Nasjonal kommunikasjons-myndighet

Internet in Norway – Annual Report 2026

June 2026

Executive Summary

Deployment of Internet Access Services

At the end of 2025, respectively 99.3% and 96.3% of all households had access to internet services offering download speeds of at least 100 Mbit/s and 1000 Mbit/s. At the same time, the baseline household coverage for 4G and 5G in Norway was estimated at 100% and 99.8%, respectively[1].

Deployment of IPv6-enabled Accesses and Share of IPv6 Traffic

Over the past year, the share of IPv6 traffic in Norway — based on various international measurement sources — increased by 16 percentage points, reaching 48% as of March 2026. Norway now ranks first among the Nordic countries in terms of IPv6 usage. At the European level, Norway has risen from 15th to 7th place.

Norwegian internet providers have continued to increase IPv6 activation for their subscribers over the past year. However, fixed wireless broadband — included for the first time this year in the IPv6 statistics for fixed broadband — somewhat reduces the proportion of accesses activated for IPv6. There is also considerable variation in IPv6 activation rates between providers. Nkom continues to monitor developments and once again emphasises the importance of market players facilitating IPv6 usage to the greatest possible extent. Nevertheless, Nkom considers annual reporting to be sufficient going forward.

Security in Internet Access Services

Security is one of Nkom's core areas of responsibility, including regarding internet access services. While this is not the primary focus of this report, chapter 2 contains a brief overview of the key areas related to security in internet access services and Nkom's role in this regard.

Net Neutrality and the Open Internet

Nkom's supervision of Norwegian internet providers shows that Norwegian internet users continue to benefit from open internet access through their fixed and mobile subscriptions. The providers' reporting indicates that the traffic management practices in use comply with the Open Internet Regulation.

Nkom's review of providers' websites shows that, in general, providers give satisfactory information about traffic management measures. However, on some websites it may be challenging to locate the relevant information, particularly regarding various speed parameters for fixed internet access.

Quality of Internet Access Services

Results from the Nettfart measurement service show that speeds for fixed internet access continue the positive trend from the previous reporting period. Average download and upload speeds for fixed internet access in 2026 were 173 Mbit/s and 149 Mbit/s respectively.

Based on data from Nettfart, we observe that the average download speed, upload speed and latency for 5G networks in Norway in 2026 were 198 Mbit/s, 36 Mbit/s and 39 milliseconds (ms) respectively. This represents a slight decline compared with 2025.

Digital Services Act (DSA)

The Digital Services Act (DSA) regulates intermediary services and aims to create a safer and more accountable digital environment within the EU/EEA. The Act is not yet implemented into Norwegian law. The regulation is intended, among other things, to reduce risks to minors as well as to protect users against illegal content and manipulation, on digital services. The largest online platforms are subject to particularly stringent obligations. Nkom has been designated as the coordinating authority

[1] Due to an improvement in methodology with one provider in the 2025 reporting, the figures should not be compared directly with those reported in previous years.

for the regulation in Norway, while the Norwegian Media Authority, the Norwegian Consumer Authority and the Norwegian Data Protection Authority will be assigned supervisory responsibilities within their respective areas.

AI Act

The AI Act, which is not yet implemented into Norwegian law, establishes a common regulatory framework for the development and use of artificial intelligence within the EU/EEA, with the aim of ensuring safe and responsible AI. The regulation is based on a risk-based approach, imposing strict requirements on high-risk AI systems, while certain AI practices are prohibited.
Specific rules are also introduced for the most powerful AI models, which may impose obligations on Norwegian businesses using them. Nkom serves as the coordinating market surveillance authority and single point of contact for the AI Act in Norway.

Data Regulation

The Data Governance Act (DGA) has been proposed for implementation in Norway through a new Data Governance Act. A legislative proposal was submitted to Parliament in spring 2026, and it has not yet been decided which authority will receive supervisory powers under the new legislation.
The Data Act (DA) is already in force within the EU and is currently under consideration by the EEA EFTA states. The DA is intended to facilitate data sharing between participants in the European data market.
The Digital Omnibus package was presented by the European Commission on 19 November 2025. Its purpose is to simplify and coordinate existing digital legislation.

Anti-Fraud Work in the Internet Sector

The scale of digital fraud and attempted fraud on the internet is significant. This challenges trust in the internet as a service and as critical national infrastructure and may inflict major financial losses on individuals and businesses. Reduced trust in the internet may hinder digitalisation and digital inclusion within society. Nkom contributes to addressing these challenges through its anti-fraud efforts and through supervision of the .no domain name administration. The National Expert Group against Digital Fraud consists of both public and private entities and is led by Nkom in partnership with Økokrim. The group has primarily focused on voice and SMS fraud, but in December 2025 it received a renewed mandate to also address fraud involving internet-based services.

International Internet Governance

International internet governance passed an important milestone during the transition from 2025 to 2026. Norway hosted the 20th annual international meeting on internet governance in June 2025 (IGF 2025), and in December 2025 the United Nations General Assembly decided to continue international cooperation on internet governance (WSIS+20).
In 2026, two parallel international internet governance processes will contribute to further development of the field. At the end of April, a new application round for generic top-level domains within the DNS system opened, organised by the governing body ICANN. In October, the Plenipotentiary Conference of the UN agency ITU will take place, with key internet-related topics on the agenda.

Table of Contents

1 Status of the Internet in Norway

1.1 Introduction and Background

The internet constitutes a fundamental infrastructure within Norwegian society and provides major opportunities for innovation and growth across many sectors. Internet access has gradually become the most widely used electronic communications service in Norway and has now become virtually indispensable: High-quality, secure internet access, combined with an effective regulatory framework both nationally and internationally, is an essential prerequisite for implementing the new national digitalisation strategy[2]. Our vision reflects Nkom's role in this: "*We ensure a safe and accessible digital everyday life for everyone*."

Chapter 1 of this report describes the status of the internet in Norway, based on an assignment given to Nkom by the Ministry through White Paper No. 28 (2020–2021), "*Our Shared Digital Foundation – Mobile, Broadband and Internet Services*."

The internet provides an open platform for communication and content distribution. Consumers, business customers and content providers all connect to the platform through their respective internet providers, enabling consumers and content providers to communicate freely over the internet. This helps maintain incentives for innovation, which in turn contributes to increased demand for content.

While security aspects is not a main theme of this report, chapter 2 provides a brief overview on Nkom's role in relation to security and reliability of internet access services, data centres and other critical digital infrastructure.

Chapter 3 describes the state of net neutrality in Norway. Net neutrality is the principle that internet traffic should be treated equally, regardless of sender, recipient, equipment, application, service or content. Annual reporting on net neutrality is a statutory task assigned to Nkom under the Open Internet Regulation[3].

Chapters 4 and 5 describe the status of the Digital Services Act (DSA) and the AI Act respectively. Nkom's roles as Digital Services Coordinator and as national supervisory authority pursuant to the AI Act are also presented. Chapter 6 addresses data regulation, Chapter 7 addresses anti-fraud work relating to the internet sector, and Chapter 8 outlines the status of international internet governance.

1.2 Deployment of Internet Access Services[4]

At the end of 2025, respectively 99.3% and 96.3% of all households had access to fixed internet services with download speeds of at least 100 Mbit/s and 1000 Mbit/s. At the same point of time, baseline household coverage for 4G and 5G in Norway was estimated at 100% and 99.8% respectively[5].

Internet access service availability largely corresponds to broadband coverage. Nkom's 2025 coverage survey shows that 99.3% and 96.3% of all households had access to fixed broadband offering download

[2] "The Digital Norway of the Future", Ministry of Digitalisation and Public Governance, Nov 2024

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

[4] Last year's figures in latest publication of statistics are to be considered preliminary until the publication of the statistics for the following year, cf. ch. 5.8 in the Nkom Electronic Communications Statistics Methodology document.

[5] Due to an improvement in methodology with one provider in the 2025 reporting, the figures for mobile based coverage should not be compared directly with those reported in previous years.

speeds of at least 100 Mbit/s and 1000 Mbit/s respectively[6]. This is primarily based on fibre or hybrid fibre coaxial ("HFC")[7] networks, although fixed wireless access also contributes to coverage figures.

In Norway, 98% of households have access to alternative connection options, including fixed wireless access in addition to fibre and HFC. Although there are geographical disparities, most Norwegian households overall have good opportunities to connect to the internet.

Deployment of the 5G network began in 2020. Nkom's coverage survey at the end of 2025 shows that combined baseline 5G coverage for all mobile operators reached 99.8% of households. At the same point the previous year, coverage was estimated at approximately 99.7%[8]. Most counties have coverage exceeding 95%, and for most counties, coverage is close to 100%.[9]

Electronic communications statistics for 2025[10] show that Telenor, Altibox[11], Telia, GlobalConnect and NextGenTel together accounted for approximately 86% of the fixed internet access market – in terms of number of access lines - when combining residential and business markets. In the mobile internet access market, concentration is even higher. Together, Telenor, Telia and Ice account for approximately 90% of mobile subscriptions, slightly down compared to 2024.

Towards the end of 2022, internet access via low Earth orbit (LEO) satellites from Starlink became available across Norway[12]. Eutelsat-OneWeb offers a similar service on a somewhat more limited scale. Other providers are also expected to offer internet access via LEO satellites in coming years to both consumers and professional users, including Amazon LEO. Work is also underway to enable such constellations to communicate directly with ordinary mobile phones for simple voice, text and data services in areas lacking terrestrial coverage. Starlink, Amazon LEO and AST SpaceMobile are examples of companies developing these solutions for future commercial launch in Europe.

1.3 Volume of Data Traffic in Norwegian Mobile Networks, Roaming Abroad and of Internet Interconnection

In 2025, the combined data traffic in mobile networks in Norway and traffic from Norwegians roaming abroad, amounted to 1,160 petabytes (PB), representing an increase of 10% compared with 2024.

In January 2026, the maximum level of incoming internet interconnection traffic ("peak throughput") to the largest fixed network providers and mobile operators during peak hour ranged between 0.3 Tbit/s and 3 Tbit/s.

The distribution of internet traffic across different applications is relatively similar between mobile and fixed networks, except for streaming services, which account for a much larger share in fixed networks.

Data Traffic in the Mobile Networks

Traffic growth is influenced by technological development and the resulting increase in network capacity, as well as growth in customer numbers and higher data allowances.

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

[7] Hybrid Fibre Coaxial (HFC) refers to the use of fibre optic and coaxial cables in combination within a cable network.

[8] Due to an improvement in methodology with one provider in the 2025 reporting, the figures for mobile based coverage should not be compared directly with those reported in previous years.

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

[10] Electronic Communications Statistics 2025

[11] Altibox refers to the Altibox partnership, consisting of Lyse and approximately 30 other regional providers based on FTTH networks.

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

Figure 1 illustrates the development of data traffic distributed across ordinary mobile subscriptions, dedicated internet subscriptions[13], roaming abroad and M2M. Ordinary mobile subscriptions generate most of the data traffic in mobile networks (more than 80%). In 2025, total internet traffic in mobile networks reached 1,160 petabytes (PB)[14], an increase of 10% compared with 2024. The volume of internet traffic carried over mobile networks in 2025 is close to double the level recorded in 2021.

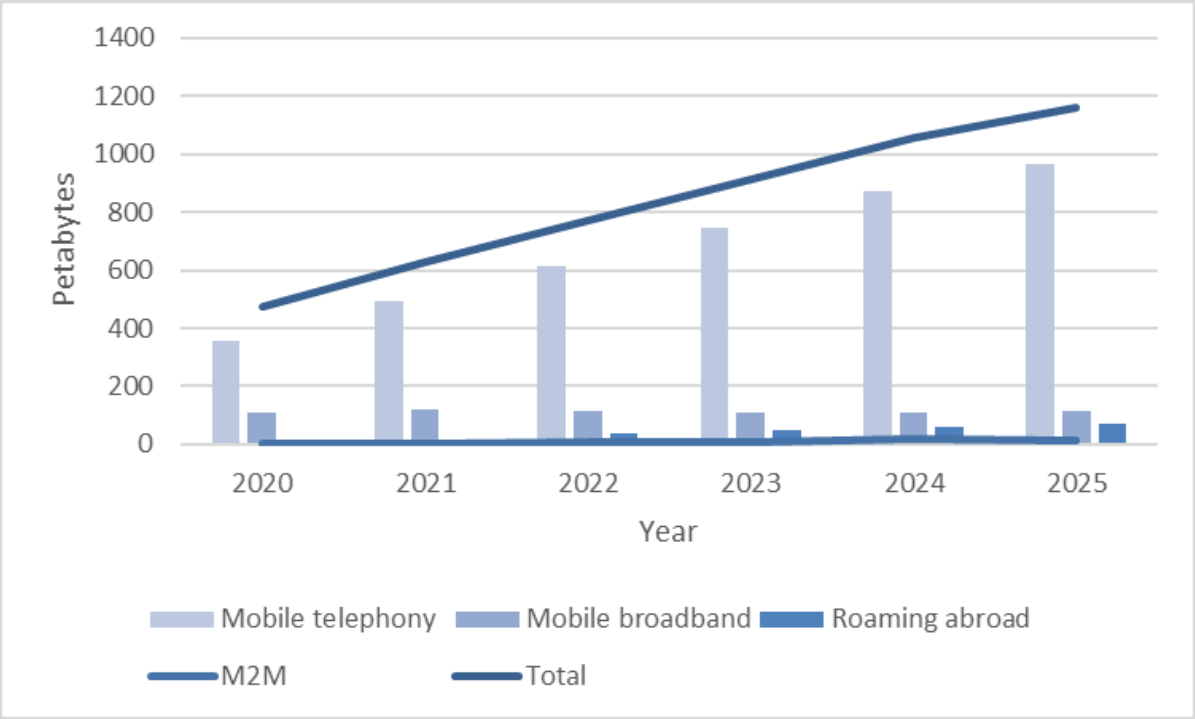

Figure 1– Internet traffic by mobile subscription category (Source: Nkom Electronic Communications Statistics 2025)

Internet traffic from roaming abroad reached 72 petabytes (PB) in 2025, representing a 17% increase compared with the previous year.

1.4 Deployment of IPv6-enabled Accesses and Share of IPv6 Traffic

Over the past year, the share of IPv6 traffic in Norway - based on various international measurement sources - increased by 16 percentage points, reaching 48% in March 2026. Norway now ranks first among the Nordic countries in IPv6 usage. At the European level, Norway has risen from 15th to 7th place.

Norwegian internet service providers have continued increasing IPv6 activation for subscribers over the past year

However, fixed wireless broadband - included for the first time this year in IPv6 statistics for fixed broadband - somewhat reduces the proportion of accesses activated for IPv6. There is also significant variation in IPv6 activation rates between providers. Nkom continues to monitor developments and once again emphasises the importance of market participants facilitating IPv6 usage to the greatest extent possible. Nevertheless, Nkom considers annual reporting sufficient going forward.

[13] Dedicated internet subscriptions comprise products that provide a dedicated data service using a separate SIM card. The user is provided with a data-only connection between the terminal device and the mobile network, and through this connection gains access to the Internet.

[14] A petabyte (PB) is equal to 1,000 terabytes (TB) or 1,000,000 gigabytes (GB).

1.4.1 On the Transition from IPv4 to IPv6

IP (Internet Protocol) is the fundamental protocol used to transfer traffic across the internet. The protocol exists in two versions: IPv4 and IPv6. Public IP addresses are globally unique identifiers for computers connected to the internet.

There is a need to increase the use of IPv6 on the internet due to the shortage of available IPv4 addresses. The complexity of today's internet means that the transition from IPv4 to IPv6 must occur gradually, beginning with a period in which both protocols coexist.

IPv6 helps ensure sufficient IP addresses for a large number of new devices, thereby supporting growth and development in IoT solutions. This in turn contributes to a more open and scalable internet, providing a foundation for innovation and growth.

1.4.2 Deployment in Norway Compared with Other Countries

The figures below show the status of IPv6 deployment in Norway compared with other countries. The data is based on the three main publicly available sources on IPv6 deployment: Google[15], Facebook[16] and APNIC[17], with data collection carried out in March 2026.

Both Google and Facebook measure traffic distribution to their own services from various users, while APNIC's measurements are based on users interacting with advertisements designed to facilitate IP version measurement. These factors may introduce certain biases. In 2025, Cloudflare was therefore added as a new statistical source. Cloudflare measures traffic distribution between IPv4 and IPv6 at centrally located nodes in IP networks in most countries. Overall, measurements from Google, Facebook and APNIC show relatively small variations between one another, while Cloudflare generally reports lower IPv6 shares at centrally located measurement points. Nkom has chosen to continue using the same data sources as last year to ensure comparability over time and across countries.

Within a single year, IPv6 deployment in Norway increased by 15.9 percentage points to 47.8% in March 2026. As can be seen from
Figure 2 below, Norway now ranks first among the Nordic countries in IPv6 usage. Figure 3 below shows that at the European level, Norway ranks seventh, an increase of eight places from the previous year.
Among the countries with the highest IPv6 deployment globally[18], Norway moved significantly upward from 44th to 21st place.

[15] Share of Google users accessing services by IPv6: Map-based presentation of data from Google, as well as table presentation of the same data

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

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

[18] Only the 150 countries in the world with the highest number of internet accesses are included in this comparison.

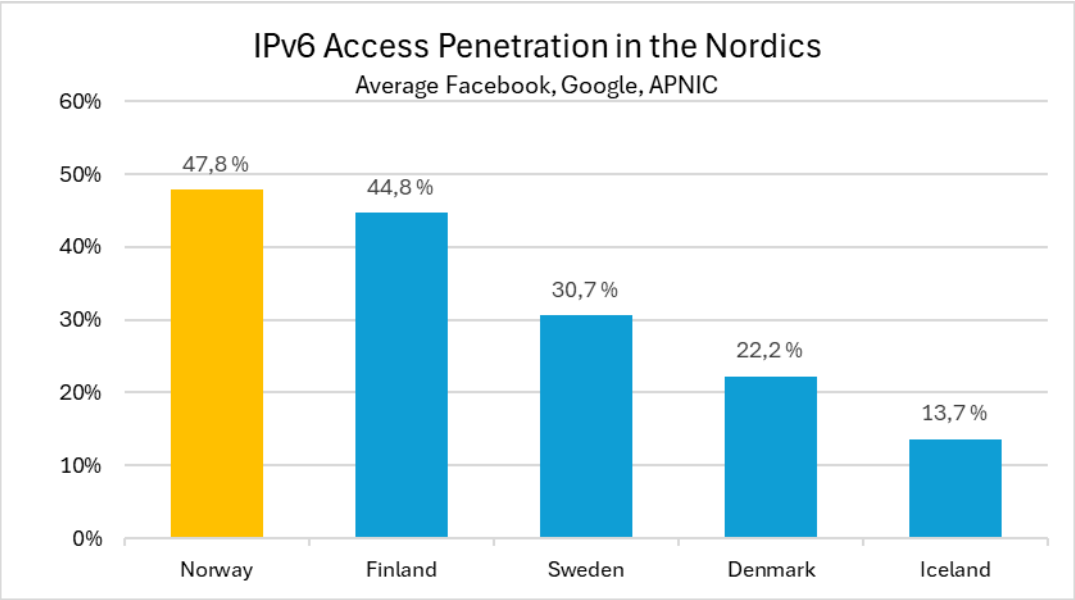

Figure 2 – IPv6 adoption in the Nordic countries

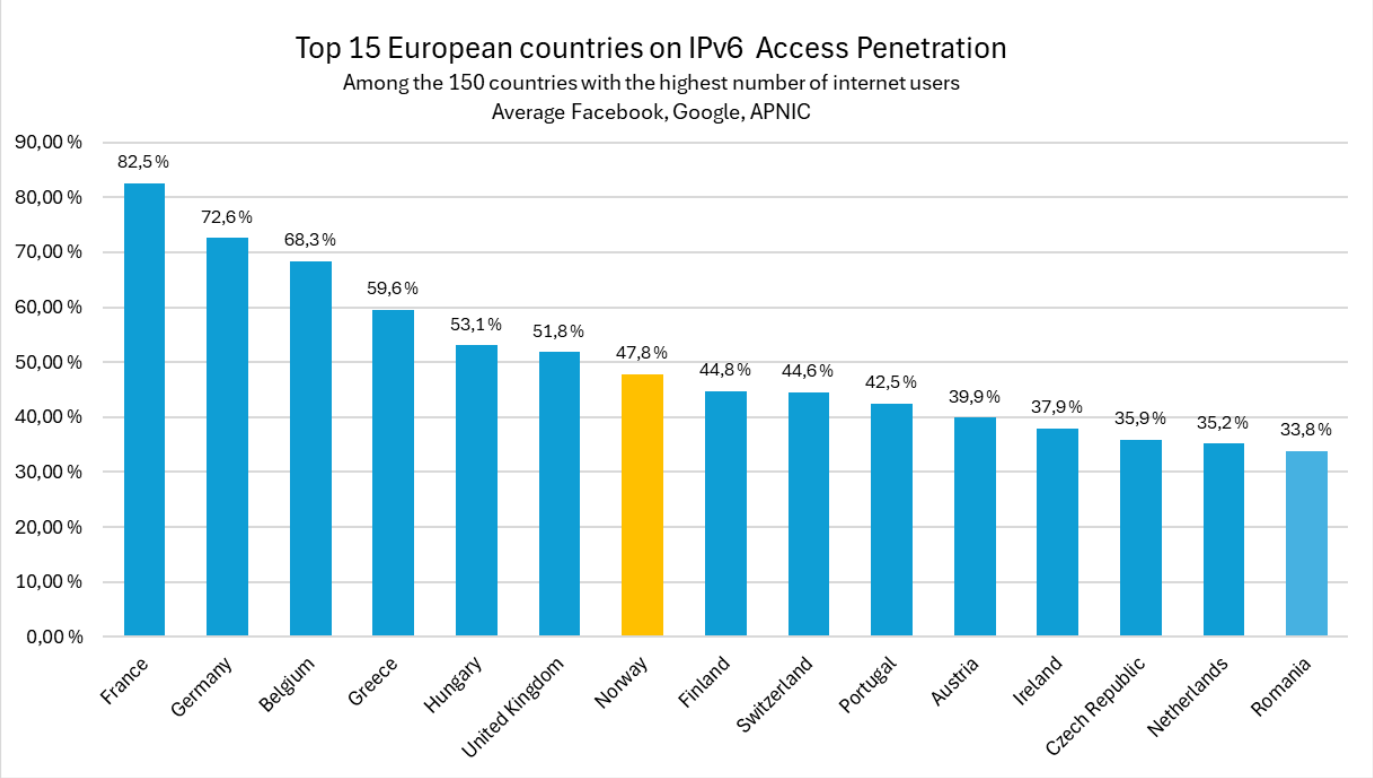

Figure 3 – IPv6 adoption in the top 15 countries in Europe

Figure 4 and Figure 5 below show Cloudflare measurements of the proportion of IPv6 traffic recorded at measurement nodes located centrally within the networks, respectively for the Nordic countries and for the 21 European countries with the highest share of IPv6 traffic, which are also among the 150 countries in the world with the largest numbers of internet users[19].

[19] https://radar.cloudflare.com/adoption-and-usage - Data Extract as of March 26

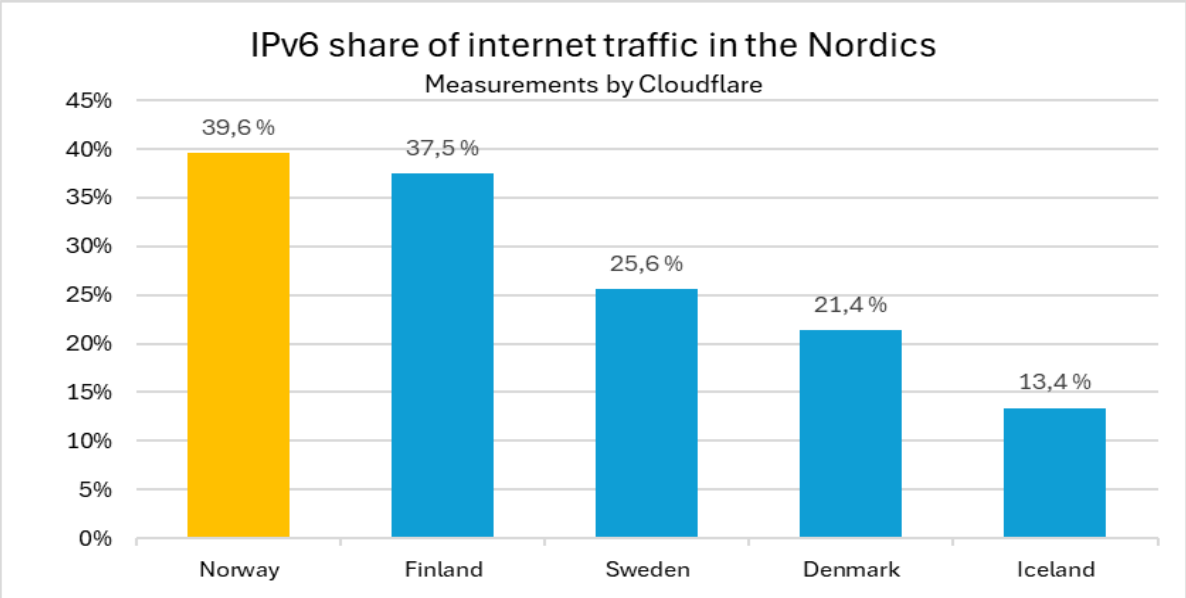

Figure 4 - Share of Internet Traffic Using IPv6 – Nordic Countries

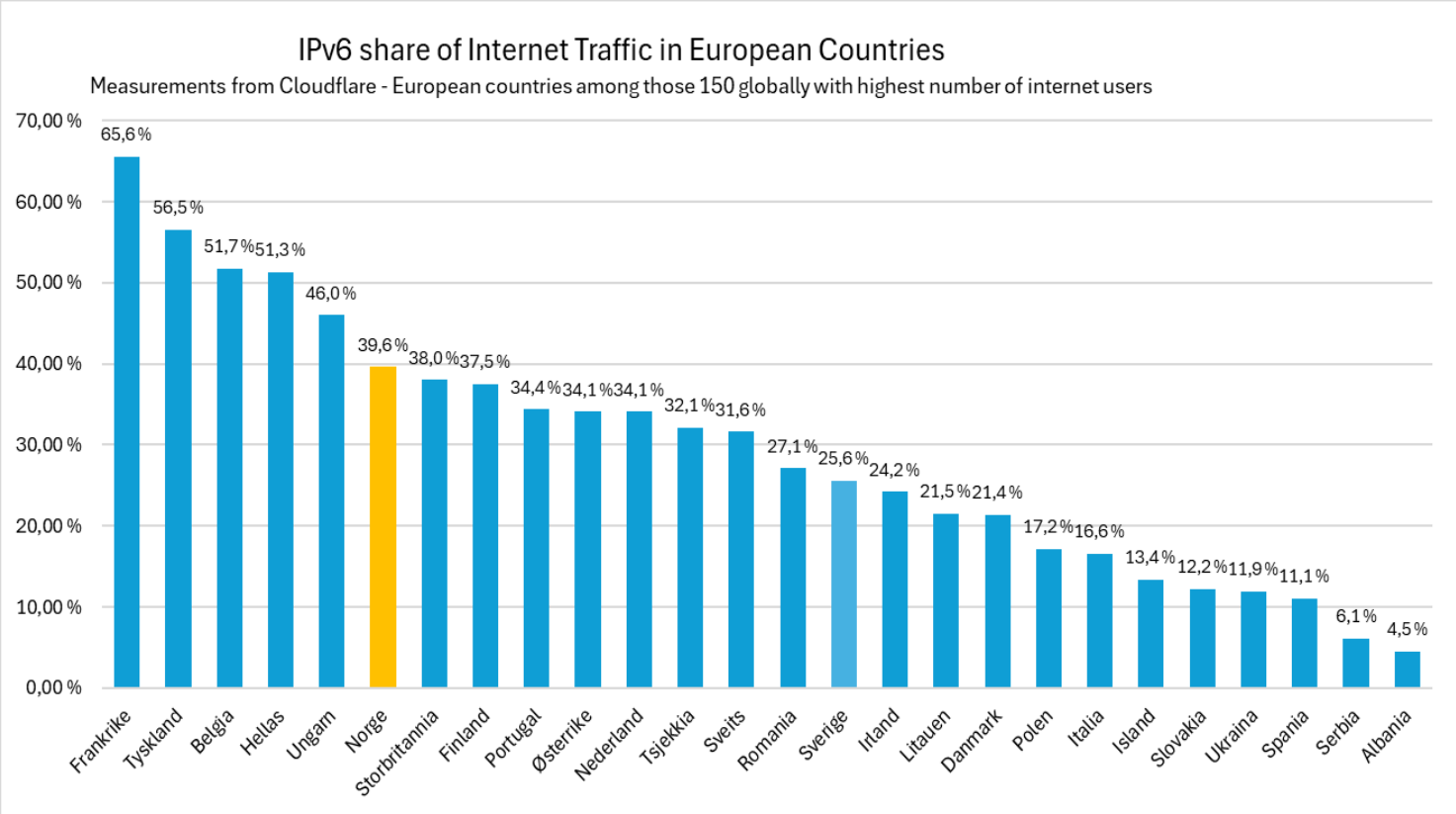

Figure 5 - European countries with the highest share of IPv6 traffic among the 150 countries with the largest number of users

1.4.3 IPv6 Activation Rates among Norwegian Providers

Figure 6 and Figure 7 below present IPv6 activation rates for fixed internet access services, including FWA, and for mobile networks, respectively, aggregated for the largest providers in Norway. The

figures are based on information submitted by the providers[20]. For mobile networks, the figures also show the proportions of IPv4 and IPv6 traffic within the networks.

Largest fixed internet access service providers combined - FWA included from 2025	31.12.23	31.12.24	31.12.25
Percentage of accesses activated for IPv6	63 %	78 %	79 %
Percentage of IPv6 compatible operator deployed CPEs	86 %	97 %	94 %
Percentage of CPEs which will have to be replaced to support IPv6	14 %	3 %	6 %

Figure 6 - IPv6 activation and the proportion of IPv6-compatible operator deployed CPE equipment among the largest fixed broadband providers

Largest mobile operations combined	31.12.23	31.12.24	31.12.25
Percentage of subscriptions which are IPv6 ready	85 %	91 %	97 %
Percentage of internet traffic volume - IPv6	42 %	40 %	45 %
Percentage of internet traffic volume - IPv4	58 %	60 %	55 %

Figure 7 - IPv6 activation and the IPv4/IPv6 share of traffic volume among the largest mobile network operators

1.4.4 Regulatory Follow-up

In April 2023, Nkom held dialogue meetings on IPv6 with the largest internet providers in the Norwegian market to encourage the transition from IPv4 to IPv6.

Nkom presented the following targets for a phased IPv6 implementation plan over the next two to three years, and Norwegian internet providers broadly indicated alignment with the proposal[21]:

1. *By 30 April 2024, Norwegian ISPs should activate IPv6 for all internet subscribers, except where physical replacement of home routers is required.*
2. *By 30 April 2025, Norwegian ISPs should activate IPv6 for all internet subscribers and replace any home routers that cannot be upgraded through software.*
3. *Home routers based on DSL technology connected to copper networks do not need to be replaced until the copper network phase-out has been completed.*

Nkom will continue to monitor IPv6 development in the Norwegian market closely during the transition period.

- *Nkom will publish periodic statistics on active IPv6 availability among Norwegian ISPs, together with statistics from external sources concerning IPv6 usage in the Norwegian market.*
- *Based on developments up to the end of 2025, Nkom will assess whether there is a need to introduce national regulation making IPv6 mandatory for Norwegian ISPs.*

The largest ISPs now submit annual overviews of IPv6 activation in their networks to Nkom, and the overall trend among operators is moving in the right direction.

In light of the targets above and the reported IPv6 activation rates compared with IPv6 traffic shares, Nkom believes that continued follow-up is necessary regarding both further activation of accesses and

[20] The figures were obtained from the network operators in March 2026.

[21] Internet in Norway – Annual Report 2023, p. 21

replacement of end-user equipment. Nevertheless, given the positive developments, Nkom considers annual reporting to be sufficient.

Nkom encourages Norwegian ISPs to intensify their efforts to increase IPv6 usage in the internet access services they provide. This work takes place alongside trends among equipment and software vendors to introduce IPv6 support in end-user devices.

2 Security in Internet Access Services

Security in internet access services is a prerequisite for use by society, businesses and individuals. Nkom works to ensure a safe and resilient internet through regulation, supervision, and close cooperation with industry stakeholders and public authorities. Through activities including incident follow-up and requirements for adequate security, Nkom helps to prevent and manage digital threats. This work encompasses the protection of electronic communications networks, data centres and critical digital infrastructure. Nkom actively collaborates with national and international stakeholders to address an increasingly complex and evolving threat landscape. Taken together, these efforts help to strengthen trust in the internet and digital services. The objective is to ensure that citizens, businesses and public authorities have access to secure and reliable digital services throughout the country.

The Electronic Communications Act[22] requires providers of internet access services to deliver electronic communications services with adequate security for users in times of peace, crisis and war. The Digital Security Act and the associated regulations entered into force on 1 October 2025 and establish security requirements for the central registry of Norwegian top-level domains (.no), recursive DNS services that, on average over a 30-day period, respond to more than 15,000 domain name system queries per second, and internet exchange points (IXPs). Together, these two regulatory frameworks help ensure that internet access services are secure and safe for users.

3 Status of Net Neutrality in Norway

The state of net neutrality in the Norwegian market remains generally good. Work on this year's report has not revealed any major changes or deviations compared with last year's assessment.

3.1 Introduction and Background

Net neutrality is the principle that all internet traffic shall be treated equally, regardless of sender, recipient, equipment, application, service, or content. A common European regulatory framework for net neutrality was introduced in 2015 and incorporated into Norwegian law in 2017[23]. The main purpose of the regulation is "*to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users' rights. It aims to protect end-users and simultaneously to guarantee the continued functioning of the internet ecosystem as an engine of innovation.*"[24]

Nkom regulates net neutrality in Norway on the basis of this framework and BEREC's net neutrality guidelines, developed pursuant to Regulation 2015/2120, Article 5(3). According to recital 19, regulators shall take the utmost account of BEREC's guidelines when applying the Regulation.

This report covers the period from 1 May 2025 to 30 April 2026.

[22] Cf. unofficial translation available here.

[23] Cf. Regulation on Electronic Communications Networks and Services, §1-11

[24] Regulation 2015/2120, Recital (1)

3.2 Access to an Open Internet

Nkom's follow-up of Norwegian internet service providers shows that Norwegian internet users continue to benefit from open internet access through their fixed and mobile subscriptions. Reporting from providers indicates that the traffic management measures in use comply with the Open Internet Regulation.

3.2.1 The Right to Open Internet Access

End users are entitled to open internet access, enabling them to decide for themselves how the connection is used, including which content is accessed or delivered and which applications are used or offered, pursuant to Article 3(1) of the Regulation. ISPs shall transmit traffic in a non-discriminatory manner but may implement certain traffic management measures, such as blocking traffic for security reasons.

Providers may also offer specialised services, such as IPTV, in parallel with internet access services where such services require quality levels that cannot be guaranteed over the public internet. Furthermore, specialised services may only be offered where network capacity is sufficient to ensure that availability and general quality of internet access services for end users are not adversely affected.

3.2.2 Traffic Management of Internet Access

Nkom has obtained information from Norwegian internet providers regarding traffic management of internet access services. This year's results show no significant differences compared with last year.

According to the collected information, typical traffic management measures include blocking of domain names in DNS following court orders, Kripos[25] Child Abuse Filter and blocking of TCP/UDP ports as part of specific security measures, for example to prevent DDoS attacks and other forms of cyberattack.

In the Norwegian market, differentiated speed tiers for mobile internet access are offered. BEREC's guidelines state that such subscriptions comply with the Regulation provided that they are application-agnostic, meaning that all applications are subject to equal traffic management.

3.2.3 Specialised Services

Nkom has also gathered information regarding specialised services, meaning services provided in parallel with internet access services that fulfil the specific criteria laid down in the Regulation. A typical specialised service in fixed networks is IPTV. Similarly, VoLTE is commonly offered as a specialised service in mobile networks.

Nkom also asked providers how they ensure that network capacity is sufficient to prevent specialised services from negatively affecting the general quality of internet access for end users. The common response was that traffic levels across network connections are continuously monitored and capacity is expanded where necessary.

Nkom has not carried out detailed investigations of the reported traffic management measures and specialised services but assumes that these are provided in accordance with the Regulation. In future, Nkom may conduct more extensive investigations.

[25] National Criminal Investigation Service

3.3 Information on the Internet Access Service

Nkom's review of internet providers' websites shows that providers generally give satisfactory information regarding traffic management measures. However, on some websites it may be difficult to locate the relevant information, particularly concerning various speed parameters for fixed internet access.

3.3.1 Information Requirements

Article 4 of the Regulation establishes information requirements regarding internet access services that providers must make available to end users. Article 4(1) establishes transparency requirements for agreements between providers and end users, while Article 4(2) regulates providers' obligation to maintain transparent, simple, and effective complaint handling procedures.

Nkom has reviewed relevant providers' websites and assessed compliance with Article 4 of the Regulation. The following sections provide comments on the review.

3.3.2 Information About Traffic Management

Providers of internet access services are required to inform users about the traffic management measures employed.

Relevant traffic management measures are described in ch. 3.2.2 above. According to the Regulation, providers shall include information about these measures in their contractual terms and make the information publicly available, typically on their websites. Although providers can demonstrate that such information is publicly available, it is also relevant to assess the content and quality of the information.

Nkom's review shows that providers present traffic management measures in varying but generally satisfactory ways. On some websites it can be difficult to locate the relevant information. Some providers maintain dedicated net neutrality pages where traffic management is one of several topics. Others provide more direct information in terms and conditions and elsewhere on their websites. Dedicated information pages give end users a more comprehensive overview of net neutrality, although both approaches are considered by Nkom to comply with the regulatory framework.

3.3.3 Information About Speed

Fixed Internet Access

Article 4(1)(d) of the Regulation requires end users to be informed about the speed that providers can realistically deliver.

Providers of fixed internet access services shall specify the following speed parameters for both download and upload:

- Minimum speed
- Normally available speed
- Maximum speed
- Advertised speed

"Normally available speed" refers to the speed an end user can expect to achieve most of the time while using the service. This is likely the parameter that provides end users with the most relevant information regarding service performance. Regarding the Regulation's transparency requirements, BEREC considers certain types of Fixed Wireless Access (FWA) to constitute fixed internet access. This includes cases where wireless technology, including mobile networks, is used to provide internet

access at a fixed location using dedicated equipment and either capacity reservation or dedicated frequency bands. In such cases, requirements relating to contractual information and website publication should correspond to those applicable to fixed internet access.

For fixed internet access, Nkom observes that providers vary in the extent to which they disclose the required speed parameters. Advertised and maximum speeds are generally presented clearly on providers' websites, while information regarding minimum and normally available speeds is more inconsistent and in some cases incomplete.

Mobile Internet Access

In mobile networks, normally available speed within a given cell is difficult to predict due to varying numbers of active users. For this reason, only providers of fixed internet access are required to disclose this speed parameter.

However, the Regulation requires providers of mobile internet access to specify the following speed parameters:

- Estimated maximum speed
- Advertised speed

Mobile internet access services include both ordinary mobile subscriptions and dedicated internet subscriptions, as both provide internet access. Standard mobile subscriptions support internet access as well as telephony and SMS services, while dedicated internet subscriptions support internet access only. The former are commonly used via smartphones, whereas the latter are typically used through routers.

Regarding dedicated internet subscriptions in mobile networks, a distinction is often made between *"fixed wireless access*" provided at a fixed geographical location, often using permanently mounted outdoor antennas, and "*dedicated mobile internet access*" that may be used freely across different geographical locations within the coverage area. These differences may lead to varying conditions affecting achievable internet speeds.

For mobile internet access, Nkom considers that providers generally disclose the speed parameters required by the Regulation.

Conclusion

Nkom's review shows that providers vary in how they present information about internet access services. On some websites, it may be difficult to locate relevant information, and in certain cases information appears to be missing. End users should therefore be aware of which information they are seeking or contact their provider for specific guidance on where the information is available. In connection with this year's reporting, Nkom has chosen to follow up more closely with certain providers that do not appear to have published speed information in accordance with net neutrality requirements.

3.4 Quality of Internet Access Services

Results from the Nettfart measurement service show that speeds for fixed internet access continue the positive trend observed during the previous reporting period. Average download and upload speeds for fixed internet access in 2026 are 173 Mbit/s and 149 Mbit/s respectively.

Based on data from Nettfart, the average download speed, upload speed, and latency for 5G networks in Norway in 2026 were 198 Mbit/s, 36 Mbit/s, and 39 milliseconds (ms) respectively. This represents a slight decline compared with 2025.

3.4.1 Requirements Regarding Quality of Internet Access Services

Article 5 of the Regulation states that national regulatory authorities have monitoring and reporting obligations to ensure that providers of internet access services comply with their obligations relating to open internet access. Furthermore, NRAs shall promote non-discriminatory internet access with quality levels reflecting technological development.

Recital 17 emphasises the importance of ensuring that specialised services and the use of such services do not reduce the general quality of customers' internet access. For internet access via mobile networks, a certain flexibility is permitted due to the special circumstances associated with varying numbers of active users per cell and non-uniform coverage. Nevertheless, over time, the general quality of internet access is also expected to be maintained in mobile networks.

3.4.2 Regulatory Follow-up

One regulatory measure for monitoring compliance with Article 5(1) of the Regulation is to track developments in the quality experienced by end users through measurements of their internet access. In this report, Nkom has assessed results from its Nettfart measurement service, which can be used through both a web browser and as a mobile app. Nettfart is based on crowdsourcing, meaning that users themselves actively perform measurements and thereby generate the dataset analysed by Nkom.

As with all forms of crowdsourcing, the statistical basis may have limitations in terms of representativeness. Nevertheless, the results provide an indication of the quality experienced by end users. The dataset also demonstrates that information is collected over time from a very large proportion of Norwegian providers.

3.4.3 Measurement Results

Measurement Results from nettfart.no

This section presents results from measurements performed via the website nettfart.no. For fixed internet access, the development in average speeds across different subscriptions is presented.

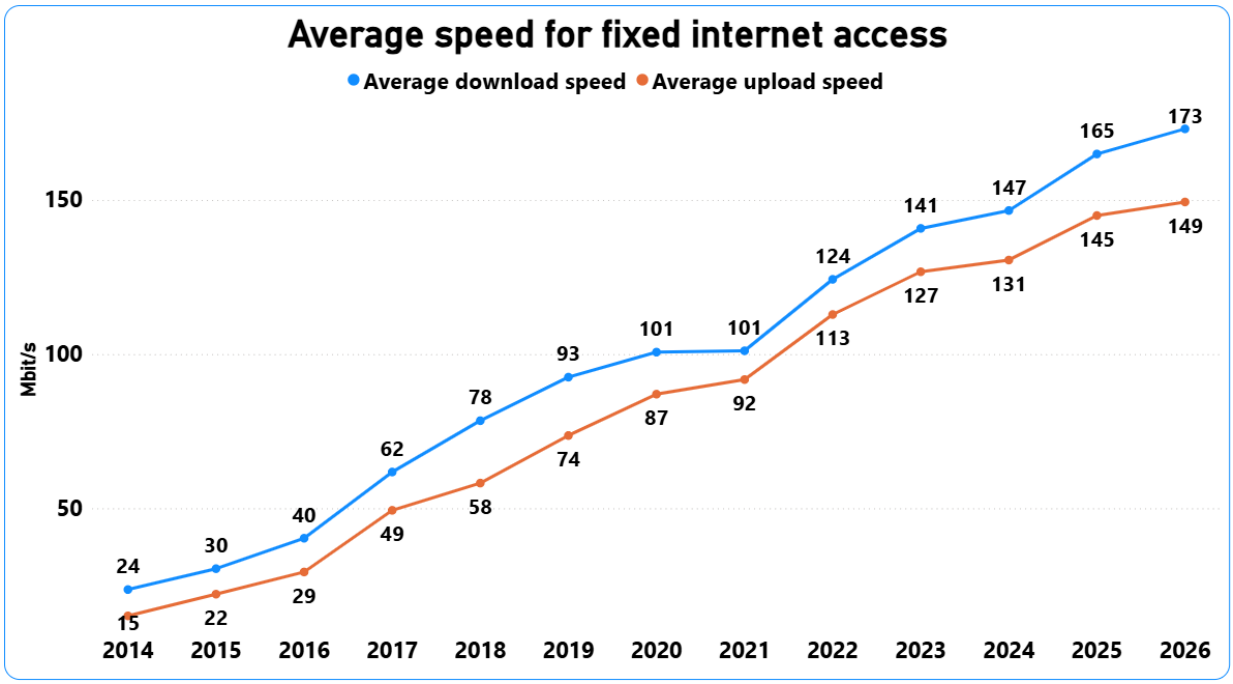

Figure 8 - Average Speed for Fixed Internet Access

Figure 8 shows that the average measured download speed across end users' subscriptions in 2026 is approximately 70% higher than the equivalent figures five years earlier in 2021. The trend of annual growth of 10–20 Mbit/s per year appears to be flattening somewhat compared with previous years.

Measurement Results from the Nettfart Mobile App

This section presents results measured through the Nettfart mobile application, beginning with average speed per technology (4G, 5G, and WLAN), followed by key figures for measurements performed by users of Norwegian mobile networks in 2025.

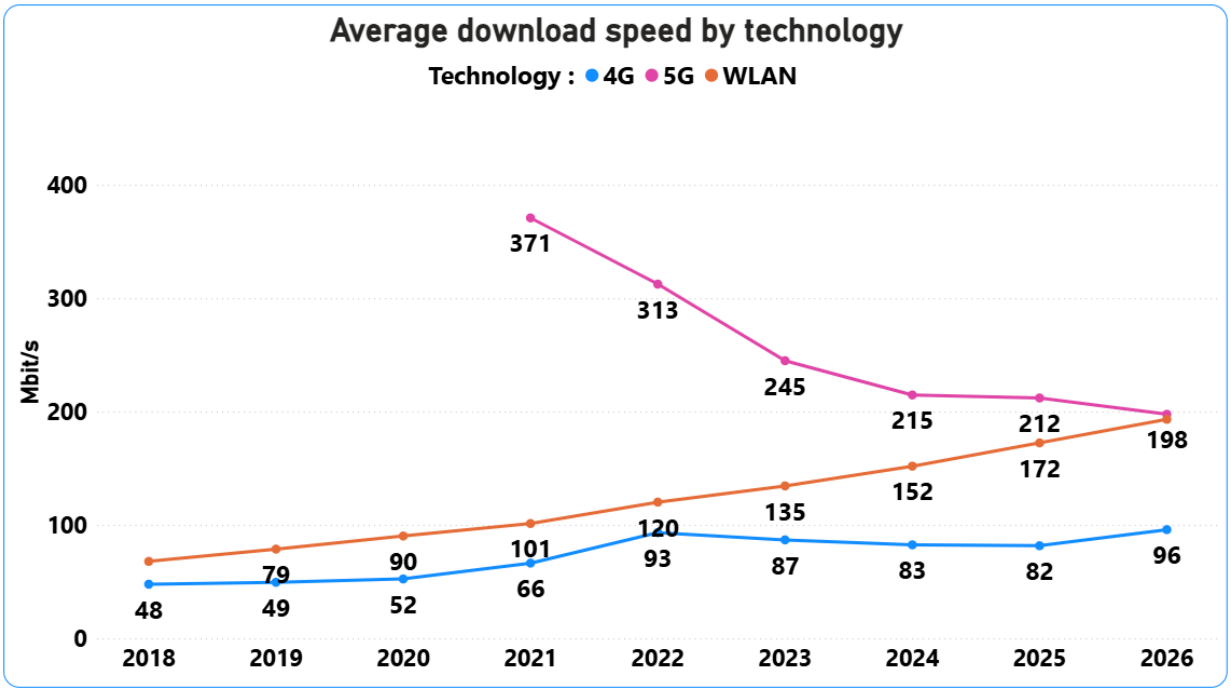

Figure 9 - Average Download Speed by Technology (Source; "Nettfart" mobile app)

Figure 9 shows average download speeds by technology. The figure demonstrates that users of the Nettfart mobile application achieve significantly higher download speeds when measuring over 5G compared with 4G. New this year is that measurements performed via WLAN achieve the same average speeds as those performed via 5G. For the mobile technologies 5G and 4G, the figure shows that 4G performance has improved somewhat compared with last year, whereas 5G performance has declined.

Overall, the average download speed for 4G and 5G combined in 2026 is identical to the values observed in 2025. Total traffic volumes in mobile networks have increased during the past year, and so far, it appears that mobile operators continue to expand capacity to keep pace with this development.

Average download speed for WLAN continues to increase and has risen by 15% over the past year. For WLAN measurements, however, it is uncertain which transmission medium is used between the measurement location and the network. This may include fibre, hybrid cable, or fixed wireless broadband.

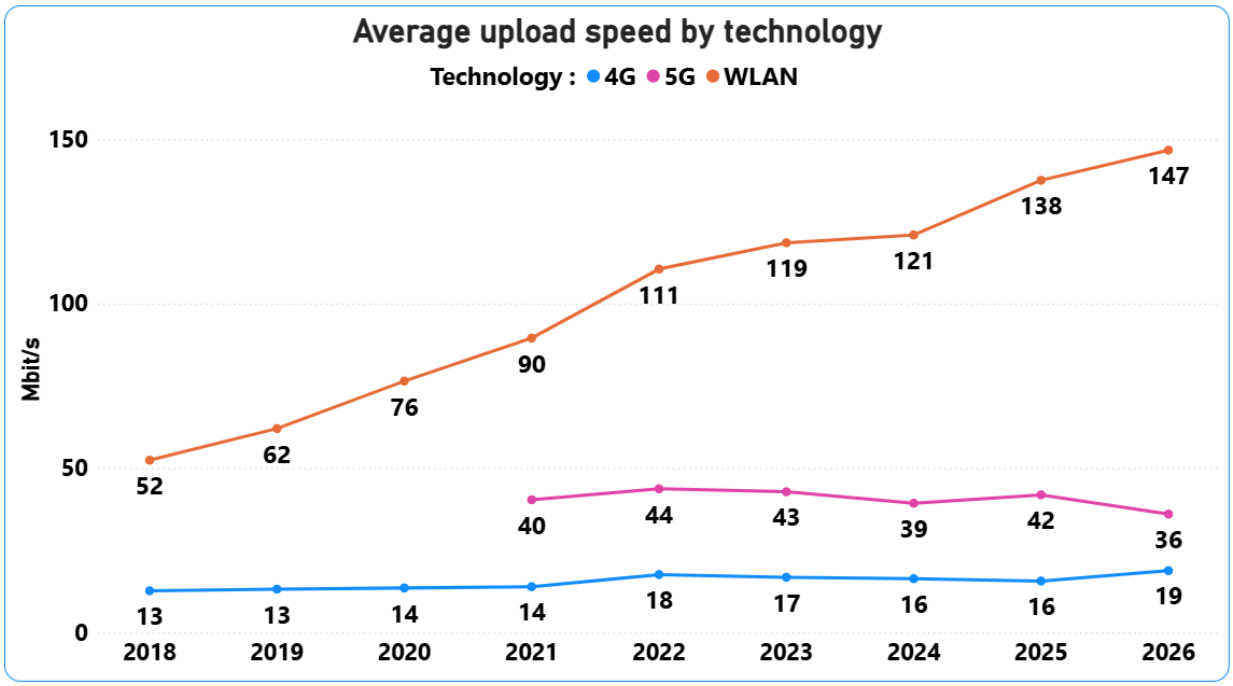

Figure 10 - Average Upload Speed by Technology

Figure 10 shows that mobile technologies (4G and 5G) exhibit significantly lower upload speeds than measurements performed via WLAN. One possible explanation is that WLAN connections are more frequently linked to access lines with symmetrical characteristics, such as those offered by many fibre subscriptions.

The figure also shows that average upload speeds in mobile networks are substantially lower than download speeds, cf. Figure 9. This is likely because mobile networks reserve a larger share of available spectrum resources, and/or time allocation in 5G, for downloading traffic, on the assumption that this represents the dominant direction of internet traffic for individual users. Nkom observes that average upload capacity for 5G as of May 2026 is lower than five years ago when reporting first began.

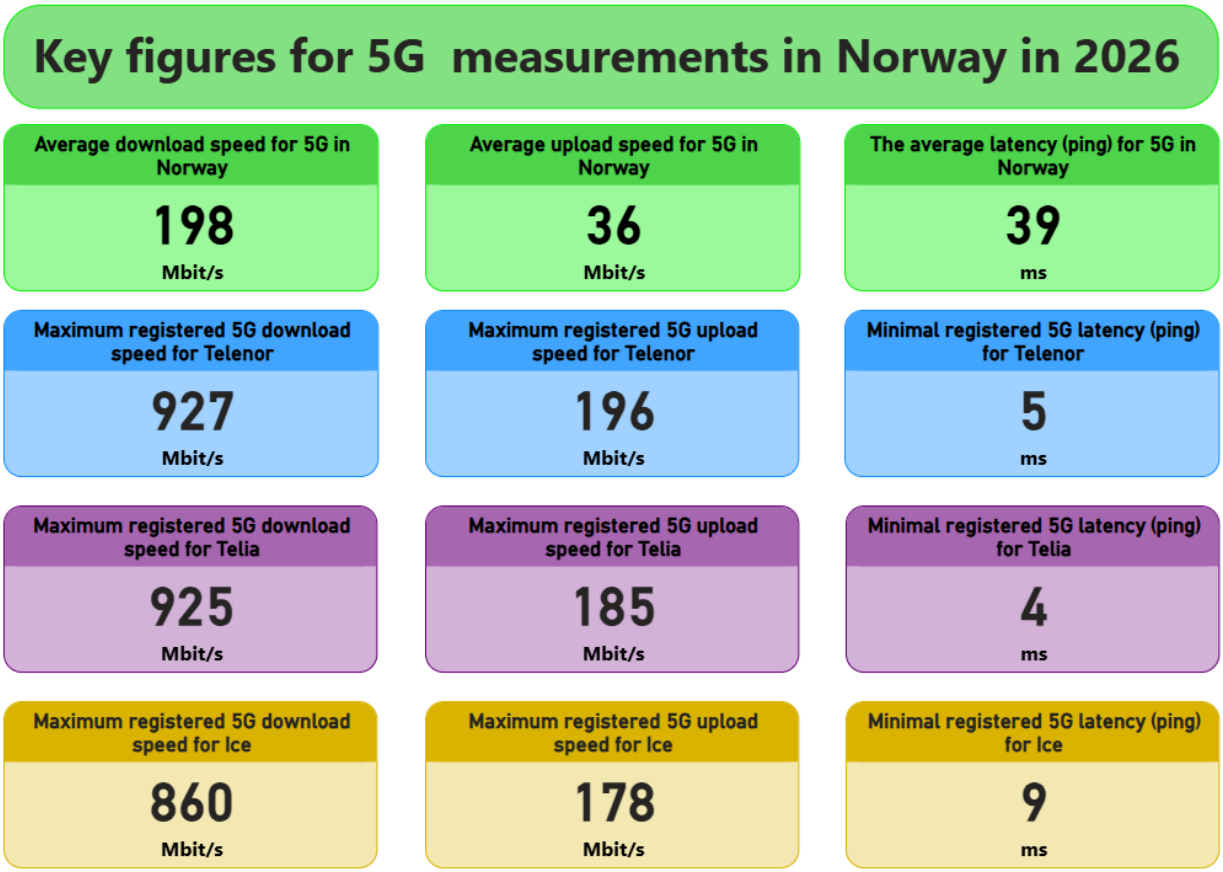

Figure 11 - Key Figures for Norwegian 5G Networks in 2026

Figure 11 presents selected key figures for 5G measurements in Norwegian mobile networks in 2026. Average download speed, upload speed, and latency for Norwegian 5G networks in 2025 were 198 Mbit/s, 36 Mbit/s, and 39 milliseconds respectively. Measurements from the Nettfart mobile app show that Norwegian 5G networks provide internet access with high speeds and low latency. It will also be interesting to observe how future activation of 5G Stand Alone for smartphones will influence these key indicators.

3.4.4 General Quality of Internet Access Services

Nkom has applied BEREC's methodology for evaluating the general quality of internet access services to measurements performed in mobile networks. The method uses a forecasting function based on average download speed, upload speed, and latency from previous years to estimate expected values for subsequent years. Estimated and measured values may then be compared to identify significant deviations.

The figures below show forecasts[26] for download speed, upload speed, and latency for measurements conducted in Norwegian mobile networks, aggregated across all mobile operators. The blue line represents measured values, while the dashed pink line represents the forecast for 2025.

[26] Forecasts for 2025 are based on historical data from 2018–2024.

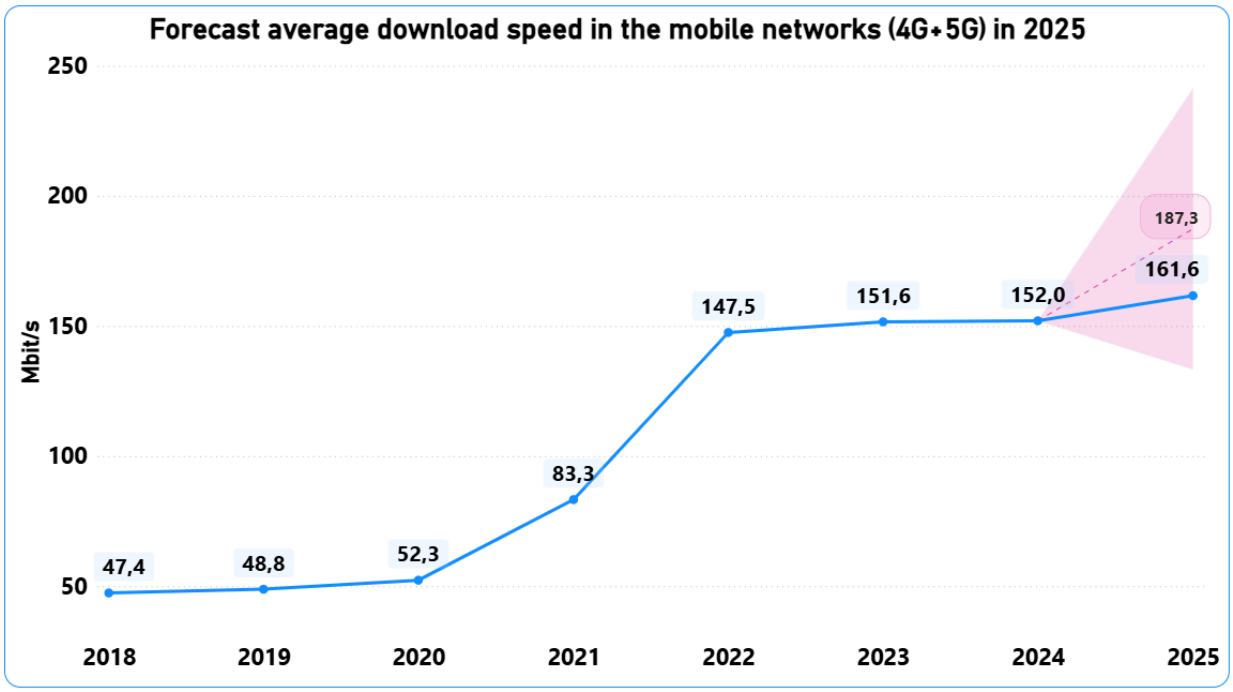

Figure 12 - Forecast for Average Download Speed in Mobile Networks in 2025

Figure 12 shows a forecast average download speed for 2025 of 187 Mbit/s, while the measured average value was approximately 162 Mbit/s. This indicates that the development of download speeds in mobile networks during 2025 did not meet the mathematical expectation based on previous years' values. Nevertheless, the deviation between measured and predicted values remains at an acceptable level.

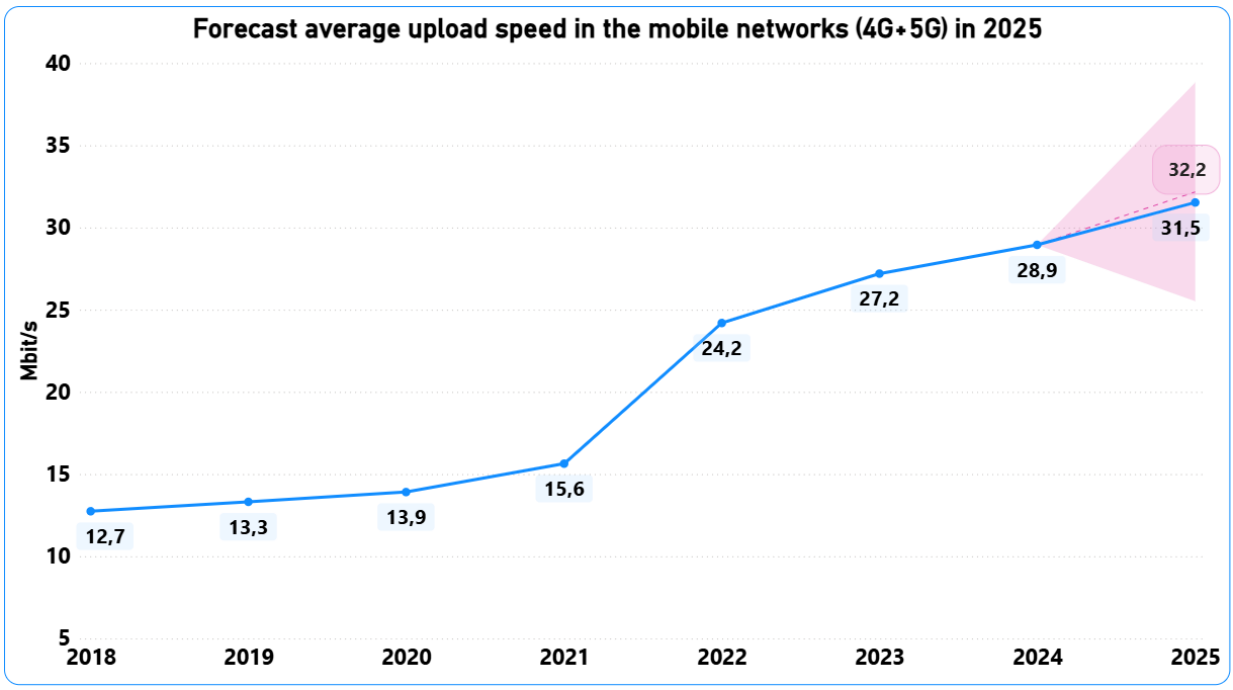

Figure 13 – Forecast for Average Upload Speed in Mobile Networks in 2025

Figure 13 shows a forecast average upload speed for 2025 of approximately 32 Mbit/s, while the measured average value was 31.5 Mbit/s. This demonstrates that upload speed development in mobile networks closely matched the forecast.

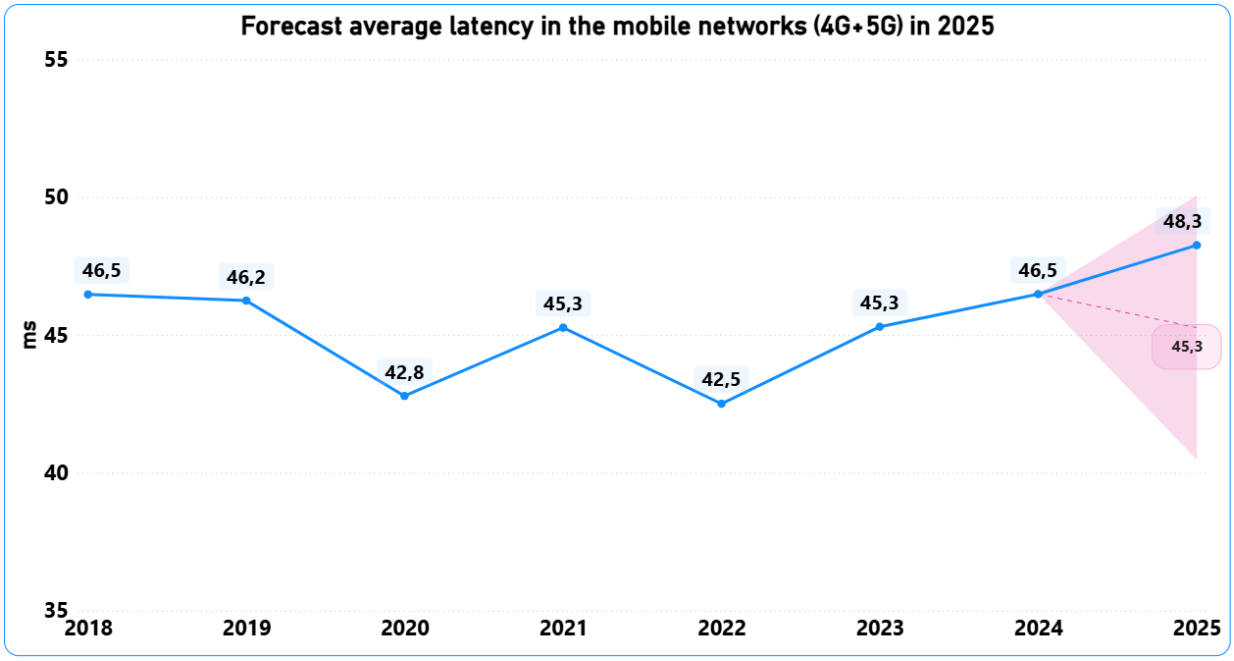

Figure 14 - Forecast for Average Latency in Mobile Networks in 2025

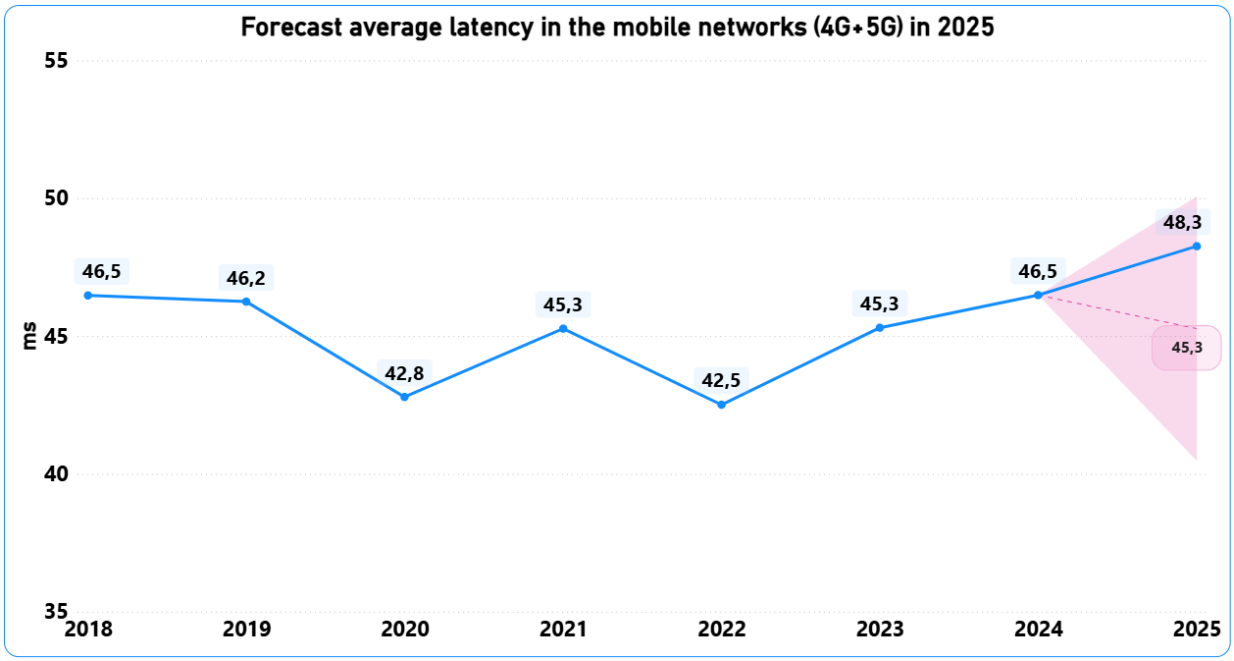

Figure 14 shows that the forecast average latency for combined 4G and 5G in 2025 was 45 ms, while the measured average value was approximately 48 ms. This indicates that latency performance in mobile networks was somewhat worse than forecast. However, Nkom has analysed the figures in greater detail by examining 4G and 5G separately. As the following figures show, results from 4G measurements largely influence the overall trend.

Figure 15 shows the values when the 4G measurements are considered separately:

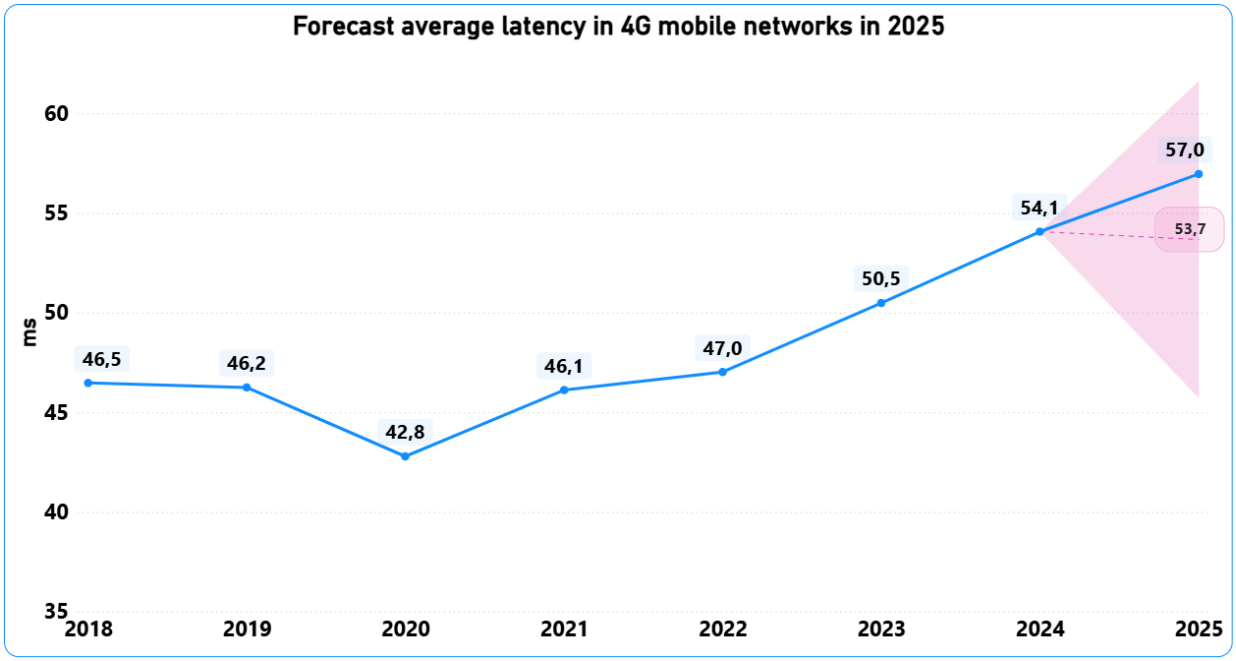

Figure 15 - Forecast for Average Latency in 4G for 2025 Forecast for Average Latency in 4G for 2025

For 4G, the results demonstrate that latency development deviates more clearly from expectations.

For 5G, the trend differs and technological differences become more apparent:

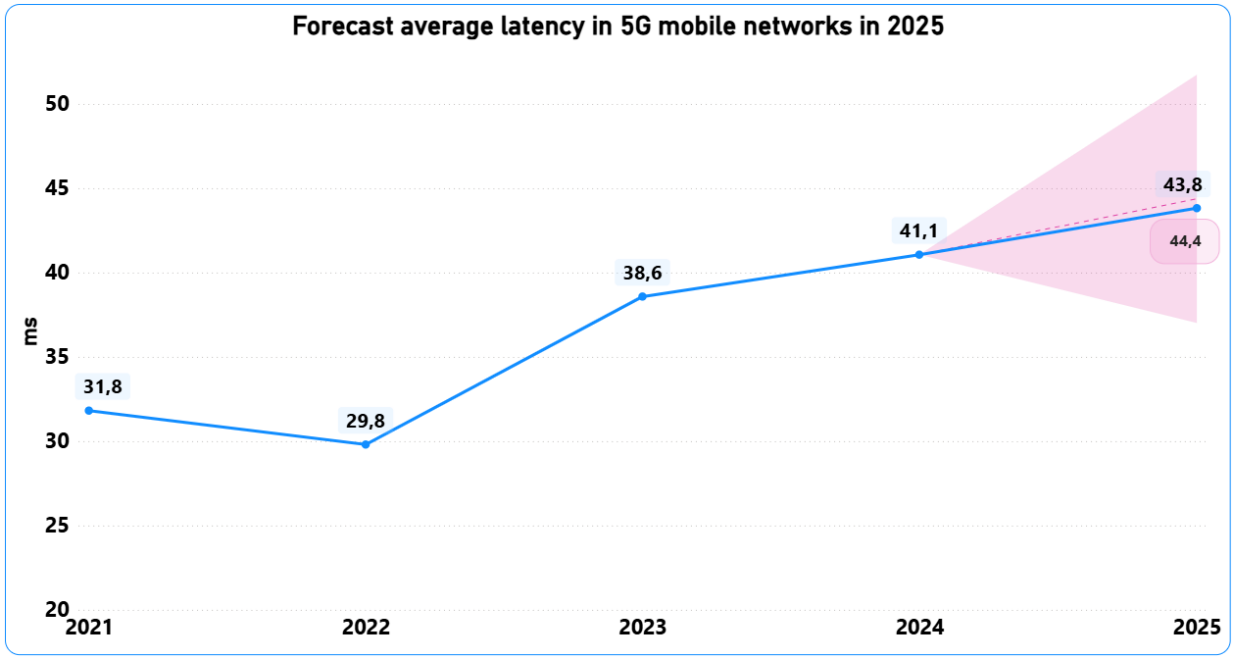

Figure 16 - Forecast for Average Latency in 5G for 2025

The measurement results shown in Figure 16 are closely aligned with mathematical expectations.

Conclusion

Nkom's analysis of measurement results from Nettfart, both via the website and the mobile

application, reveals two trends. Firstly, measured capacity in fixed networks continues to increase. Secondly, the same trend is not reflected as strongly in measurements performed in mobile networks. Given the expected continued increase in data traffic, it will be important to monitor whether mobile network operators are able to respond by continuing to expand capacity in their networks.

Over the coming years, 5G Stand Alone is expected to be introduced for ordinary smartphones, and there are significant expectations regarding the contribution this technology may make to customers' quality of experience.

4 Digital Services Act (DSA) and Nkom's Role as Digital Services Coordinator (DSC)

The Digital Services Act (DSA) regulates internet-based services and platforms, with the objective of creating a safer and more accountable digital space within the EU. The regulation is intended, among other things, to protect users from illegal content and manipulation, while also safeguarding minors using digital services. The largest online platforms are subject to particularly strict obligations. Nkom has been designated as the coordinating authority for the regulation in Norway, while the Norwegian Media Authority, the Consumer Authority, and the Data Protection Authority will each be assigned supervisory responsibilities within their respective areas of competence.

4.1 Background and Purpose – Nkom's Web Pages on DSA

Norway and the EU are currently experiencing extensive regulatory developments that will significantly influence the future of the internet. One important European legislative acts is the Digital Services Act (DSA), which was adopted by the EU in October 2022 and entered into force in November 2022. The implementation of the regulation into Norwegian law is currently in progress.

The purpose of the DSA is to ensure a safer and more transparent internet for users of online services and platforms, while strengthening the protection of users' fundamental rights. Global companies are required to provide greater transparency regarding how their platforms function, how services are delivered to users, how user information is processed, and which systemic risks the services may entail – including risks relating to freedom of expression, democratic processes, and users' safety and rights.

Further information is available on Nkom's web pages concerning safe internet use and the DSA.

4.2 Nkom as DSC

The DSA will be enforced both nationally and at the European level. Nationally, several competent authorities have been appointed with supervisory powers within their respective areas, in addition to a coordinating authority (DSC) with overall responsibility for supervision and enforcement of the DSA at national level. At the European level, the European Commission has the authority to supervise the largest online platforms and search engines (VLOPs and VLOSEs), defined as companies individually reaching more than 10 per cent of the EU population, approximately 45 million people[27]. There will also be cross-border collaboration among DSCs.

The Ministry of Digitalisation and Public Governance has appointed Nkom as the national Digital Services Coordinator (DSC) in Norway. This means that Nkom will have the primary responsibility for ensuring that internet-based services and platforms comply with the regulation, as well as responsibility for coordinating supervision. The Norwegian Media Authority, the Consumer Authority, and the Data Protection Authority have been designated as competent authorities and will each be

[27] Digital Services Act (DSA) - regjeringen.no. Cf. ch. 4.4 for further details.

assigned supervisory responsibility within their respective areas of expertise. Together with Nkom, these authorities will form the national DSA network, ensuring cooperation and coordination in the enforcement of the DSA in Norway.

Where there are grounds for suspecting that a provider in Norway has breached obligations under the DSA, Nkom or the other competent authorities may use the investigative and enforcement measures provided for in the legislation. These measures may include orders to provide information, requirements to cooperate in inspections, and requests for representatives of the undertaking to explain and account for relevant information and details concerning the matter. If, on the basis of the information gathered or other investigations, infringements of the DSA are identified, both Nkom and the other designated competent authorities may adopt decisions imposing necessary measures and sanctions within their respective areas of responsibility. Such measures may include orders to cease or modify the infringement, administrative fines, and/or restrictions on access to the service.

Nkom is subject to the authority of the Ministry of Digitalisation and Public Governance and performs its administrative functions in accordance with the Ministry's annual letter of allocation and any additional instructions and mandates issued. However, pursuant to Article 50(2) of the DSA, the DSC and the competent authorities are required to act with complete independence from other authorities and private parties. Accordingly, the Ministry may not instruct Nkom, in its role as DSC, to reach a specific outcome in complaint proceedings, to draft the annual activity report in a prescribed manner, or to prioritise particular areas of supervision.

Pursuant to Article 55 of the DSA, Nkom is required to prepare an annual activity report. The report shall include an overview of the number of complaints received and how those complaints have been handled, and it must cover the activities of both the DSC and the other designated competent authorities in Norway. The report must be submitted to the European Commission and the European Board for Digital Services.

4.3 Platform Obligations and Users' Rights

The DSA establishes several requirements for internet-based services and platforms, also referred to as intermediary services. The obligations vary depending on the type of service and the size of the platform. The regulation also applies to services offered from outside Europe, if they are directed at European users.

The regulation imposes extensive obligations on online platforms, particularly the very largest ones. All online platforms must, among other things:

- Develop effective systems to identify, report, and remove illegal content;
- Provide users with reasons when content or accounts are removed;
- Offer complaint mechanisms;
- Report on the scope of removed or modified content;
- Ensure that traders on marketplaces can be identified and traced.

In addition, the largest platforms are required to conduct risk assessments related to systemic societal risks and provide access to relevant data for authorities and researchers.

To ensure compliance with the obligations imposed by the DSA, providers of intermediary services must operate transparently and publish clear criteria explaining how content is handled. This is essential for enabling users to understand how their information and content will be processed.

When a user disagrees with a decision made by an online platform, such as the removal of content or suspension of an account, the DSA grants the user the right to lodge a complaint with the provider. Platforms are required to provide effective complaint handling mechanisms and transparent complaint procedures that are accessible and free of charge.

If a user disagrees with a platform's decision following internal complaint handling, the matter may be referred to a certified out-of-court dispute settlement body. The dispute resolution shall be out-of-court and provide a cost- and time-effective process. The dispute may concern decisions related to mattes such as removal or restriction of content, failure to remove content after notification or content considered incompatible with the platform's terms and conditions. The dispute settlement body assesses whether the platform has handled the matter in accordance with the regulation and the platform's own terms and conditions. The scheme must be affordable for users, and platforms shall normally bear the costs if the user's complaint is upheld. The dispute settlement body may be an existing entity, or a Member State may establish such a body. The body must be impartial and independent, including financially independent, from both platform providers and service recipients. Organisations wishing to operate as out-of-court dispute settlement bodies under the DSA must be certified by the DSC in their country of establishment. Certification is valid throughout all Member States. Service recipients may still bring the matter before the courts even if it has already been handled by an out-of-court dispute settlement body[28].

The DSA also grants service recipients and others acting on their behalf the right to contact authorities if they believe a provider of intermediary services has infringed the DSA. Complaints must be submitted to the DSC or competent authority responsible for the relevant area in the Member State where the service recipient resides or is established. The competent authority shall assess the complaint but retains discretion regarding how and to what extent the complaint should be followed up. If the matter falls within another authority's competence in the same Member State, the complaint shall be forwarded accordingly. Where the complaint concerns an intermediary service established in another Member State, the complaint may, where appropriate, be forwarded to the DSC in the country of establishment. A forwarded complaint of this kind may also include a statement from the DSC in the country of origin.

It is important to note that DSCs and competent authorities do not function as general appeals bodies for platforms' decisions. Their role is to assess whether platforms have complied with their obligations under the DSA, such as maintaining an internal complaints system under Article 20 or providing adequate reasons under Article 17. The DSC or competent authorities will not determine whether the actual content decision was substantively correct, but rather whether the decision-making process complied with the requirements of the DSA.

4.4 Obligated Entities under the DSA

The DSA applies regardless of where the service provider is established, provided that the service is directed at users within the EU. The DSA will also apply to Norwegian users once implemented into Norwegian law. Providers not established within the EU must appoint a legal representative in one of the Member States where the service is offered. This representative shall, inter alia, be responsible for communication with the relevant authorities, the European Commission and the European Board for Digital Services in matters relating to the receipt, compliance with and enforcement of decisions.

Recipients of services may lodge a complaint with the DSC or with the competent authority in the member state where the user is located if they consider that a provider has infringed the DSA. If the provider is established in another EU Member State, the DSC must forward the complaint to the appropriate DSC, where relevant accompanied with an assessment of the complaint.

The DSA applies to all types of intermediary service providers, not only the largest ones. However, the extent of the obligations imposed depends on the category to which the service provider belongs.

The DSA applies to all providers of intermediary services, not only the largest ones. However, the scope of obligations depends on the category of service provider.

[28] Consultation Document on Act on Digital Services - regjeringen.no, p. 19 ch. 5.4.3

The regulation distinguishes between several categories of intermediary services:

1) Mere conduit services, such as internet service providers (ISPs);
2) Caching services;
3) Hosting services.
   a) Online platforms are **one** subcategory of hosting services. Examples include online marketplaces that bring together sellers and consumers, app stores, and social media platforms. Micro and small enterprises operating as online platforms are largely exempted from heavy administrative obligations under the DSA.
      i) Very Large Online Platforms ("VLOPs") are **one** subcategory of online platforms with extended obligations.[29]
4) Very large online search engines (VLOSEs) are a distinct category of intermediary services under the DSA. They are not online platforms, but they are subject to many of the same enhanced obligations that apply to very large online platforms (VLOPs).

At the national level, it is primarily providers that fall within the first two categories of intermediary services, and providers of online platforms except VLOPs, that will be subject to supervision by Nkom and other competent authorities at national level. The obligations imposed on providers under the DSA are partly general and partly dependent on the type of service offered. The purpose of structuring the obligations in this matter is to assign providers a more active role in then handling and organization of content — such as its storage, presentation, or dissemination to users — and to impose additional and more extensive obligations than those applicable to providers engaged solely in the mere transmission of information.[30]

At the European level, the European Commission supervises the very large online platforms and search engines. These entities are subject to particularly extensive obligations relating to risk assessment, risk mitigation measures, and transparency.

These obligated entities (VLOPs and VLOSEs) have an average of 45 million or more monthly active users in the EU. Such high user numbers give rise to a particularly significant systemic risk. The European Commission has the authority to supervise and enforce the specific obligations that apply to these entities. DSCs cannot enforce these specific obligations on their own, but they may assist the European Commission by providing information and may request that the Commission investigate potential breaches of the regulatory framework. When the European Commission initiates proceedings against a VLOP or VLOSE, all DSCs are notified simultaneously and are then required to provide any relevant information they may hold in relation to the case.

As of 26 March 2026, the Commission had designated the following companies as VLOPs/VLOSEs:[31]

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	

[29] Digital Services Act - regjeringen.no

[30] Obligations on Providers - Nkom

[31] Supervision of the designated very large online platforms and search engines under DSA – European Commission

4.5 The DSA and the Government's Proposal for an Age Limit on Social Media

One example of legislation promoting the objectives of the DSA is the requirement for enhanced protection of minors. All providers of digital platforms accessible to minors must implement measures ensuring a high level of privacy, security, and safety for young users.

In addition to the DSA's protection requirements for minors, the Norwegian Government has announced that it will present a legislative proposal introducing a statutory age limit for children using social media. Prime Minister Støre stated that this represents "*an important step towards safeguarding children's digital everyday life*", and Norway will be among the first countries to introduce a statutory age limit for social media. The Government considers that the DSA provides a legal framework enabling platforms to be required to enforce national age limits, including through obligations relating to age verification and the protection of minors[32].

5 The AI Act and Nkom's Role as AI Authority

The AI Act establishes a common regulatory framework for the development and use of artificial intelligence within the EU/EEA, with the objective of ensuring safe and responsible AI. The regulation is based on a risk-based approach, imposing strict requirements on high-risk AI systems while prohibiting certain AI practices altogether. Separate rules are also introduced for the most powerful AI models, which may impose obligations on Norwegian businesses using them. Nkom has been appointed as the coordinating market surveillance authority and the national single point of contact for the AI Act in Norway.

5.1 Background and Purpose – Nkom's New Web Pages on AI

Artificial intelligence is becoming an increasingly integral part of everyday life, from digital services to healthcare and public administration. To address both the opportunities and challenges associated with AI, the EU has adopted the AI Act. This is the first comprehensive regulation establishing binding rules for artificial intelligence. The AI Act is intended to create legal predictability for affected entities in both the public and private sectors, including providers and users of AI systems. At the same time, it seeks to facilitate innovation and technological development within frameworks that safeguard fundamental societal values and rights.

The AI Act is an EU regulation that establishes legally binding rules in the EU Member States. For the EU AI Act to take effect in Norway, it must be incorporated into the EEA Agreement through Norway's forthcoming Artificial Intelligence Act. The Norwegian legislation will primarily refer to the EU AI Act while supplementing it where national discretion exists, including provisions concerning the responsibilities of national authorities relating to supervision and enforcement. The Government has appointed Nkom as the coordinating market surveillance authority and single point of contact for the AI Act in Norway.

Please see Nkom's new web pages on AI for further information.

[32] Norwegian Social Media age restrictions Law on Track to Be Introduced This Year – This Is How the Age Limit for Social Media Will Work – regjeringen.no

5.2 Risk-Based Regulation of AI

The AI Act adopts a risk-based approach whereby regulation varies depending on the level of risk posed by the AI system. Four categories of risk are established: unacceptable risk, high risk, limited risk, minimal or no risk.

1. **Systems with unacceptable risk**
   Some AI systems are considered to pose an unacceptable risk to human rights, safety, or other core societal values and are therefore prohibited from being developed or used within the EU/EEA. The prohibited AI practices are listed in Article 5 of the AI Act. The rationale behind these prohibitions is that the potential harm and ethical violations associated with the use of such AI systems are so severe that no risk mitigation measures could render them acceptable. The prohibitions include, among other things, AI systems that manipulate individuals through subliminal or deceptive techniques, exploit vulnerable groups, engage in social scoring, support certain forms of predictive policing, collect facial images through mass scraping, perform emotion recognition in workplaces and educational institutions (with certain exceptions), carry out biometric categorisation based on sensitive characteristics, and enable law enforcement authorities to conduct real-time remote biometric identification in public spaces (subject to limited exceptions).

2. **High-risk systems**
   Most of the requirements and obligations under the AI Act apply to AI systems classified as high-risk pursuant to Article 6. These systems are considered high-risk because errors, biases, or misuse may have serious consequences for individuals' lives, health, or fundamental rights. High-risk AI systems are not prohibited as such; however, their development, placement on the market, and use are permitted only if they comply with the stringent requirements laid down in the AI Act. In this respect, the AI Act follows the same principles as other product safety legislation, aiming to ensure that AI systems placed on the EU/EEA market are safe to use.

   High-risk AI systems are categorised under two separate annexes (Annexes I and III) of the AI Act, depending on whether the AI system is integrated into a safety-critical product, such as machinery, electronic communications equipment or toys (Annex I), or whether the AI system is intended for specific use cases listed in Annex III. AI systems classified as high-risk under Annex III are "stand-alone" in the sense that they are not integrated into a physical product. The use cases specified in Annex III are:

   - Biometrics
   - Critical infrastructure
   - Education and vocational training
   - Employment, workers management and access to self-employment
   - Essential private and public services and benefits
   - Law enforcement
   - Migration, asylum and border control management
   - Administration of justice and democratic processes

   There are, however, nuances and exceptions to the high-risk classification. If an AI system listed in Annex III does not, in practice, pose a significant risk of harm to the health, safety, or fundamental rights of natural persons, the provider may argue that the system should not be considered high-risk under the AI Act. In such cases, the provider must document and justify this assessment before the AI system is placed on the market.

3. **Limited Risk Systems**
   The next level in the "risk pyramid" consists of AI systems presenting what is referred to as "limited risk". Under Article 50, providers and deployers of such AI systems are subject to specific

transparency and labelling obligations relating to AI-generated or manipulated content. This is not a separate risk category, as the requirements of Article 50 may apply both to high-risk AI systems and to AI systems that are not classified as high-risk. The provision covers three main types of AI systems:

- AI systems that interact directly with natural persons
- AI systems used for emotion recognition or biometric categorisation
- AI-generated or manipulated content ("deepfakes")

4. **Minimal or No Risk Systems**
   All AI systems that do not fall within any of the categories above are regarded as presenting minimal or no risk. For such systems, the AI Act does not impose requirements relating to authorisation, conformity assessment, or labelling. They may be developed and deployed freely, provided that their use complies with other applicable technology-neutral legislation.

   Examples of AI systems presenting minimal or no risk include AI-powered spell checkers, recommendation algorithms for music and films, and AI used in certain types of games. Such systems are considered to have such limited potential for harm that specific AI regulation is not deemed necessary. For many organisations, this means that a large proportion of the AI tools they develop and use will not trigger legal obligations under the AI Act. Nevertheless, organisations should maintain an awareness of ethical considerations and potential consequences and familiarise themselves with relevant industry best practices.

5.3 Separate Rules for the Most Powerful AI Models

These large AI models often function as the "raw material" underpinning various AI systems, as they are trained on broad datasets and can be applied to a wide range of tasks. The AI Act contains a dedicated set of rules for the most powerful models, referred to as *"general-purpose AI (GPAI) models"*. These provisions were added to the AI Act during the legislative process at EU level, as the launch of ChatGPT in November 2022 highlighted the need for specific regulation of the most powerful AI models. These rules became applicable in the EU on 2 August 2025.

For Norwegian organisations, it is important to be aware that although the obligations set out in Chapter V of the AI Act are directed at providers of general-purpose AI (GPAI) models, the use of such models may also give rise to extensive obligations. This may occur, for example, where an organisation adopts a general-purpose AI model and incorporates it into its own solution. If the organisation modifies the intended purpose of the AI system in such a way that it is classified as a high-risk AI system, the organisation or actor will be regarded as a *"provider of an AI system"*. This means that an organisation that is initially only a user or integrator of an AI model may nevertheless become subject to the full set of provider obligations under the AI Act. Norwegian organisations must therefore assess not only which AI model they use, but also how and in what context it is used. Attention should be paid to whether the solution may fall within one of the high-risk categories, or whether its use involves a change of purpose that triggers more stringent requirements.

Even where an organisation is not considered a provider of a high-risk AI system, the use of general-purpose AI models may give rise to other obligations under the AI Act. Providers of AI systems that generate synthetic text, images, audio or video must ensure that the output is marked in such a way that it can be identified as AI-generated or manipulated. In addition, deployers must disclose the use of so-called "deepfakes", unless an exemption applies, for example on grounds of freedom of expression or artistic expression. In many cases, these requirements will be directly relevant to Norwegian organisations that use generative AI solutions in their services, marketing activities, customer interactions or decision-support processes.

The rules governing general-purpose AI models do not replace the obligations that apply to AI systems. When such a model is integrated into a specific application or service, it forms part of an AI system. An organisation that builds a service based on such a model will then act as the provider of an AI system vis-à-vis end users and must comply with the regulatory requirements applicable to the classification and use of that AI system. This means that the organisation must assess whether the use is prohibited, whether the AI system is classified as high-risk, and whether transparency and labelling requirements apply.

Enforcement of the rules relating to AI models is mostly centralised at EU level. The European Commission has exclusive competence to supervise and enforce these provisions, and it is the Commission's AI Office that is responsible for carrying out these tasks.

5.4 Roles and Actors

The AI Act applies to all entities developing, offering, or using certain AI systems within the EU/EEA, regardless of where the business is established.

This means that businesses outside the EU, including those in the United States and China, must comply with the regulation if their AI systems are placed on the European market.

The AI Act is largely structured as a product safety regime where the primary responsibility rests with the provider. The provider is responsible for ensuring that the AI system complies with the AI Act before being placed on the market or put into service. The regulation also imposes obligations on importers, distributors, and deployers of AI systems.

A provider is defined as a person or entity developing, or commissioning the development of, an AI system or GPAI model under its own name or trademark. Suppliers include both large technology companies that develop advanced AI models and smaller companies that create more specialised AI solutions. In some cases, other persons or entities in the AI value chain may assume provider responsibility for high-risk AI systems. A distributor, importer, deployer or other third party shall be considered a provider if that person or entity:

> a) places its name or trademark on a high-risk AI system that has already been placed on the market or put into service;
>
> b) makes a substantial modification to such a system, such that it remains a high-risk AI system under Article 6; or
>
> c) changes the intended purpose of the system — including, in the case of a general-purpose AI system — so that it becomes a high-risk AI system.

5.5 Requirements and Obligations for High-Risk AI Systems

The most extensive requirements under the AI Act apply to high-risk AI systems. The requirements cover the entire lifecycle of the system and include risk management systems, data governance and data quality, technical documentation, logging and record-keeping, transparency and information obligations, human oversight, robustness and cybersecurity.

Providers of high-risk AI systems must ensure that the systems comply with all applicable requirements. They are also responsible to carry out a conformity assessment before a high-risk AI system is placed on the market. Depending on the specific AI system, this assessment may involve either internal control procedures or an independent notified technical inspection body. Providers must also affix CE marking to high-risk AI systems. In addition, obligations relating to monitoring, reporting and cooperation with the supervisory authorities apply.

High-risk AI systems must be treated as controllable products rather than software simply released onto the market. Providers are therefore required to establish, document, and maintain mechanisms ensuring ongoing compliance throughout the system's entire lifecycle.

5.6 Sanctions for Breaches of the AI Act

The AI Act introduces new rules governing how artificial intelligence is to be developed and used in Europe. To ensure the effectiveness of these rules, a system of sanctions is also established. At the same time, there is a degree of national discretion to determine the nature of the sanctions to be included in Norway's AI Act.

The EU AI Act requires countries to establish rules on sanctions and other enforcement measures within the framework of the said act. Sanctions must be proportionate to the infringement and have a deterrent effect, while also considering the size of the undertaking concerned, including start-ups.

The EU AI Act sets maximum levels for administrative fines for certain infringements but leaves it to individual countries to determine how sanctions are organised and enforced within those limits. Each country must also establish rules specifying the extent to which administrative fines may be imposed on its own public authorities and bodies.

Regarding sanctions at EU level, it is the European Data Protection Supervisor (EDPS) that may impose administrative fines, subject to specific maximum amounts and procedural safeguards.

For providers of general-purpose AI models, the European Commission may impose fines for certain infringements, up to a maximum of 3% of global annual turnover or EUR 15 million, whichever is higher.

5.7 Interaction with Other Legislation

The AI Act must be viewed in conjunction with other relevant EU/EEA legislation concerning digital services and cybersecurity. For AI systems integrated into products or equipment, there is interaction with legislation such as the Cyber Resilience Act (CRA) and he Radio Equipment Directive (RED), in particular regarding cybersecurity requirements. AI may also form part of an organisation's broader risk profile under the NIS2 framework and must therefore be addressed within security governance and risk management processes.

The AI Act is also closely linked to the DSA, as AI is increasingly used in digital services and platforms, including recommendation systems and content moderation. In addition, access to and use of data is fundamental to the development and deployment of AI, creating close interaction with the Data Act. Nkom's dual role as both DSA Coordinator and AI authority facilitates coordinated enforcement of these regulatory frameworks.

6 Data Regulation

The Data Governance Act (DGA) has been proposed for implementation in Norway through a new Data Governance Act. A legislative proposal was submitted to the Norwegian Parliament in spring 2026, and it has not yet been decided which authority will be designated as the competent bodies under the new legislation. The Data Act (DA) is in force in the EU and is currently under consideration in the EEA-EFTA countries. The DA is intended to facilitate data sharing between entities in the European data market. The Digital Omnibus package was presented by the European Commission on 19 November 2025. The purpose of the Digital Omnibus is to simplify and harmonise existing digital regulations.

6.1 Background: A European Strategy for Data

As part of the EU's efforts to establish a common digital market, a European Strategy for Data was adopted in 2020[33]. In November 2025, the "*Data Union Strategy*"[34] was introduced under the subtitle "*Unlocking Data for AI*". However, this strategy has a much broader focus than artificial intelligence alone and represents, as the Commission itself states, a significant shift from the 2020 strategy: the focus changed "*from rules to results*". Measures such as independent cloud services have gained greater prominence in light of data becoming geopolitical assets: "*Strengthening Europe's ability to collect, curate, and use its own data is both an economic and security imperative.*"

Minister Karianne Tung participated in the launch of Telenor Sovereign Cloud in May 2026. In a press release connected with the launch, Tung stated:

> *"In a more unstable world, control over our own data and digital infrastructure is crucial. Initiatives such as this contribute to strengthening Norwegian digital sovereignty and preparedness and are fully aligned with the Government's plans for Norway."*

The EU's strategic focus on data policy has been expressed through several key legislative acts intended to facilitate greater digital autonomy in Europe, interoperability, increased data sharing, and the re-use of data. Important regulatory instruments include the Data Governance Act (DGA) and the Data Act (DA). Common to these frameworks is their close connection to electronic communications and internet and cloud architecture. Over time, Nkom has monitored developments in EU data regulation and prepared for potential supervisory responsibilities related to these regulations once implemented into Norwegian law.

The DGA and DA are discussed below in Chapters 5.2 and 5.3 respectively, before the EU's proposed simplification package within data regulation (Digital Omnibus) is described in Chapter 5.4.

6.2 Data Governance Act

The Data Governance Act (DGA) entered into force in the EU on 23 June 2022 and has applied since 24 September 2023. The DGA has been incorporated into the EEA Agreement and will eventually be implemented into Norwegian law. A legislative proposal for a new Norwegian Data Governance Act implementing the DGA into Norwegian law was submitted to Parliament in March 2026.

The purpose of the DGA is to strengthen trust in data sharing and establish mechanisms that make it easier and safer to share data. The regulation focuses in particular on the re-use of protected public-sector data, the establishment of new data-sharing intermediaries (so-called data intermediation services), and the facilitation of voluntary data sharing for purposes of general interest (so-called data altruism organisations). The regulation is therefore intended to increase the availability of data while safeguarding fundamental rights, trade secrets, and privacy.

The regulation must be viewed in conjunction with the Data Act (DA), described in ch. 6.3, as well as other digital regulations such as the Digital Services Act (DSA) and the Artificial Intelligence Act (AI Act). Furthermore, the regulation requires national authorities to designate competent supervisory authorities, including for data intermediation services and data altruism organisations. In the consultation on the proposed Norwegian Data Governance Act, conducted in 2024, Nkom recommended that this supervisory responsibility be assigned to Nkom due to its expertise in electronic communications, data, and internet architecture. As of spring 2026, no decision has been made regarding which authority will be granted supervisory competence for these services under the DGA.

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

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

6.3 Data Act

The Data Act (DA) is a key element of the EU's digital strategy and constitutes a cornerstone for the development of a common European data market. The DA entered into force in the EU on 11 January 2024 and has applied since 12 September 2025. The regulation is currently under consideration in the EEA-EFTA countries.

The regulation is designed to strengthen the EU data economy and promote a competitive data market by making data — particularly industrial data[35] — more accessible and usable, encouraging data-driven innovation, and increasing access to data. The DA is intended to serve as a legal instrument for promoting data sharing between actors in the European data market.

Core principles of the regulation include openness, data portability, and interoperability, which also create substantive links between the DA and the Data Governance Act (DGA). The European data market must also be understood in connection with the market for internet-based services and platforms, which will also be affected by the Digital Services Act (DSA), Digital Markets Act (DMA) and the Artificial Intelligence Act (AI Act).

Substantively, the regulation concerns who may benefit from data. Users of electronic communication services in the EU generate enormous volumes of data. Large data platforms, in particular, may gain advantages through data-driven feedback loops[36] and network effects. Access to data is regarded as a decisive factor in the development of future internet-based services and platforms. Easier and improved access may also increase customer mobility, improve regulation, and contribute to updated, innovative, and future-oriented public services. According to the report "*Market Study on the Norwegian Data Economy*"[37], developments in artificial intelligence have significantly increased awareness among Norwegian actors regarding the value of data.

According to the DA, supervisory authorities for the provisions within the DA on switching between data processing services (DPS) and interoperability of DPSs, must have experience in the field of data and electronic communication services. Nkom is therefore preparing for possible supervisory responsibilities under the DA. At the same time, the Body of European Regulators for Electronic Communications (BEREC) is working to obtain a role in ensuring harmonised implementation of those parts of the Data Act related to DPS. Several regulators within BEREC have already carried out substantial work concerning competition conditions and the economic and technical aspects of the DPS provisions. BEREC believes such a role could contribute to effective interaction between the Data Act and other EU digital regulations such as the Digital Markets Act and the proposed Digital Networks Act.

6.4 Digital Omnibus

The Digital Omnibus package was presented by the European Commission on 19 November 2025. Through the Digital Omnibus, the Commission proposes repealing the Data Governance Act (DGA), the Free Flow of Non-Personal Data Regulation (FFDR), the Open Data Directive (ODD), and the Platform-to-Business Regulation (P2B). Important provisions from these instruments are proposed to be transferred to, among others, the Data Act (DA). The Commission has also proposed a separate omnibus package for the AI Act (AI Omnibus).

The Digital Omnibus is a simplification and consolidation package for the EU's digital regulatory framework, in which the DA will continue as the principal legislative instrument for large parts of EU

[35] This particularly applies to connected products commonly referred to as the Internet of Things (IoT), as well as related services.

[36] A feedback loop on large internet platforms arises when users' interactions generate data that the platform can use to personalise content, which in turn influences users' behaviour and generates even more data. This can create a self-reinforcing cycle that shapes both the user experience and the content available on the platform.

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

data regulation. The aim is to reduce overlap, reporting burdens, and ambiguities while maintaining the same level of protection. The Digital Omnibus also proposes changes to the EU framework governing data storage, sharing, and re-use.

The Commission's proposal includes amendments to the following legislative acts[38]:

- General Data Protection Regulation (GDPR)
- Single Digital Gateway Regulation
- ePrivacy Directive
- Common level of cybersecurity across the Union (NIS2)
- Directive on the resilience of critical entities
- Regulation (EU) 2018/1725

The proposal also includes amendments to several provisions of the DA, particularly those concerning:

- Trade secrets in mandatory IoT data sharing between businesses (B2B) and between businesses and consumers (B2C)
- Mandatory data sharing between businesses and public authorities (B2G)
- Switching between cloud service providers (cloud switching)

The Data Act is regarded as EEA relevant, whereas the Digital Omnibus has not currently been designated as EEA relevant by the Commission.

7 Anti-Fraud Efforts in the Internet Sector

The extent of digital fraud and attempted fraud on the internet is substantial. This challenges trust in the internet as a service and as a critical national infrastructure and may inflict significant financial losses on individuals and businesses. Reduced trust in the internet may slow digitalisation and digital inclusion in society. Nkom contributes to addressing these challenges through its anti-fraud efforts and through supervision of the .no domain name administration.

The National Expert Group Against Digital Fraud consists of public and private sector entities. It is led by Nkom in partnership with National Authority for Investigation and Prosecution of Economic and Environmental Crime ("Økokrim"). The group initially focused on voice and SMS based fraud but was given a renewed mandate in December 2025 to also address fraud through internet-based services.

7.1 Background and Scope

Digital fraud is a social problem. It weakens trust in digital communications, imposes financial and emotional burdens on individuals and also supports international organised crime.

According to the Financial Supervisory Authority of Norway ("Finanstilsynet"), approximately NOK 1.2 billion was lost to fraud in 2024. During the same year, banks prevented attempted fraud amounting to nearly NOK 3 billion.[39] Globally, even more substantial sums are lost to fraud. The Global Anti-Scam Alliance conducted extensive surveys in 42 countries in 2025 and estimated annual losses at NOK 442 billion.[40]

Fraud occurs across most digital channels and internet-based platforms. Through surveys conducted by Respons Analyse, Nkom has observed a decline in traditional telephony and SMS based fraud attempts from 2024 to 2025.[41] At the same time, fraud is increasingly occurring across a wide range of internet-

[38] Digital Package - Omnibus VII presented by European Commission - stortinget.no

[39] https://www.finanstilsynet.no/publikasjoner-og-analyser/svindel-og-svindelstatistikk/2025/h1/svindelstatistikk-forste-halvar-2025/#forhindret-svindel, Table 12.

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

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

based channels and platforms, such as email, social media, online shops, and various voice and messaging services, often in combination. Fraud methods and tactics are constantly evolving.

Fraud can affect anyone. A survey conducted by Ipsos on behalf of Nkom in November 2025 showed that older individuals more frequently encounter fraud attempts through telephone calls, while younger individuals are more often targeted through internet-based platforms such as social media and gaming platforms. Those with particularly high screen time were also more exposed to fraud. The survey further showed that email is the channel through which most people encounter fraud attempts, while social media, fake online shops, and dating applications stand out as particularly high-risk scenarios for successful fraud. This demonstrates that the fraud threat is situational and that measures targeting the internet domain will become increasingly important.

Fraudsters may be large professional international criminal networks operating sophisticated "scam centres" but may also be smaller, regional organizations/networks - or individuals. International fraudsters have also used accomplices in Norway to gain access to information, bank accounts, or SIM cards.

There is no comprehensive overview of the scale of fraud within the "internet domain". However, Telenor has estimated that 70 per cent of newly created websites are fraudulent.[42] The company reports that in 2025 it carried out 2.1 billion internet-based blocks related to digital crime.[43] Various platforms and services also provide insight into the scale of fraud through public statements and reports. For example, Google has stated that in 2024 it blocked "hundreds of millions" of harmful or fraud-related search results every day.[44]

Within this context, the use of artificial intelligence has made certain fraud methods more sophisticated and credible, including through deepfake technology for video and voice, tailored and flawless texts, and misuse of information gathered from social media. Interpol estimates that AI-generated fraud is 4.5 times more profitable than traditional methods.[45]

There is a risk that the extent of AI-assisted fraud via internet-based services will increase. At the same time, AI is also actively used to combat fraud.

Loss amounts, channels, methods, scale, profiles of threat actors, and technological developments all underscore the need for increased international and national efforts to combat digital fraud as a social problem.

7.2 International Bodies and the EU Have Increased Their Focus on Digital Fraud

Interpol, Europol, UNODC, the EU, CEPT and other international bodies have in recent years intensified their focus on the global challenge posed by digital fraud. On 16–17 March 2026, UNODC and Interpol organised the first Global Fraud Summit in Vienna, attended by 1,400 representatives from relevant stakeholders. The summit resulted in a "*Call to Action on Combating Fraud*" and a "*Global Public-Private Partnership Framework against Fraud*".[46]

Industry organisations such as GSMA, i3Forum, One Consortium, the Mobile Ecosystem Forum, the Global Anti-Scam Alliance, and the Communications Fraud Control Association actively participate in international dialogue regarding the challenges posed by digital fraud.

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

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

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

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

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

Article 103 of the proposed Digital Networks Act introduces an obligation for internet service providers and providers of person-to-person communication services to cooperate with authorities in identifying effective methods for preventing fraud. It is also proposed that BEREC should issue guidance on technical and legal measures capable of protecting end users against fraud. Furthermore, the proposal introduces an independent obligation for competent authorities to implement anti-fraud measures and allows the European Commission to adopt delegated acts. This may strengthen Europe's overall resilience against digital fraud.

Nkom actively contributes to international efforts, particularly through the Numbering and Networks working group within CEPT and through BEREC working groups. Nkom also leads a global initiative, the Global Informal Regulatory Antifraud Forum (GIRAF), which includes a dedicated subgroup on fraud via internet-based services such as social media, led by the Irish regulator ComReg. However, GIRAF is a two-year project due to expire in June 2026 unless a sufficient number of regulators choose to extend the initiative.

7.3 National Efforts Against Digital Fraud on the Internet

The National Digitalisation Strategy 2024–2030[47] identifies the further development of interdisciplinary cooperation and information for citizens as measures towards 2030 aimed at preventing digital fraud. Citizens must also become more resilient against fraud through increased knowledge of common fraud methods and safe online behaviour. Nkom's vision is to ensure a safe and accessible digital everyday life for everyone, and the authority aims to be a driving force for a safer internet. Nkom's anti-fraud work within the internet domain is a natural operationalisation of these strategic priorities.

Efforts against internet fraud consist of a complex ecosystem of public and private sector stakeholders and remedies. Police, financial institutions, electronic communications providers, consumer authorities, and security authorities are among those actively contributing within their respective sectors. Cross-sector cooperation is, however, becoming increasingly important.

Several regulatory frameworks are relevant to combating digital fraud, including regulations concerning electronic communications (including the Open Internet Regulation) privacy, artificial intelligence, marketing, domain names, criminal law, and finance. Nkom's "*Discussion paper on DNS-based security measures*"[48] from 2021 is also relevant. Once the Digital Services Act (DSA) and its associated supervisory structure are implemented into Norwegian law, this will also become an important instrument defining which measures are expected from, among others, global platforms. Fraudulent content will typically qualify as "illegal content" under the DSA, which may affect risk assessments, transparency obligations, notification mechanisms, and reporting.

Norid administers the Norwegian country code top-level domain .no and has established routines and rules for domain name registration. This has contributed to .no becoming regarded as a "good neighbourhood" on the internet, with relatively limited levels of fraud compared with other top-level domains. Although fraud also occurs under .no, the general picture is positive. This is supported by the fact that .no is ranked by Global Signal Exchange as the top-level domain with the fewest reports of abuse worldwide.[49]

Norid operates within frameworks established by the Electronic Communications Act and the Domain Regulation. Norid determines allocation rules within the framework of the regulation, while Nkom supervises compliance with these provisions. Norwegian domain names may also be seized by the police pursuant to criminal procedural law.

Finans Norge ("*Finance Norway*") is the trade organisation for the Norwegian financial industry and represents around 315 financial enterprises. Finans Norge works actively against fraud and has

[47] "The Digital Norway of the Future", Ministry of Digitalisation and Public Governance, Nov 2024

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

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

established, among other initiatives, a specialist anti-fraud committee for banks (FAB), the information website svindel.no, and recommendations for 16 anti-fraud measures.[50]

In 2025, the police established a digital reporting solution for fraud and scam cases. This may provide improved situational awareness and a better overview of the scale and development of fraud.

Nkom has conducted — and will continue to conduct — active information campaigns across various channels to strengthen the population's ability to defend itself against digital fraud. Information and knowledge sharing, being central to society's efforts against internet fraud, are also undertaken by several other public and private entities. For example, The Norwegian Consumer Council and the Norwegian Consumer Authority provide guidance on avoiding online fraud through their websites. Advice and guidance on digital security are also available at www.sikkert.no, a national portal developed through cooperation between The Norwegian National Security Authority, The Norwegian Digitalisation Agency (DigDir), the police, and The Norwegian Data Protection Authority. Several electronic communications providers also carry out active consumer information campaigns. The Norwegian Business and Industry Security Council particularly focuses on the business sector and has established its own Cyber Security Centre.

Cooperation and information sharing are becoming increasingly important. Several positive collaborative initiatives have already been launched, both internationally and nationally. For example, on 18 March 2026 the Norwegian Government, through the Ministry of Digitalisation and Public Governance, organised a high-level meeting among key stakeholders on how online fraud can be more effectively prevented and combated.[51]

The National Expert Group Against Digital Fraud was established by Nkom in 2023 in partnership with Økokrim[52]. The group has members from both the public and private sectors, including the three operators Telenor, Telia and Ice/Lyse, NRDB[53], The Norwegian National Security Authority (NSM), The Norwegian Business and Industry Security Council (NSR), Finance Norway, The Norwegian Digitalisation Agency (DigDir), the Financial Supervisory Authority and Stø AS[54]. Nkom leads the group, which in December 2025 received a renewed and expanded mandate for a further two years. The group will also address fraud through internet-based services and vulnerabilities and measures at the intersection between banking and electronic communications. The mandate further stipulates that if no participant has concrete ownership of a proposed solution, the group may, as a national resource, formulate problem descriptions for submission to relevant national or international entities.

The National Criminal Investigation Service (Kripos) stated in *Cyberkriminalitet 2025*[55]:

> *"It is highly likely that criminals will continue to exploit the gap between rapid technological development and society's slower ability to develop effective countermeasures."*

In light of this, shared situational awareness, cooperation, data sharing, and regulatory development will be important success factors in anti-fraud efforts relating to the internet domain.

Going forward, effective combatting of digital fraud will increasingly require cooperation across sectors and may involve stakeholders such as internet service providers, domain name administrators, internet-based platforms, banks, payment intermediaries, electronic communications providers, as well as Nkom and the police.

---

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

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

[52] National Authority for Investigation and Prosecution of Economic and Environmental Crime

[53] The industry owned company operating the National Reference Database (NRDB) for ported telephone numbers

[54] A company owned by 104 banks, providing the two leading services in Norway on electronic identification and electronic payments.

[55] Cyberkriminalitet 2025 - National Criminal Investigation Service (Kripos)

8 International Internet Governance

International internet governance reached an important milestone at the turn of the year 2025/2026. Norway hosted the 20th annual international meeting on internet governance in June 2025 (IGF 2025), and in December 2025 the United Nations General Assembly adopted a resolution to continue international cooperation on internet governance (WSIS+20).

In 2026, two parallel processes within international internet governance will contribute to the further development of the field. At the end of April, a new application round for generic top-level domains within the DNS was opened by the internet governance body ICANN. In October, the Plenipotentiary Conference of the UN agency ITU will take place, with key internet-related issues on the agenda.

8.1 Background

Internet governance is a field encompassing the establishment and application of principles, norms, rules and decision-making procedures that shape the development and use of the internet. International internet governance follows several parallel tracks. This has implications for how governments and other stakeholder groups may engage in the field, and it influences how the internet plays a central role in geopolitical developments.

Nkom supports the Ministry of Digitalisation and Public Governance (DFD) in Norway's participation in international internet governance through organisations such as ITU and ICANN to safeguard Norwegian interests. Nkom works in line with the Government's objective to[56]:"*.. participate actively in the debate on the development of the internet and, through the electronic communications authority, participate in international organisations working on internet governance, the further development of internet technology and internet architecture.*"

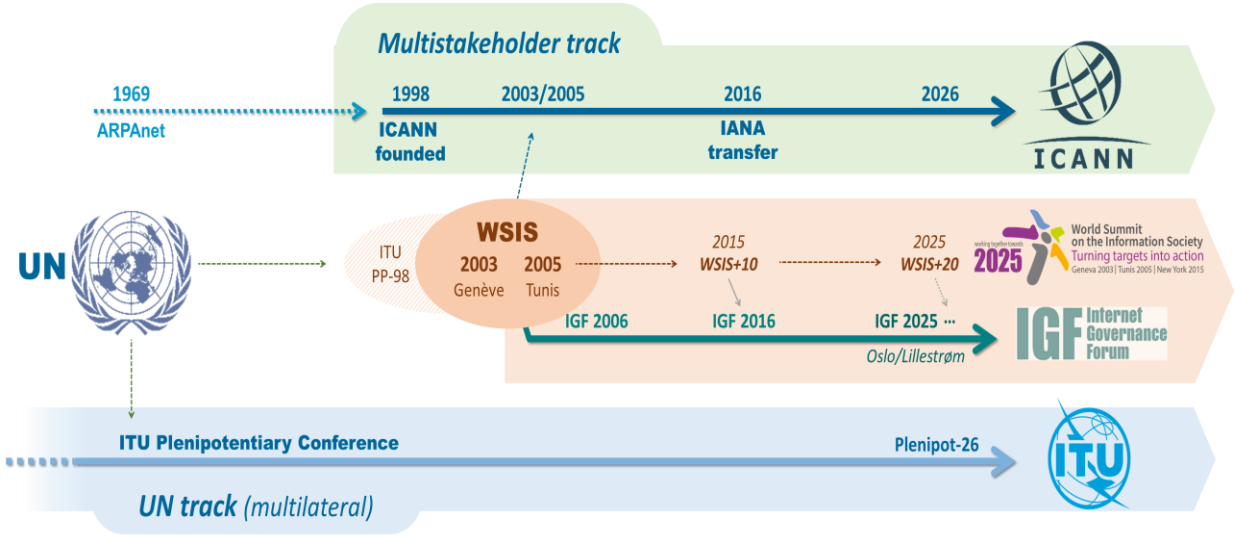

Figure 17 Internet governance unfolds along parallel tracks: The multistakeholder track and the multilateral UN track.

On the one hand, the internet may be regarded as an electronic communications network comparable to more traditional telecommunications networks. This forms the basis of the UN track in internet governance, which is based on a "**multilateral governance model"**. Historically, the establishment of electronic communications infrastructure was the responsibility of national authorities, which organised international cooperation within the UN body ITU (International Telecommunication Union).

[56] Report to the Storting (*White Paper*) No. 28 (2020–2021): *"Our Shared Digital Foundation – Mobile, Broadband and Internet Services"* (In Norwegian only)

As internet technology has gradually been adopted for electronic communications services, internet governance has become a key issue for ITU.

On the other hand, the internet originated as a research network established by the United States government. As the network expanded both within the US and internationally, internet governance was organised by US institutions. When the internet grew into a global communications network during the 1990s, the need to internationalise its governance increased. Through a comprehensive multi-year process, responsibility for internet governance was formally transferred in 2016 from the US to the international organisation ICANN (Internet Corporation for Assigned Names and Numbers).

A key prerequisite for the internationalisation of ICANN was the organisation's bylaws, which ensure that it operates according to the "**multistakeholder model**". This forms the basis of the multistakeholder track within internet governance, see Figure 17 above. Governments, private sector, civil society, technical community and academia are key stakeholder groups within this model. In summary, the UN track may be regarded as representing the continuous development of traditional telecommunications over the past 150 years, while the multistakeholder track focuses on the disruptive transformation that the internet has brought to electronic communications during recent decades.

International internet governance became established within these two tracks through the UN process WSIS (World Summit on the Information Society). Two WSIS meetings were held in 2003 and 2005, and the final communiqué from WSIS 2005 ("Tunis Agenda") remains a foundational document for internet governance work. One important outcome of the WSIS process was the establishment of the IGF (Internet Governance Forum), which may be viewed as an "intermediate track" linked both to the UN system including ITU and to the multistakeholder model (like ICANN).

Within the tension between the traditional multilateral UN track centred on ITU and the newer multistakeholder track centred on ICANN, key geopolitical processes as presented in the following subchapters continue to unfold.

8.2 IGF 2025 in Norway

Once a year, participants from all over the world gather for the IGF meeting. This has continued since the first IGF meeting held in Athens in 2006. Norway hosted IGF 2025 in Lillestrøm[57]. This was the 20th IGF meeting. IGF is a global forum for dialogue on internet governance based on the mandate established in the "Tunis Agenda". At the annual meetings, key issues related to emerging technologies and critical infrastructure are placed on the agenda. Participants contribute to information sharing and competence-building across sectors of society. IGF develops recommendations, but it does not adopt binding decisions.

Norway's candidacy as host country for IGF was announced by Minister of Foreign Affairs Espen Barth Eide with the following statement: "A free and open internet is fundamental to democracy, human rights and freedom of expression. International cooperation to ensure that the internet remains a safe and inclusive arena for everyone is more important than ever before. Norway wishes to contribute to this." The national digitalisation strategy further states that it is important that Norway "takes greater responsibility in the continued development of the internet. Norway shall contribute to safeguarding long-term strategic interests in global internet governance and help set the agenda on issues of major importance."

The implementation of IGF 2025 in Norway received broad support. UN Secretary-General António Guterres stated: "I am pleased to participate in this year's IGF – and thanks to Norway for hosting. This year, the forum has worked for twenty years to promote inclusive cooperation on internet policy". Prime Minister Jonas Gahr Støre expressed it this way: "Technology must go hand in hand with a

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

human touch. I have no doubt that this conference will provide valuable insight, proposals and recommendations that can guide internet policy and practice for the benefit of all."

The topics addressed at IGF meetings cover a broad spectrum. The internet ecosystem is an interaction between the internet's communications infrastructure (often referred to as the "network layer" or "technical layer") and the content and services conveyed across this infrastructure (often referred to as the "application layer"). Current issues include the domain name system, internet security, net neutrality, data governance, the role of platforms, artificial intelligence, the risk of internet fragmentation, democracy and freedom of expression.

One of the sessions organised by Nkom at IGF 2025 was entitled *"Building trust and combatting fraud in the internet ecosystem"*[58]. The session examined how trust in internet communication and online content can be maintained in a situation where a quarter of the world's population has lost money due to fraud. Many fraudulent attempts involve social engineering, phishing and identity theft. Measures to counter these threats range from establishing legislation and institutions to protect users, to educating citizens so they become more resilient against fraud through greater awareness of online safety.

IGF 2025 also served as part of the preparations for WSIS+20 later in the year, including discussions relating to the multistakeholder model. The session *"Multistakeholder Perspectives: WSIS+20 & the Technical Layer"*[59] discussed the importance of the multistakeholder model for maintaining a secure, stable and open internet. The model facilitates cooperation on equal terms between different stakeholders, including governments, private sector, civil society, technical community and academia. Both the Norwegian representative and several other panellists emphasised the importance of ensuring that decisions concerning internet governance are made based on an understanding of the technical implications for the internet's architecture. Avoiding fragmentation and centralised control is essential to preserving the internet's global and open architecture.[60]

At the high-level closing session, *"Charting the Path Forward for the WSIS+20 Review and Role of the IGF"*, Minister of Digitalisation Karianne Tung summarised Norway's position as follows: "*I believe that over the past twenty years we have demonstrated that IGF and the multistakeholder model can be trusted. Therefore, it is important for Norway – indeed it is Norway's view – that IGF should receive a strengthened mandate, become permanent, and that we should be able to integrate the different processes more effectively.*"

8.3 WSIS – The 20-Year Milestone

IGF was established as an international meeting place for internet governance through the WSIS meetings in Geneva in 2003 and Tunis in 2005. At the Tunis meeting, a key issue was the future role of ICANN as the global coordinator for the allocation of domain names and IP addresses. At the time, ICANN remained under US government oversight, although with the aim of becoming internationalised.

At the beginning of the WSIS+20 negotiations in 2025, there was significant uncertainty regarding the future direction of internet governance. The geopolitical debate that began in 2003–2005 and has continued ever since, had demonstrated that establishing an open multistakeholder approach to internet governance requires active engagement from all stakeholders contributing to the shaping of the internet's future.

At the Tunis meeting in 2005, some countries argued that internet coordination functions should be organised under multilateral governmental control and placed within ITU. Other countries, together

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

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

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

with representatives from civil society, the technical community and academia, warned that greater state control could threaten the openness of the internet, while also acknowledging shortcomings in ICANN's existing governance structure. Human rights advocates also expressed concern that governance through a multilateral body might restrict freedom of expression.

It proved difficult to reach agreement on how to resolve these disagreements, and the issue remained unanswered in the final resolution, "*The Tunis Agenda*"[61]. Consequently, ICANN's role remained unchanged through the WSIS process, and the parallel tracks of international internet governance continued. Another aspect of the compromise was the establishment of IGF as a global platform for dialogue on internet governance. In the final communiqué, IGF was granted a time-limited mandate. In 2015, this mandate was extended for a further ten years (WSIS+10).

The WSIS+20 negotiations began in June 2025, and consensus was achieved after six months. The final resolution[62] contains several elements reflecting the original WSIS vision. Paragraph 1 refers to international law and human rights, paragraph 2 reaffirms the Tunis Agenda, and paragraph 3 recognises the multistakeholder model as central to the development of the information society. Regarding the recurring question of extending IGF's mandate, substantial progress was achieved as IGF was granted a permanent mandate.

In a press release from the Ministry of Digitalisation[63], it was stated that: *"The United Nations General Assembly reached agreement on a joint final declaration and a permanent mandate for IGF – the UN's leading forum for dialogue among all relevant stakeholders concerning the future of the internet. This was decided at a summit in New York, where Norway was one of the countries supporting the principle that the internet should remain democratic, free and open to everyone."*

However, the issue of future financing for IGF remains unresolved. The UN Secretary-General is expected to present a proposal to the UN General Assembly to secure sustainable financing for the forum. Another unresolved issue is that although the multistakeholder model has been consolidated, some countries continue to advocate a stronger governmental role within the model ("top-down"), while others believe governments should hold an equal role alongside the other stakeholders ("bottom-up").

The debate between multilateralism and multistakeholderism is therefore far from settled. This continues to be reflected in the way the WSIS process unfolds within the UN system. For much of the process, it functions as a genuine multistakeholder process, where governments work together with the private sector, civil society, the technical community and academia in open dialogue. Yet in the final phase, negotiations revert to a closed multilateral UN process conducted exclusively between governments.

8.4 ICANN Opens Application Round for New Top-Level Domains

The internet's global communications service depends upon coordination of core internet functions such as addressing and routing of network traffic and the naming functions of the domain name system (DNS). ICANN's role is to maintain a consistent and stable set of globally unique identifiers (domain names and IP addresses) that make communication possible across the networks constituting the internet. This part of internet governance is sometimes referred to as "technical internet governance".

As described above, ICANN is based on the multistakeholder model. Any weakening of this model risks sidelining the technical community and introducing geopolitical influence into decision-making in ways

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

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

[63] Broad Consensus in the UN on the governance of the future internet, DFD, 19 December 2025, press release (Norwegian)

that could undermine the maintenance of an open and interoperable internet. In this respect, ICANN plays a particularly important role.

ICANN has evolved since its establishment in 1998. For many years there was disagreement between different countries concerning ICANN's role. In 2016, however, ICANN's formal status changed when the US government relinquished its oversight role and transferred it to the international multistakeholder community through an agreement with ICANN. An important aspect of this change was the transfer of the "IANA function". The Internet Assigned Numbers Authority (IANA) function manages the registry of domain names, IP addresses and other identifiers used on the internet.

In 2026, the application round for new generic top-level domains[64] will be at the top of ICANN's agenda. This is the second such application round in history. The first round took place in 2012 and led to a significant increase in the number of top-level domains after more than a thousand applications were submitted. The application process will remain open from 30 April until 12 August this year. The domain names applied for will then be published in October ("Reveal Day"). Following a period allowing applicants to adjust the domain names, the final list of top-level domains applied for will be published in November ("Confirmation Day").

A comprehensive process within ICANN will then begin, expected to continue for several years, much like the 2012 round. Within ICANN, governments are organised within the Governmental Advisory Committee (GAC), which may play a central role during the application round. Individual GAC members may submit objections to top-level domain applications through "GAC Early Warnings", while GAC collectively may issue "GAC Consensus Advice". Such objections will subsequently undergo formal processes within ICANN before ultimately being either dismissed or upheld.

Another long-running issue within ICANN concerns adapting WHOIS to GDPR and other privacy regulations[65]. WHOIS is a global distributed database containing information such as the holders of domain names, and these data were originally publicly accessible. The register is, among other things, an important tool in combating crime. When GDPR entered into force in May 2018, it triggered a process within ICANN aimed at bringing WHOIS into compliance with privacy rules. Some WHOIS data were consequently hidden from public access, and a pilot service for legitimate requests concerning protected registration data was established, for example for law enforcement authorities.

A relatively new issue within ICANN is the "Review of Reviews", which relates to protecting the multistakeholder model within the organisation. ICANN's bylaws include provisions for a series of regular audits intended to ensure that the organisation operates in accordance with its objectives. In recent years, however, it has become apparent that the organisation has fallen behind in this work, with new audit rounds beginning before previous ones have been completed. ICANN is therefore exploring ways to adjust the audit system to make it more manageable without undermining the purpose of the audits.

8.5 Plenipotentiary Conference 2026 of ITU approaching

Traditional telecommunications existed long before the internet, and international telecommunications governance has been organised by the UN agency ITU. As the internet has gradually become society's most important communications service, ITU has increased its activity relating to internet issues. The Plenipotentiary Conference (commonly referred to as "Plenipot") is ITU's highest decision-making body. It is held every four years, and the next conference will take place from 9–27 November this year[66].

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

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

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

Discussions concerning the role of the multilateral UN track represented by ITU, versus the multistakeholder track represented by ICANN, occasionally surface during ITU meetings under the term "New IP". The clearest example of this debate occurred in 2019, when Chinese delegates to ITU proposed establishing an alternative standardisation framework for the IP technology used on the internet, within ITU. Since the internet's inception, however, standardisation of IP technology has been carried out within the IETF (Internet Engineering Task Force), which is based on the multistakeholder model.

A report prepared for the European Parliament[67] explains that, according to the Chinese representatives, "*the current IP design is not efficient enough to support technologies such as holographic communication or autonomous vehicles.*" The report further states that "*the Chinese proposal generated mixed reactions from the international community. Iran, Russia, Saudi Arabia and several African countries supported the proposal, while Western countries such as the United States, the United Kingdom, the EU and civil society expressed concern.*"

Following intense debate, however, the Chinese proposal failed to gain sufficient support. Nevertheless, the undercurrent towards shifting the centre of gravity for internet governance and standardisation under the ITU umbrella has not disappeared. In 2022, a similar proposal was presented by Chinese representatives under the designation "IPv6+". The IETF is already conducting standardisation work that continuously evolves the IP technology, including design requirements like those envisioned in "New IP"[68].

Any fragmentation of the standardisation processes governing internet technologies would create a major risk of internet fragmentation, which would conflict with the objective of preserving an open and interoperable internet. Western countries therefore place considerable emphasis on closely monitoring developments within ITU to encourage greater openness and broader participation more closely aligned with the multistakeholder model.

At this year's Plenipotentiary Conference, there is once again considerable anticipation regarding how discussions surrounding internet-related resolutions will unfold. Two key resolutions are "*IP-based networks*" (Resolution 101) and "*International public policy issues pertaining to the Internet*" (Resolution 102). These resolutions are typically revised every four years during plenipotentiary negotiations[69].

Resolution 101 addresses issues such as interoperability of IP technology, strengthening internet participation in the Global South, and cooperation with other standardisation organisations including the IETF. Resolution 102 covers topics such as governance of domain names and IP addresses, as well as ITU's role in facilitating international dialogue on internet-related public policy issues.

ITU's Plenipotentiary Conference in November will be influenced by the WSIS+20 outcome, but naturally also by ongoing technological, economic and political developments. We live in a period of rapid change, and this forms an important part of the backdrop to the forthcoming conference. This year's Plenipotentiary Conference may prove at least as eventful as previous conferences.

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

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

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