varemerke. Leverandører omfatter både store teknologiselskaper som utvikler avanserte KI-modeller, og mindre selskaper som utarbeider smalere KI-løsninger. I noen tilfeller kan også de andre aktørene i KI-verdikjeden overta leverandøransvaret for et høyrisiko KI-system. En distributør, importør, idriftsetter eller annen tredjepart anses som leverandør dersom vedkommende:

a) setter sitt navn eller varemerke på et høyrisiko KI-system som allerede er brakt i omsetning eller tatt i bruk

b) foretar en vesentlig endring («substantial modification») av et slikt system slik at det fortsatt er høyrisiko etter artikkel 6

c) endrer systemets tiltenkte formål – herunder for et KI-system for allmenne formål – slik at det blir et høyrisiko KI-system

5.5 Krav og forpliktelser for høyrisiko KI-systemer

De mest omfattende kravene i KI-forordningen pålegges bruk eller omsetning av KI-systemer med høy risiko. Kravene til selve KI-systemet gjelder for hele livsløpet til KI-systemet, og omfatter risikohåndteringssystem, data og dataforvaltning, teknisk dokumentasjon, registrering og logging, åpenhet og formidling av opplysninger, menneskelig tilsyn, robusthet og cybersikkerhet.

Leverandører av KI-systemer med høy risiko skal sikre at deres KI-systemer oppfyller systemkravene. De skal også sikre at det gjennomføres en samsvarsvurdering før et høyrisiko KI-system slippes på markedet. Denne samsvarsvurderingen kan enten gjennomføres ved internkontroll eller med involvering av et meldt organ (et uavhengig teknisk kontrollorgan), avhengig av det aktuelle KI-systemet. Leverandøren skal også CE-merke KI-systemer med høy risiko. I tillegg gjelder det forpliktelser knyttet til overvåkning, rapportering og samarbeid med tilsynsmyndighetene.

Høyrisiko KI-systemer må behandles som et produkt som kan kontrolleres, ikke bare som en programvare som lanseres og «slippes fri». Leverandøren må etablere, dokumentere og vedlikeholde mekanismer som virker før KI-systemet bringes i omsetning og tas i bruk, og som fortsetter å fungere og oppdateres gjennom KI-systemets levetid.

5.6 Sanksjoner ved brudd på KI-forordningen

KI-forordningen innfører nye regler for hvordan kunstig intelligens skal utvikles og brukes i Europa, men for at reglene skal ha effekt innføres det også et sanksjonssystem. Samtidig gis det et nasjonalt handlingsrom til å bestemme hvordan sanksjonene skal være i den norske KI-loven.

KI-forordningen krever at landene fastsetter regler om sanksjoner og andre håndhevelsestiltak innenfor rammene av KI-forordningen. Sanksjonene skal stå i forhold til overtredelsen og virke avskrekkende, og samtidig skal det tas hensyn til virksomhetens størrelse, herunder oppstartsbedrifter.

Forordningen setter maksimumsnivåer for administrative overtredelsesgebyr for bestemte overtredelser, men overlater til landene å bestemme hvordan sanksjoner organiseres og håndheves innenfor disse rammene. Hvert land skal fastsette regler for i hvilken utstrekning overtredelsesgebyr kan ilegges sine egne offentlige myndigheter og organer.

Når det gjelder sanksjoner på EU-nivå er det EUs datatilsyn (European Data Protection Supervisor – EDPS) som kan ilegge administrative gebyrer, innenfor særskilte maksimalbeløp og prosessuelle garantier.

For leverandører av KI-modeller for allmenne formål kan Kommisjonen ilegge bøter ved bestemte brudd med en maksgrense på 3 % av global omsetning eller 15 millioner euro, der det høyeste beløpet gjelder.

5.7 Samspillet med annet regelverk

KI-forordningen må ses i sammenheng med annet relevant EU/EØS-regelverk på internett- og sikkerhetsområdet. For KI-systemer som inngår i produkter eller utstyr vil det være et samspill med regelverk som Cyber Resilience Act (CRA) og radioutstyrsdirektivet (RED), særlig når det gjelder krav til cybersikkerhet. Videre vil bruk av KI kunne inngå som en del av virksomheters samlede risikobilde etter NIS2-regelverket, og må håndteres innenfor kravene til sikkerhetsstyring og risikohåndtering.

KI-forordningen har også sammenheng med Digital Services Act (DSA), ettersom KI i økende grad benyttes i digitale tjenester og plattformer, blant annet i anbefalingssystemer og innholdsmoderering. I tillegg er tilgang til og bruk av data en grunnleggende forutsetning for utvikling og anvendelse av KI, noe som innebærer et nært samspill med Data Act. At Nkom har rolle som både DSA-koordinator og som myndighet etter KI-forordningen, gjør håndheving av regelverkene lettere.

6 Dataregulering

Dataforvaltningsforordningen (DGA) er foreslått innført i Norge som ny dataforvaltningslov. Lovproposisjon ble sendt til Stortinget våren 2026 og det er ikke besluttet hvem som får tilsynskompetanse etter den nye loven. Dataforordningen (Data Act/DA) er gjeldende i EU, og er nå til vurdering i EØS-EFTA-landene. DA er ment å bidra til datadeling mellom aktørene i det europeiske datamarkedet. Digital Omnibus ble lagt frem av Europakommisjonen 19. november 2025. Formålet med Digital Omnibus er å forenkle og samordne eksisterende digitale regelverk.

6.1 Bakgrunn: En europeisk strategi for data

Som en del av arbeidet i EU med å etablere et felles digitalt marked ble det i 2020 vedtatt en europeisk strategi for data[31]. I november 2025 kom «*Data Union Strategy*»[32] - med undertittel «*Unlocking data for AI*». Denne strategien har imidlertid et langt videre fokus enn KI alene, og innebærer – som Kommisjonen selv peker på i dokumentet – et vesentlig skifte i fokus fra 2020-strategien: Fokuset ble endret – *«fra regler til resultater».* Tiltak som uavhengige skytjenester får større fokus i lys av at data har blitt geopolitiske aktiva: «*Strengthening Europe's ability to collect, curate, and use its own data is both an economic and security imperative*."

Statsråd Karianne Tung deltok i lanseringen av selskapet Telenor Sovereign Cloud i mai 2026, og i pressemelding i denne sammenheng sa Tung: «*I en mer urolig verden er kontroll over egne data og digital infrastruktur avgjørende. Initiativ som dette bidrar til å styrke norsk digital suverenitet og beredskap og er helt i tråd med regjeringens plan for Norge.*»

EUs strategiske satsing på datapolitikk har kommet til uttrykk gjennom flere sentrale rettsakter, som skal tilrettelegge for mer digital autonomi i Europa, interoperabilitet, økt datadeling og viderebruk av data. Sentrale regulatoriske virkemidler er blant andre dataforvaltningsforordningen (Data Governance Act, DGA) og dataforordningen (Data Act, DA). Felles for regelverkene er at de har en nær sammenheng med elektronisk kommunikasjon, samt internett- og skyarkitektur. Nkom har over tid monitorert den dataregulatoriske utviklingen i EU og forberedt mulig tilsynskompetanse for de nevnte forordningen når de innføres i norsk rett.

DGA og DA behandles i det følgende under kapittel 6.2 og 6.3, før EUs foreslåtte forenklingspakke innen dataregulering *(Digital Omnibus)* beskrives i kapittel 6.4.

6.2 Dataforvaltningsforordningen

Dataforvaltningsforordningen (Data Governance Act/DGA) trådte i kraft i EU den 23. juni 2022 og har vært gjeldende fra 24. september 2023. DGA er innlemmet i EØS-avtalen og vil etter hvert gjennomføres i norsk rett. Lovproposisjon med forslag til ny dataforvaltningslov som vil gjennomføre DGA i norsk rett ble sendt til Stortinget i mars 2026.

Formålet med DGA er å styrke tilliten til datadeling og etablere mekanismer som gjør det lettere og sikrere å dele data. Forordningen retter seg særlig mot viderebruk av beskyttede data fra offentlig sektor, etablering av nye datadelingsaktører (såkalte dataformidlingstjenester) og tilrettelegging for frivillig deling av data til allmennyttige formål (såkalte dataaltruismeorganisasjoner). Forordningen skal dermed bidra til å øke tilgjengeligheten av data, samtidig som grunnleggende rettigheter, forretningshemmeligheter og personvern ivaretas.

[31] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066

[32] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0835

Reguleringen må ses i sammenheng med dataforordningen (DA), som beskrives i kapittel 6.3, samt øvrig digitalt regelverk som Digital Services Act (DSA) og Artificial Intelligence Act (AI Act). Videre fremgår det av forordningen at nasjonale myndigheter må utpeke kompetente tilsynsmyndigheter, blant annet for dataformidlingstjenester og dataaltruismeorganisasjoner. I høringen av forslag til ny dataforvaltningslov, som ble gjennomført i 2024, har Nkom anbefalt at dette tilsynet legges til Nkom, blant annet på grunn av vår fagkompetanse innen elektronisk kommunikasjon, data, og internettarkitektur. Per våren 2026 er det ikke besluttet hvilken myndighet som får tilsynskompetanse for disse tjenestene etter DGA.

6.3 Dataforordningen

Dataforordningen (Data Act/DA) er et sentralt element i EUs digitale strategi og utgjør en grunnpilar for utviklingen av et felles europeisk datamarked. DA trådte i kraft i EU 11. januar 2024, og har vært gjeldende fra 12. september 2025. Forordningen er til vurdering i EØS-EFTA-landene.

Forordningen er utformet for å styrke EUs dataøkonomi og fremme et konkurransedyktig datamarked ved å gjøre data (særlig industrielle data[33]) mer tilgjengelige og brukbare, oppmuntre til datadrevet innovasjon og øke datatilgangen. DA er ment å være et juridisk virkemiddel for å fremme datadeling mellom aktører i det europeiske datamarkedet.

Gjennomgående hensyn og prinsipp i reguleringen er åpenhet, dataportabilitet og interoperabilitet, hvilket også gjør at DA får en innholdsmessig sammenheng med Data Governance Act (DGA). Det europeiske datamarkedet må også forstås i tilknytning til markedet for internettbaserte tjenester og plattformer, som også vil bli påvirket av Digital Services Act (DSA), Digital Markets Act (DMA) og Artificial Intelligence Act (AI Act).

Innholdsmessig er rettsakten knyttet til hvem som kan nyttiggjøre seg data. Brukere av elektroniske kommunikasjonstjenester i EU genererer enorme mengder data. Særlig store dataplattformer kan oppnå fordeler gjennom datadrevne feedback loops[34] og nettverkseffekter. Tilgang til data anses for å være en avgjørende innsatsfaktor i utviklingen av fremtidens internettbaserte tjenester og plattformer. Enklere og bedre tilgang kan også gi større kundemobilitet, bedre regulering, samt oppdaterte, innovative og fremtidsrettede offentlige tjenester. Ifølge rapporten «*Market study on the Norwegian Data Economy*[35]» har særlig utviklingen innen kunstig intelligens økt oppmerksomheten knyttet til verdien av data hos norske aktører.

Ifølge DA skal tilsynsmyndighetene for bestemmelsene i DA om leverandørbytte for dataprosesseringstjenester (DPS) og interoperabilitet mellom DPS'er ha erfaring innenfor data og elektroniske kommunikasjonstjenester. Nkom forbereder derfor et mulig tilsynsansvar for disse og andre bestemmelser i DA. Samtidig arbeider Body of European Regulators for Electronic Communications (BEREC) med å få en rolle for å sikre en harmonisert implementering av delene av Data Act som er knyttet til DPS. Flere av regulatørene i BEREC har allerede utført betydelig arbeid knyttet til konkurranseforhold samt økonomiske og tekniske aspekter ved bestemmelsene knyttet til DPS. BEREC mener en slik rolle vil kunne bidra til effektivt samspill mellom Data Act og andre digitale EU-regelverk som Digital Markets Act og det foreslåtte Digital Networks Act.

6.4 Digital Omnibus

Digital Omnibus ble lagt frem av Europakommisjonen 19. november 2025. Med Digital Omnibus foreslår Kommisjonen å oppheve Data Governance Act (DGA), Free Flow of Non-Personal Data Regulation (FFDR), Open Data Directive (ODD) og Platform-to-Business Regulation (P2B). Viktige

[33] Dette gjelder særlig tilknyttede produkter som ofte betegnes som «Internet of Things» (IoT), samt tilhørende tjenester.

[34] En feedback loop på store internettplattformer oppstår når brukernes interaksjoner gir data som plattformen kan bruke til å tilpasse innholdet, noe som igjen påvirker brukernes atferd og genererer mer data. Dette kan skape en selvforsterkende syklus som former både brukeropplevelsen og plattformens innhold.

[35] https://nkom.no/aktuelt/nye-regler-gir-bedre-kontroll-og-konkurranse-i-datamarkedet

bestemmelser fra disse instrumentene er foreslått overført til blant annet Data Act (DA). Kommisjonen har foreslått en separat Omnibus for AI-forordningen (AI Omnibus).

Digital Omnibus er en forenklings- og konsolideringspakke for EUs digitale regelverk, der DA videreføres som «hovedstol» for store deler av EUs dataregelverk. Målet er å redusere overlapp, rapporteringsbyrde og uklarheter, samtidig som beskyttelsesnivået videreføres. Den digitale omnibusen foreslår også endringer i EUs regelverk for datalagring, deling og viderebruk.

Kommisjonens forslag innebærer endringer i følgende rettsakter[36]:

- Personvernforordningen (GDPR)
- Digital portal for informasjon om det indre markedet
- Kommunikasjonsverndirektivet
- Felles sikkerhetsnivå for digital sikkerhet (NIS2)
- Direktiv om kritiske enheters motstandsdyktighet
- Regulation (EU) 2018/1725

Forslaget innebærer også endringer i flere bestemmelser i DA, særlig de som gjelder:

- Forretningshemmeligheter i obligatorisk datautveksling for IoT mellom bedrifter (B2B) og mellom bedrifter og forbrukere (B2C)
- Obligatorisk datautveksling mellom virksomheter og offentlige myndigheter (B2G)
- Skifte av skytjenestetilbydere (cloud switching)

Data Act er ansett som EØS-relevant, mens Digital Omnibus ikke er markert som EØS-relevant av Kommisjonen p.t.

7 Antisvindelarbeid på internettområdet

Omfanget av digital svindel og svindelforsøk på internett er betydelig. Dette utfordrer tilliten til internett som tjeneste og samfunnskritisk infrastruktur og kan påføre enkeltmennesker og bedrifter store økonomisk tap. Redusert tillit til internett kan bremse digitaliseringen og digital inkludering i samfunnet. Nkom bidrar til å møte disse utfordringene blant annet gjennom sitt antisvindelarbeid og gjennom tilsyn med domenenavnsforvaltningen for .no

Nasjonal ekspertgruppe mot digital svindel består av offentlig og private aktører og ledes av Nkom i partnerskap med Økokrim. Gruppen har hatt fokus på tale og SMS, men fikk i desember 2025 fornyet mandat til også å se på svindel over internettbaserte tjenester.

7.1 Bakgrunn og omfang

Digital svindel er et samfunnsproblem som bidrar til å svekke tilliten til digital kommunikasjon, påfører enkeltmennesker økonomiske og følelsesmessige belastninger og samtidig understøtter internasjonal organisert kriminalitet.

Ifølge Finanstilsynet gikk om lag 1,2 milliarder kroner tapt til svindel i 2024. Samme år ble betydelige beløp, nesten 3 milliarder kroner, stanset av bankene som svindelforsøk. [37] Også globalt tapes store beløp til svindel. Global Anti-Scam Alliance gjennomførte i 2025 omfattende undersøkelser i 42 land og anslår at samlet tap her utgjorde 442 milliarder kroner på årsbasis.[38]

[36] Digitalpakke – Omnibus VII lagt frem av Kommisjonen - stortinget.no

[37] https://www.finanstilsynet.no/publikasjoner-og-analyser/svindel-og-svindelstatistikk/2025/h1/svindelstatistikk-forste-halvar-2025/#forhindret-svindel tabell nr. 12.

[38] https://gasa.org/knowledge-base/blog/gasa-policy-agenda-2026

Svindel foregår over de fleste digitale kanaler og internettbaserte plattformer. Nkom har, gjennom undersøkelser foretatt av Respons Analyse, registrert en nedgang i tradisjonelle telefonsvindelforsøk over telefoni og SMS fra 2024 til 2025.[39] Samtidig skjer svindel over en rekke internettbaserte kanaler og plattformer, som e-post, sosiale medier, nettbutikker og ulike tale- og meldingstjenester og gjennom kombinasjoner av disse. Svindelmetoder og moduser er i konstant utvikling.

Svindel kan ramme alle. En undersøkelse gjennomført av Ipsos på vegne av Nkom i november 2025 viste at eldre oftere opplever svindelforsøk via telefonsamtaler, og yngre via internettbaserte plattformer som sosiale medier og spill. De med særlig høy skjermtid var også mer utsatt for svindel. Undersøkelsen viste videre at e-post er den kanalen hvor flest blir utsatt for svindelforsøk, men at sosiale medier, falske nettbutikker og dating-apper peker seg ut som scenarioer med forhøyet risiko for gjennomført svindel. Det betyr at svindel- trusselen er situasjonsbestemt og at tiltak inn mot internettområdet blir viktig fremover.

Svindlerne kan være store profesjonelle internasjonale kriminelle nettverk med avanserte «scam-centers» i ryggen, men kan også være mindre, regionale eller enkeltstående aktører. Internasjonale svindlerne har også benyttet medhjelpere i Norge for å få tilgang til informasjon, bankkonto eller SIM-kort.

Det foreligger ingen samlet oversikt over omfanget av svindel på «internettområdet». Telenor har imidlertid anslått at 70 prosent av nye hjemmesider er svindel.[40] Selskapet opplyser at de i 2025 foretok 2,1 milliarder blokkeringer på nett knyttet til digital kriminalitet.[41] Ulike plattformer og tjenester kan ved offentlige uttalelser og rapporter gi innsyn i svindelomfanget. For eksempel opplyser Google at de i 2024 daglig blokkerte «hundrevis av millioner» av skadelige eller svindelrelaterte søkeresultater.[42]

Inn i denne virkeligheten ser vi at bruken av kunstig intelligens har gjort enkelte svindelmetoder mer sofistikerte og troverdige, blant annet gjennom deepfake-teknologi for video og tale, tilpassede og feilfrie tekster eller misbruk av informasjon hentet fra sosiale medier. Interpol anslår at KI-generert svindel er 4,5 ganger mer profitabel enn tradisjonelle metoder.[43]

Det er en risiko for at omfanget av KI-assistert svindel over internettbaserte tjenester vil øke. Samtidig brukes også KI aktivt til bekjempelse av svindel.

Tapsbeløp, kanaler, metoder, omfang, aktørbildet og teknologisk utvikling er faktorer som understreker behovet for en økt internasjonal og nasjonal innsats mot samfunnsproblemet som digital svindel utgjør.

7.2 Internasjonale aktører og EU har økt fokus på digital svindel

Både Interpol, Europol, UNODC, EU, CEPT og andre internasjonale aktører har i de siste årene hatt økt fokus på den globale utfordringen som digital svindel utgjør. 16.-17. mars 2026 arrangerte UNODC og Interpol en første Global Fraud Summit i Wien. 1400 representanter fra relevante aktører deltok. Møtet resulterte i "*Call to action on combating Fraud*" og et "*Global Public-Private Partnership Framework against Fraud*".[44]

[39] https://nkom.no/aktuelt/nedgang-i-tradisjonell-telefonsvindel

[40] https://www.telenor.no/online/sikkerhet/nettvern/nettvern-pluss-stopper-alle-nye-svindelsider/

[41] https://www.telenor.no/om/sikkerhet/sikkerhetspuls_aarsrapport2025/

[42] https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Search-Scam-Report-0508.pdf

[43] https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat

[44] https://www.unodc.org/unodc/en/organized-crime/global-fraud-summit/

Bransjeorganisasjoner som blant annet GSMA, i3Forum, One Consortium, Mobile Ecosystem Forum, Global Anti-Scam Alliance og Communications Fraud Control Association deltar aktivt i internasjonal dialog om utfordringene som digital svindel representerer.

I den foreslåtte Digital Networks Act artikkel 103 er det foreslått en plikt for ISP-er og tilbydere av person-til-person-kommunikasjonstjeneste å samarbeide med myndigheter om å finne effektive måter å forhindre svindel. Det er også foreslått at BEREC skal utgi veiledning om tekniske og rettslige tiltak som kan beskytte sluttbrukere mot svindel. Videre er det foreslått en selvstendig plikt for kompetente myndigheter til å innføre tiltak mot svindel og en åpning for Europakommisjonen å vedta delegerte rettsakter. Dette vil kunne styrke Europas samlede forsvarsevne mot digital svindel.

Nkom bidrar aktivt i det internasjonale arbeidet. Særlig gjelder dette gjennom arbeidsgruppe for Numbering and Networks i CEPT og gjennom arbeidsgrupper i BEREC. Nkom leder også et globalt initiativ, «*Global Informal Regulatory Antifraud Forum*» (GIRAF), som har egen undergruppe om svindel via internettbaserte tjenester, som for eksempel sosiale medier, ledet av den irske regulatøren ComReg. GIRAF er imidlertid et 2-årig prosjekt som utløper juni 2026, med mindre et tilstrekkelig antall regulatører ønsker å forlenge initiativet.

7.3 Den nasjonale innsatsen mot digital svindel på internett

I Nasjonal digitaliseringsstrategi 2024-2030[45] fastsettes videreutvikling av tverrfaglig samarbeid og informasjon til innbyggerne som et tiltak frem mot 2030 for å hindre digital svindel. Videre må innbyggerne bli mer motstandsdyktige mot svindel gjennom å øke kunnskapen om vanlige svindelmetoder og hvordan man ferdes sikkert på nettet. Nkoms visjon er å sikre en trygg og tilgjengelig digital hverdag for alle, og Nkom skal være en pådriver for et trygt internett. Nkoms antisvindelarbeid på internettområdet er en naturlig operasjonalisering av de strategiske føringene.

Innsatsen mot svindel på internett består av et sammensatt økosystem av aktører og virkemidler. Politi, finans, ekom, forbruker og sikkerhetsmyndigheter er blant aktørene som bidrar aktivt innenfor egen sektor. Samarbeid på tvers blir imidlertid stadig viktigere fremover.

Det finnes flere relevante regelverk mot digital svindel, blant annet regelverk om ekom (inkludert nettnøytralitetsforordningen), personvern, KI, markedsføring, domenenavn, straff og finans. Nkoms Prinsippnotat om DNS-baserte sikkerhetstiltak[46] er også relevant. Når DSA og tilhørende tilsynsstruktur (jf. kapittel 4) implementeres i norsk rett, vil også dette være et og sentralt virkemiddel som legger føringer for hvilke tiltak som forventes iverksatt av blant annet globale plattformer. Svindelbasert innhold vil typisk kunne anses som «ulovlig innhold» etter DSA, noe som kan få betydning for blant annet risikovurderinger, transparensforpliktelser, varslingsmekanismer og rapportering.

Norid forvalter det norske landkodetoppdomenet .no og har etablert rutiner og regler for registrering av domenenavn. Dette har medført at .no har etablert seg som et «godt nabolag» på internett, med et begrenset svindelomfang sammenliknet med andre toppdomener. Selv om svindel også forekommer under .no er det generelle bildet positivt. Dette understøttes av at .no rangeres av Global Signal Exchange på topp av toppnivåkodene i verden med færrest rapporter om misbruk.[47]

Norid opererer etter rammer fastsatt i ekomloven og domeneforskriften. Norid fastsetter tildelingsregler innenfor rammen av forskriften. Nkom fører tilsyn med at bestemmelsene i forskriften overholdes. Norske domenenavn vil kunne beslaglegges av politiet etter straffeprosessuelle.

[45] https://www.regjeringen.no/contentassets/c499c3b6c93740bd989c43d886f65924/no/pdfs/nasjonal-digitaliseringsstrategi_ny.pdf s. 32

[46] https://nkom.no/internett/nettnoytralitet/nettnoytralitet-og-sikkerhet

[47] https://www.globalsignalexchange.org/leaguetables/tld

Finans Norge er næringsorganisasjonen for finansnæringen i Norge og representerer rundt 315 finansbedrifter. Finans Norge arbeider aktivt mot svindel og har blant annet opprettet et eget fagutvalg antisvindel bank (FAB), etablert informasjonssiden svindel.no og har gitt råd om 16 tiltak mot svindel.[48]

Politiet etablerte i 2025 en løsning for digital anmeldelse av svindel og bedrageri. Dette kan gi en bedre situasjonsforståelse og oversikt over omfang og utvikling.

Nkom har - og vil fortsette med - et aktivt informasjonsarbeid i ulike kanaler. Dette for å øke befolkningens evne til selvforsvar mot digital svindel. Informasjon og kunnskapsdeling, som er sentralt i samfunnets kamp mot svindel på internettområdet, gjøres også av flere andre offentlige og private aktører. Blant annet gir Forbrukerrådet og Forbrukertilsynet råd og veiledning på sine hjemmesider om hvordan man unngår nettsvindel. Råd og veiledning om digital sikkerhet gis også på nettsiden www.sikkert.no, som er en nasjonal portal utviklet gjennom et samarbeid mellom Nasjonal sikkerhetsmyndighet, Digitaliseringsdirektoratet, Politiet og Datatilsynet. Flere ekomtilbydere har et aktivt informasjonsarbeid rettet mot forbrukere. Næringslivets sikkerhetsråd har særlig fokus inn mot næringslivet og har blant annet etablert et eget Cybersikkerhetssenter.

Samarbeid og informasjonsdeling blir stadig viktigere. Flere positive samarbeidsinitiativ er allerede igangsatt, både internasjonalt og nasjonalt. Blant annet arrangerte regjeringen ved DFD 18. mars 2026 et eget høynivåmøte mellom sentrale aktører om hvordan svindel på nett kan forebygges og bekjempes bedre.[49]

Nasjonal ekspertgruppe mot digital svindel ble etablert av Nkom i 2023 i partnerskap med Økokrim. Gruppen består av aktører fra offentlig og privat sektor, herunder Telenor, Telia, Ice/Lyse, NRDB, NSM, NSR, Finans Norge, DigDir, Finanstilsynet og Stø AS. Nkom leder gruppen, som i desember 2025 fikk fornyet og utvidet mandat for to nye år. Gruppen skal også se på svindel over internettbaserte tjenester og sårbarheter og tiltak i grensefeltet bank og ekom. Mandatet fastsetter også at dersom gruppen ikke har konkret løsningseierskap blant deltakerne, kan gruppen som en nasjonal ressurs bidra med å formulere problembeskrivelser som bringes inn for relevante nasjonale eller internasjonale aktører.

Politiet ved Kripos uttaler i Cyberkriminalitet 2025[50]:

> *Det er meget sannsynlig at kriminelle vil fortsette å utnytte avstanden mellom rask teknologisk utvikling og samfunnets tregere evne til å utvikle effektive mottiltak.*

I lys av dette vil felles situasjonsforståelse, samarbeid, datadeling og regelverksutvikling mv. være viktige suksesskriterier for antisvindelarbeid på internettområdet.

Fremover vil en effektiv bekjempelse av digital svindel i stadig større grad forutsette samarbeid på tvers av sektorer, og vil kunne berøre aktører som internettilbydere, domenenavnforvaltning, internettbaserte plattformer, banker, betalingsformidlere, ekomaktører, samt Nkom og politi.

[48] https://www.finansnorge.no/tema/okonomisk-kriminalitet/svindel/status-og-tiltak-mot-svindel-for-2026/#part0

[49] https://www.regjeringen.no/no/aktuelt/samler-sentrale-aktorer-for-a-bekjempe-nettsvindel-vi-ma-stoppe-svindelen-der-den-skjer/id3152202/

[50] Cyberkriminalitet 2025 - Kripos

8 Internasjonal internettforvaltning

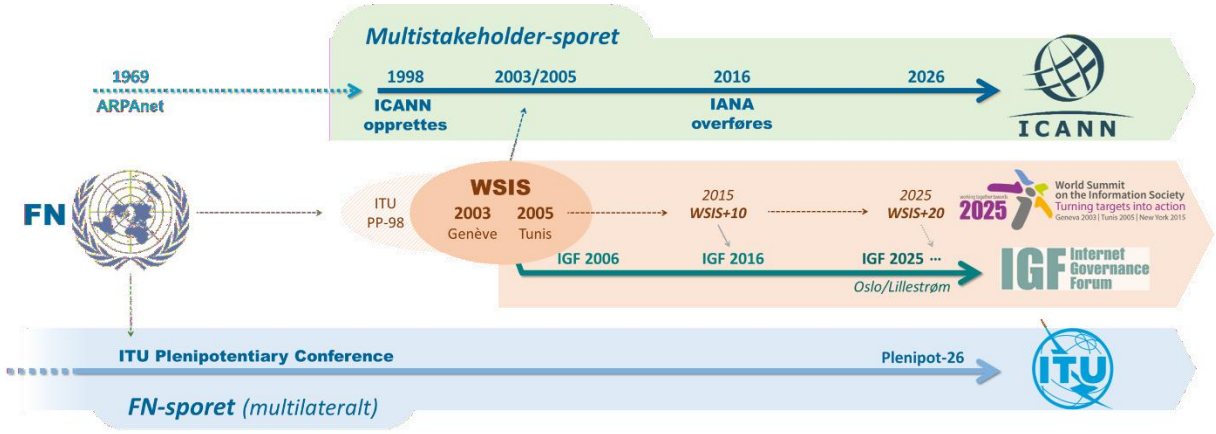
Internasjonal internettforvaltning har ved overgangen fra 2025 til 2026 passert en viktig milepæl. Norge var arrangør for det 20. årlige internasjonale møtet innen internettforvaltning i juni 2025 (IGF 2025), og FN vedtok på generalforsamlingen i desember 2025 å videreføre det internasjonale samarbeidet innen internettforvaltning (WSIS+20).

I 2026 vil to parallelle prosesser innen internasjonal internettforvaltning bidra til videreutvikling av fagområdet. Ved utgangen av april åpnet en ny søkerunde for generiske toppdomener innen DNS, organisert av forvaltningsorganet ICANN. Og i oktober gjennomføres fullmaktskonferansen til FN-organisasjonen ITU med sentrale internettema på agendaen.

8.1 Bakgrunn

Internettforvaltning («internet governance») er et fagområde som omfatter etablering og anvendelse av prinsipper, normer, regler og beslutningsprosedyrer som er med på å forme utviklingen og bruken av internett. Den internasjonale internettforvaltningen følger flere parallelle spor. Dette har konsekvenser for hvordan myndigheter og andre aktørgrupper («stakeholder groups») kan engasjere seg innen fagområdet, og det påvirker hvordan internett spiller en sentral rolle innen geopolitisk utvikling.

Nkom bistår DFD med Norges deltakelse innen internasjonal internettforvaltning gjennom organisasjoner som ITU og ICANN for å ivareta norske interesser. 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*.»[51]



Figur 17 - Internettforvaltning utspiller seg langs parallelle spor, henholdsvis multistakeholder-sporet og det multilaterale FN-sporet

På den ene siden kan internett betraktes som et elektronisk kommunikasjonsnett (ekomnett) på linje med andre mer tradisjonelle telekommunikasjonsnett. Dette er bakgrunnen for FN-sporet innen internettforvaltning, som baserer seg på en ***multilateral forvaltningsmodell***. Tilbake i tid har etablering av ekominfrastruktur vært en oppgave for nasjonale myndigheter, som organiserte det internasjonale samarbeidet innen FN-organet ITU (International Telecommunication Union). Etter hvert som internetteknologien gradvis er tatt i bruk for ekomtjenester, har forvaltningen av internett blitt et sentralt tema for ITU.

[51] Stortingsmelding 28 (2020-2021), https://www.regjeringen.no/no/dokumenter/meld.-st.-28-20202021/id2842784/

På den annen side har internett sitt opphav som et forskningsnettverk etablert av amerikanske myndigheter. Etter hvert som nettverket vokste både i USA og internasjonalt, ble forvaltningen av internett organisert av amerikanske institusjoner. Da internett på 1990-tallet vokste til et verdensomspennende kommunikasjonsnett, økte behovet for å internasjonalisere forvaltningen av nettet. Gjennom en omfattende prosess over flere år, ble forvaltningen av internett i 2016 formelt overført fra USA til den internasjonale organisasjonen ICANN (Internet Corporation for Assigned Names and Numbers).

En viktig forutsetning for internasjonaliseringen av ICANN var organisasjonens vedtekter som skal sikre at den opererer basert på «***multistakeholder model***» (flerpartsmodellen). Dette er bakgrunnen for multistakeholder-sporet innen internettforvaltning (jf. figuren over). Myndigheter, privat sektor, sivilsamfunnet, teknisk sektor og akademia er sentrale aktørgrupper i modellen. Oppsummert kan man anse FN-sporet for å omfatte den kontinuerlige utviklingen innen tradisjonell ekom som har pågått i 150 år, mens multistakeholder-sporet fokuserer på den disruptive utviklingen som internett har utgjort innen ekom de senere tiårene.

Internasjonal internettforvaltning ble befestet i disse to sporene gjennom FN-prosessen WSIS («*World Summit on the Information Society*"). Det ble avholdt to WSIS-møter i 2003 og 2005, og sluttkommunikéet fra WSIS 2005 («Tunis Agenda») representerer et basisdokument for arbeidet med internettforvaltning. Et viktig resultat fra WSIS-prosessen er opprettelsen av IGF (Internet Governance Forum) som kan ses på som et «mellomliggende spor» som både er knyttet til FN (sammen med ITU), men som baserer seg på multistakeholdermodellen (som ICANN).

I spenningsfeltet mellom det tradisjonelle multilaterale FN-sporet rundt ITU og det nyere multistakeholdersporet rundt ICANN utspiller det seg sentrale geopolitiske prosesser som drøftes i de følgende delkapitlene.

8.2 IGF 2025 i Norge

Én gang i året samles deltakere fra alle verdens hjørner til IGF-møte. Dette har pågått siden det første IGF-møtet som ble arrangert i Aten i 2006. Norge var vertsland for IGF 2025 på Lillestrøm.[52] Dette var det tjuende IGF-møtet i rekken. IGF er et globalt forum for dialog om forvaltningen av internett som har sitt mandat i «Tunis Agenda». På de årlige møtene settes sentrale saker knyttet til nye teknologier og kritisk infrastruktur på agendaen. Deltakerne bidrar til informasjonsdeling og kompetansebygging på tvers av de ulike samfunnssektorene. IGF etablerer anbefalinger, men vedtar ikke bindende beslutninger for deltakerne.

Norges kandidatur som arrangørland for IGF ble annonsert med følgende ord av utenriksminister Espen Barth Eide: «*Et fritt og åpent internett er grunnleggende for demokrati, menneskerettigheter og ytringsfrihet. Internasjonalt samarbeid for å sikre at internett forblir en trygg og inkluderende arena for alle, er viktigere nå enn noensinne. Dette ønsker Norge å bidra til».* Videre beskriver nasjonal digitaliseringsstrategi at Norge «*tar et større ansvar i den videre utviklingen av internett. Norge skal bidra til å sikre langsiktige strategiske interesser i den globale internettforvaltningen og sette dagsordenen i spørsmål av stor betydning*.»

Gjennomføringen av IGF 2025 i Norge hadde bred støtte. FNs generalsekretær Antonio Guterres uttrykte at «*Jeg er glad for å delta i årets IGF – og takk til Norge for å være vertskap. I år har forumet arbeidet med å fremme inkluderende samarbeid om internettpolitikk i tjue år*.» Statsminister Jonas Gahr Støre formulerte det slik: «*Teknologien må gå hånd i hånd med et menneskelig preg. Jeg tviler ikke på at denne konferansen vil gi verdifull innsikt, forslag og anbefalinger som kan veilede internettpolitikk og -praksis til fordel for alle*.»

Temaene som tas opp på IGF-møtene spenner over et bredt spektrum. Internetts økosystem er et samspill mellom internetts infrastruktur for kommunikasjon (ofte omtalt som «nettverkslaget» eller

[52] Internet Governance Forum 2025, https://www.intgovforum.org/en/dashboard/igf-2025

«teknisk lag»), og innhold og tjenester som formidles over denne infrastrukturen (ofte omtalt som «applikasjonslaget»). Aktuelle tema omfatter blant annet domenenavnsystemet, internettsikkerhet, nettnøytralitet, dataforvaltning, plattformenes rolle, kunstig intelligens, faren for internettfragmentering, demokrati og ytringsfrihet.

Én av sesjonene som ble arrangert av Nkom ved IGF 2025 var «*Building trust and combatting fraud in the internet ecosystem*».[53] Sesjonen analyserte hvordan man kan opprettholde tilliten til internettkommunikasjon og innhold som formidles via internett i en situasjon der en fjerdedel av verdens befolkning har tapt penger på grunn av svindel. Mange av svindelforsøkene innebærer sosial manipulasjon, phishing og identitetstyveri. Tiltak for å motvirke dette spenner fra å etablere regelverk og institusjoner som kan beskytte oss, til å utdanne innbyggere til å bli mer motstandsdyktige mot svindel ved å øke kunnskapen om hvordan man kan være trygg på nettet.

IGF 2025 fungerte som et ledd i forberedelsen til WSIS+20 senere på året, med drøftinger knyttet til flerpartsmodellen. Sesjonen «*Multistakeholder Perspectives: WSIS+20 & the Technical Layer*»[54] drøftet betydningen av flerpartsmodellen for å opprettholde et sikkert, stabilt og åpent internett. Modellen tilrettelegger for at ulike aktører, som teknisk miljø, myndigheter, sivilsamfunn og privat sektor kan samarbeide som likemenn. Både den norske representanten og flere andre av paneldeltakerne understreket betydningen av at beslutninger knyttet til internettforvaltning tas basert på forståelse av de tekniske implikasjonene for internetts arkitektur. Det er avgjørende å unngå fragmentering og sentralisert kontroll for å bevare internetts globale, åpne arkitektur.[55]

På høynivå-sesjonen «*Charting the Path Forward for the WSIS+20 Review and Role of the IGF*» på avslutningsdagen oppsummerte digitaliseringsminister Karianne Tung med disse ordene: «*Jeg tror at vi i løpet av de siste tjue årene har vist at man kan stole på IGF og flerpartsmodellen. Derfor er det viktig for Norge, ja det er Norges synspunkt at IGF bør få et styrket mandat, at forumet bør bli permanent, og at vi blir i stand til å integrere de ulike prosessene bedre.*»

8.3 WSIS – 20 års milepæl passert

IGF ble etablert som en internasjonal møteplass for internettforvaltning gjennom en omfattende prosess på WSIS-møtene i Genève i 2003 og Tunis i 2005. I Tunis var et sentralt diskusjonspunkt hvilken rolle ICANN skulle ha fremover, som global koordinator for tildeling av domenenavn og IP-adresser. På dette tidspunktet var ICANN forvaltet av amerikanske myndigheter, men med målsetning om å internasjonalisere organisasjonen.

Ved inngangen til WSIS-forhandlingene ved 20-årsjubilieet i 2025, var det knyttet stor spenning til hvilken vei utviklingen innen internettforvaltning ville gå. Den geopolitiske diskusjonen som startet i 2003/2005 og som har vart frem til i dag, hadde vist at etablering av en åpen flerpartstilnærming til internettforvaltning fordrer en aktiv innsats fra de ulike partene som bidrar til utformingen av internetts fremtid.

På Tunis-møtet tilbake i 2005 talte noen land for at koordineringsfunksjoner for internett burde organiseres under multilateral myndighetsstyring og plasseres hos ITU. Andre land, samt grupperingen innen sivilsamfunnet, teknisk sektor og akademia, advarte derimot om at større statlig kontroll kunne true internetts åpenhet, samtidig som de erkjente begrensningene i ICANNs eksisterende forvaltnings-struktur. Videre uttrykte forsvarere av menneskerettighetene bekymring for at forvaltning via et multilateralt organ kunne begrense ytringsfriheten.

Det viste seg vanskelig å oppnå enighet om en løsning på denne uenigheten, og spørsmålet ble ikke besvart i sluttresolusjonen «Tunis Agenda».[56] Dette medførte at ICANNs rolle forble uendret gjennom

[53] Building trust and combatting fraud in the internet ecosystem, IGF 2025 Day 0 Event #250

[54] Multistakeholder Perspectives: WSIS+20 & the Technical Layer, IGF 2025 Workshop #344

[55] Digital Watch Observatory by Geneva Internet Platform, IGF 2025 WS #344 Session report

[56] Tunis Agenda for the Information Society, https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

denne WSIS-prosessen, og parallelle spor for internasjonal internettforvaltning ble opprettholdt. En annen side ved kompromisset var at IGF ble opprette som en global plattform for dialog om internettforvaltning. I sluttkommunikéet ble IGF gitt et tidsbegrenset mandat. Og i 2015 ble mandatet forlenget med ti nye år (WSIS+10).

WSIS+20-forhandlingene startet juni 2025, og etter seks måneder ble konsensus oppnådd. Sluttresolusjonen[57] inneholder flere momenter som gjenspeiler den opprinnelige visjonen WSIS. Paragraf 1 refererer til folkeretten og menneskerettighetene, paragraf 2 bekrefter Tunis Agenda og paragraf 3 anerkjenner flerpartsmodellen som sentral for utviklingen av informasjonssamfunnet. Når det gjelder det tilbakevendende spørsmålet om forlengelse av IGF-mandatet, ble det imidlertid gjort vesentlig fremskritt ved at IGF ble gitt et permanent mandat.

I pressemeldingen[58] fra Digitaliseringsdepartementet heter det at «*Generalforsamlingen i FN kom til enighet om en felles slutterklæring og et permanent mandat for IGF – FNs ledende møteplass for dialog mellom alle relevante parter om fremtidens internett. Dette ble bestemt på et toppmøte i New York, der Norge var ett av landende som støttet opp om at internett fortsatt skal være demokratisk, fritt og åpent for alle*.»

Hvordan IGF skal finansieres fremover er derimot ikke løst, men FNs generalsekretær skal legge frem et forslag for FNs generalforsamling for å sikre en bærekraftig finansiering for forumet. Videre er det en uløst problemstilling at selv om flerpartsmodellen er befestet, ser noen land fortsatt for seg en sterkere rolle for myndighetene innenfor flerpartsmodellen («top-down»), mens andre land mener myndigheten skal ha en likeverdig rolle med de andre partene innen flerpartsmodellen («bottom-up»).

Siste ord er nok ikke sagt i debatten om multilateralisme og «multistakeholderism». Dette gjenspeiler seg fortsatt i måten prosessen rundt WSIS utspiller seg innen FN. Relativt langt utover i prosessen er det en reell flerpartsprosess, hvor myndighetene arbeider sammen med privat sektor, sivilsamfunnet, teknisk sektor og akademia i en åpen dialog. Men når prosessen går inn i siste fase, er forhandlingene en lukket FN-prosess hvor myndighetene forhandler multilateralt seg imellom.

8.4 ICANN starter søkerunde for nye toppdomener

Internetts globale kommunikasjonstjeneste forutsetter koordinering av internetts kjernefunksjoner, som adressering og ruting av nettverkstrafikk samt navnetjenesten til domenenavnsystemet (DNS). ICANNs rolle er å opprettholde et konsistent og stabilt sett med globalt unike identifikatorer (domenenavn og IP-adresser) som gjør det mulig å kommunisere på tvers av de ulike nettverkene som internett består av. Denne delen av internettforvaltningen omtales av og til som «teknisk internettforvaltning».

ICANN er, som beskrevet over, basert på flerpartsmodellen. Ved en eventuell svekkelse av flerpartsmodellen risikerer man å sette det tekniske miljøet på sidelinjen og introdusere geopolitisk innflytelse i beslutningstakingen som vil kunne overstyre opprettholdelsen av et åpent og interoperabelt internett. I denne sammenheng har ICANN en særlig viktig funksjon.

ICANN har utviklet seg siden opprettelsen i 1998. I flere år var det uenighet mellom ulike land om rollen til ICANN. I 2016 ble imidlertid den formelle statusen for ICANN endret ved at amerikanske myndigheter sa fra seg sin tilsynsrolle og overførte denne til det internasjonale flerpartsfellesskapet gjennom en avtale med ICANN. En viktig side ved endringen var overføringen av «IANA-funksjonen». IANA-funksjonen (Internet Assigned Numbers Authority) håndterer registeret over domenenavn, IP-adresser og andre identifikatorer som brukes på internett.

[57] Resolution adopted by the General Assembly on 17 December 2025, United Nations, A/RES/80/17

[58] Bred enighet i FN om forvaltning av fremtidens internett, DFD, 19. desember 2025, pressemelding

I 2026 vil det være søkerunden for nye generiske toppdomener[59] som står øverst på agendaen hos ICANN. Dette er andre gang i historien at en slik søkerunde gjennomføres. Første søkerunde var i 2012, noe som førte til en markant økning i antall toppdomener etter at over tusen søknader ble mottatt den gangen. Søknadsprosessen vil være åpen fra 30. april til 12. august i år. Deretter vil domenenavnene det søkes om offentliggjøres i oktober («Reveal Day»). Etter en periode med mulighet for å justere domenenavnene, vil den endelige listen over søkte toppdomener publiseres i november («Confirmation Day»).

Deretter starter en omfattende prosess innen ICANN som forventes å vare i flere år fremover, på liknende måte som ved 2012-runden. Innen ICANN er offentlige myndigheter organisert i undergruppen GAC (Governmental Advisory Committee), og GAC kan komme til å spille en sentral rolle gjennom søkerunden. Enkeltmedlemmer innen GAC vil kunne inngi protester mot søknader på toppdomener i form av «GAC early warnings», og GAC i fellesskap vil kunne gjøre det i form av «GAC consensus advice». Disse protestene vil videre gjennomgå ulike formelle prosesser innen ICANN hvor de til sist kan bli avvist eller tatt til følge.

En annen sak som har pågått i lengre tid innen ICANN, er tilpasning av WHOIS til GDPR og andre personvernregelverk[60]. WHOIS er en global, distribuert database som inneholder informasjon som innehavere av domenenavn, og disse dataene var opprinnelig åpent tilgjengelige. Registeret er blant annet et viktig verktøy for bekjempelse av kriminalitet. I mai 2018 trådte GDPR i kraft, og dette ansporet en prosess innen ICANN for å bringe WHOIS i overenstemmelse med reglene for personvern. En del WHOIS-data ble nå skjult for allmenheten, og en prøvetjeneste for legitim spørring etter skjermede registreringsdata er etablert, for eksempel for politimyndighetene.

En relativt ny sak innen ICANN er «Review of Reviews» som er knyttet til beskyttelsen av flerpartsmodellen innen organisasjonen. ICANNs vedtekter inneholder bestemmelser om en rekke revisjoner som jevnlig skal gjennomføres for å kontrollere at organisasjonen opererer i overensstemmelse med målsetningen. De senere årene har det imidlertid vist seg at man er kommet på etterskudd i dette arbeidet, hvor nye revisjonsrunder starter før forrige runde er fullført. ICANN undersøker derfor muligheten for å justere revisjonssystemet på en måte som gjør dette mer gjennomførbart, men uten å gå på bekostning av formålet med revisjonene.

8.5 ITU på vei mot Plenipot 26

Tradisjonell telekommunikasjon eksisterte lenge før internett, og internasjonal forvaltning av telekom har vært organisert innen FN-organet ITU. Etter hvert som internett gradvis har overtatt som samfunnets viktigste kommunikasjonstjeneste, har ITU økt sin aktivitet knyttet til internett. Fullmaktskonferansen (Plenipotentiary Conference, ofte omtalt som «Plenipot») er ITUs høyeste organ. Plenipot avholdes hvert fjerde år og skal neste gang arrangeres 9.-27. november i år.[61]

Diskusjonen om rollen til det multilaterale FN-sporet som ITU representerer, kontra multistakeholdersporet hvor ICANN befinner seg, dukker av og til opp på møtene innen ITU, under navnet «New IP». Det mest markante eksemplet på denne diskusjonen fant sted i 2019 da kinesiske delegater til ITU foreslo å etablere en alternativ standardisering av IP-teknologien som brukes på internett, innen ITU. Så lenge internett har eksistert, har standardisering av IP-teknologien derimot vært utført innen IETF (Internet Engineering Task Force) som er basert på multistakeholdermodellen.

En rapport utarbeidet for Europaparlamentet[62] forklarer at ifølge kineserne «er ikke nåværende IP-design effektiv nok til å støtte teknologier som holografisk kommunikasjon eller selvkjørende biler.» Videre beskriver rapporten at «*det kinesiske forslaget skapte blandede reaksjoner fra det*

[59] The New Generic Top-Level Domains (gTLD) Program «2026 Round», ICANN, https://newgtldprogram.icann.org/en

[60] Data Protection and Privacy, Policy Development Overview, ICANN, https://www.icann.org/dataprotectionprivacy

[61] ITU Plenipotentiary Conference 2026 (Plenipot 26), https://pp.itu.int/2026/en/

[62] «Internet governance», Briefing European Parliamentary Research Service, September 2024

internasjonale samfunnet. Iran, Russland, Saudi-Arabia og flere afrikanske land støttet forslaget, mens vestlige land som USA, Storbritannia, EU og sivilsamfunnet uttrykte bekymring for dem.»

Etter intens debatt, fikk imidlertid det kinesiske forslaget ikke tilstrekkelig støtte. Men den underliggende strømningen om å forflytte tyngdepunktet for internettforvaltning og standardisering inn under ITU-paraplyen er ikke borte. Også i 2022 ble det presentert et liknende forslag fra kineserne, denne gangen under betegnelsen «IPv6+». IETF utfører allerede standardiseringsarbeid som kontinuerlig videreutvikler IP-teknologien, inklusive tilsvarende designbehov som «New IP».[63]

En eventuell oppsplitting av standardisering av teknologien som brukes på internett vil innebære en stor risiko for fragmentering av nettet, noe som vil stride mot målsetningen om å bevare et åpent og interoperabelt internett. Blant vestlige land legges det derfor vekt på å følge nøye med på prosessene innen ITU for å drive utviklingen fremover mot større åpenhet og bredere deltakelsen som ligger nærmere opp til flerpartsmodellen enn tidligere.

På årets fullmaktskonferanse knyttes det igjen spenning til hvordan diskusjonen rundt de internettrelaterte resolusjonene vil utspille seg. To sentrale resolusjoner er «*IP-based networks*» (Res. 101) og «*International public policy issues pertaining to the Internet*» (Res. 102). Resolusjonene blir gjerne revidert hvert fjerde år i løpet av forhandlingene på plenipot.[64]

Resolusjon 101 omhandler tema som interoperabilitet for IP-teknologien, styrking av internett-deltakelsen blant globale sør, og samarbeid med andre standardiseringsorganisasjoner som blant annet IETF. Resolusjon 102 dekker tema som forvaltning av domenenavn og IP-adresser, samt ITUs rolle med å fasilitere internasjonalt ordskifte om policyspørsmål knyttet til internett.

ITUs fullmaktskonferanse i november vil påvirkes av resultatene fra WSIS+20-prosessen, men vil naturligvis også påvirkes av pågående teknologisk, økonomisk og politisk utvikling. Vi lever i en tid med raske skiftningen, og dette er en vesentlig del av bakteppet til den kommende konferansen. Årets plenipot kan bli minst like spennende som tidligere fullmaktskonferanser.

[63] Internet Engineering Task Force (IETF), https://www.ietf.org/, IETF working groups, https://datatracker.ietf.org/wg/

[64] Resolutions 101, 102, and more, ITU, https://www.itu.int/md/S25-RCLINTPOL22-C-0002