
Nasjonal kommunikasjons-myndighet

# Internet in Norway – Annual Report 2023

June 2023

# Summary


Part 1 of the report describes the status of net neutrality in Norway. Annual reporting on net neutrality is a statutory task for Nkom based on the Open Internet Regulation.

Part 2 describes the status of the core functions of the internet in Norway, and covers a) infrastructure and traffic development, b) regulatory development and c) a description of the geopolitical picture.

### *1) Status of net neutrality in Norway*

Nkom observes that the status of net neutrality in the Norwegian market is generally good.

BEREC's net neutrality guidelines were updated during the reporting period and specify that zero-rating of selected content do not comply with the requirement for equal treatment of traffic on the internet access service. Telenor and Telia therefore withdrew their "Music Freedom" zero-rating offer from the market at the end of 2022.

With regard to traffic management, this year Nkom has focused on fixed wireless internet access and the offer of TV and video streaming in parallel with this form of internet access. At this year's dialogue meetings concerning net neutrality, however, it emerged that these parallel services are treated in the same way as internet traffic.

In its work on the report, Nkom has not uncovered any breaches of the rules concerning transparency about the internet access service. However, the way providers offer information varies, from dedicated webpages to fragmented information distributed across different webpages. Nkom encourages providers to make the information as easily accessible as possible to their customers.

Regarding the quality of the internet access service, the measurement results from Nettfart show that the rising performance trend is continuing. For fixed internet access, the speed has increased by 12% since the previous reporting period. For mobile networks, Nkom observes that measured speed shows better development than the forecast expected in the general quality of the internet access service.

### *2) Core functions of the internet in Norway*

#### *a) Infrastructure and traffic development*

In the first half of 2022, respectively 94% and 93% of Norwegian households were offered internet access with at least 100 Mbit/s and 1000 Mbit/s in download speed. The development in Norwegian internet traffic shows annual growth of around 20-30% in both fixed and mobile networks. Streaming services are the biggest traffic driver, accounting for around 70% of network traffic.

*Adoption of IPv6*

In April 2023, Norway ranked 24th in the world in terms of IPv6 adoption, up 11 places from last year. In the course of one year, IPv6 adoption in Norway increased from 24% to 36%. At European level, Norway advanced four places from last year, up to 10th place.

In the spring of 2023, Nkom held dialogue meetings concerning IPv6 with the largest internet service providers in the Norwegian market, to stimulate the transition from IPv4 to IPv6. Nkom presented a proposal for an escalation plan for IPv6, with the aim that Norwegian internet service providers gradually increase the activation of IPv6 for all their subscribers towards 2025. The Norwegian internet service providers have stated that in many ways, they are in line with this proposal.

*Internet interconnection in Norway*

Most of the interconnection between Norwegian internet service providers is geographically centralised in Oslo, at private interconnection points. In addition, NIX's public interconnection points are used in Oslo, Stavanger, Bergen, Trondheim and Tromsø respectively.

All the major internet service providers in Norway today have CDNs in place from operators such as Akamai, Apple, Facebook, Google, Microsoft and Netflix. The internet service providers report that caching efficiency is 75-90%.

Most of the international internet traffic is conveyed via the international transit providers Arelion and Lumen, and the major Norwegian internet service providers Telenor, Telia, GlobalConnect and Altibox.

### *b) Regulatory development*

There is extensive development of European legal acts and national legislation that will greatly influence the internet of the future. If the regulatory development is to benefit internet users, it is vital to ensure the effective exercise of authority at international and national level. To that end, Nkom expects to play an active role as national regulator of electronic communications.

The Digital Services Act (DSA) and the Digital Markets Act (DMA) came into force within the EU in November 2022. This legislation regulates end-users' rights on the internet and the competition between the largest internet-based platforms, respectively. The legislation is the first of its kind in the world, and the goal is to reduce the platforms' dominant position.

Developments in artificial intelligence made great progress during the past year. EU lawmakers have realised that the time has come to establish legislation to regulate the use of this technology, for the benefit of society. The development of the Artificial Intelligence Act (the AI Act) has accelerated, and formal approval of the regulation is expected by the end of 2023.

Internet-security related regulation is also further developed during this period. In September 2022, the European Commission presented a proposal for regulation of security of internet-connected equipment (CRA), which is likely to replace the safety requirements under the Radio Equipment Directive. In December 2022, the updated Directive on Security of Networks and Information Systems (NIS2) was adopted by the EU, and in 2024 will replace the current NIS directive.

### *c) The geopolitical picture*

In 2021/2022, the members of ETNO (European Telecommunications Network Operators' Association) launched the "fair share" initiative proposing that large platform providers should pay more for interconnection with internet service providers. The European Commission's consultation on this issue could take the debate a step further. In the spring of 2023, Nkom held dialogue meetings with the major Norwegian internet service providers, and the results from this showed that the status of the Norwegian market is more reconciled, and that today's interconnection regime functions with relatively few conflicts.

The internet infrastructure and the internet ecosystem are exploited for security attacks, digital sabotage and impact operations, and play an important role in a global security policy context. From the war in Ukraine, for example, we have seen rerouting of internet traffic in occupied areas, and how DDoS attacks against Norwegian targets have been used by pro-Russian hackers to generate media attention in Norway. For its part, the Norwegian government has implemented several measures to strengthen national control and digital resilience in the face of an escalating threat picture.

The green and digital future, also referred to as the twin transitions, reflect the upheavals currently taking place and that together could help reduce global greenhouse gas emissions by up to 20% before 2050. For this to be achieved, the technology must be connected to the internet in some form or other. The EU and the UN, among others, emphasise the importance of understanding the connections between digitalisation and sustainability, in terms of own emissions, as well as the benefits that can be reaped in the green and digital future.

# Contents

# 1 Status of net neutrality in Norway

Nkom observes that the status of net neutrality in the Norwegian market is generally good. The information basis for this year's report shows only minor changes compared to the previous year.

With regard to traffic management, parallel services such as TV and video streaming are treated on a par with internet traffic, including for fixed wireless internet access.

Internet service providers provide satisfactory transparency about speed and other relevant parameters, and actively follow up the regulatory developments in this area.

Concerning the quality of the internet access service, the measurement results from Nettfart show a favourable trend of rising average speeds for both fixed and mobile internet access.

## 1.1 Introduction and background

Part 1 of the Annual Report describes the status of net neutrality in Norway. This is the second year in which net neutrality reporting is included in a broader report on the status of the internet in Norway. Net neutrality is the principle that all internet communications must be treated equally, regardless of sender, recipient, equipment, application, service or content. This report covers the period from 1 May 2022 to 30 April 2023.

Net neutrality was codified by law in Norway with effect from March 2017[1] in connection with the introduction of European Open Internet Regulation.[2] The aim of the Regulation is "to establish common rules 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."[3]

Nkom also bases the regulatory assessment of net neutrality on BEREC's Open Internet guidelines, which have been established pursuant to Article 5(3) of the Regulation. According to recital 19, the national regulatory authorities must "take utmost account" of relevant guidelines from BEREC in their application of the Regulation.

*Regulatory development*

BEREC's Open Internet guidelines were updated in the course of this reporting period based on three judgements from the European Court of Justice concerning zero-rating. Zero-rating means that the traffic from selected websites is not deducted from the data allowance for the internet subscriptions; in other words that the price rate for this traffic is zero. The main change in the guidelines is that zero-rating of selected content do not comply with the requirement for equal treatment of traffic on the internet access service. The updated guidelines were launched in June 2022.

In dialogue meetings, Nkom has informed the industry about the consequences of the court decisions and the updated guidelines from BEREC. Telenor and Telia therefore withdrew their "Music Freedom" zero-rating offer from the market as of 31 December 2022. Nkom furthermore assumes that zero-

[1] The Norwegian Electronic Communications Act, section 2-16, Act relating to electronic communications (the Norwegian Electronic Communications Act) – Part 2. General provisions – Lovdata.

[2] Regulation 2015/2120, EUR-Lex – 32015R2120 – EN – EUR-Lex (europa.eu).

[3] First recital of Regulation 2015/2120.

rating services of the same nature as those ruled to be illegal by the European Court of Justice are not offered.

*Content of the Annual Report*

Part 1 of the Annual Report has the following structure: Chapter 1.1 presents the status of net neutrality and describes the regulatory development during the past year, including the status of zero-rating offers in the Norwegian market. Chapter 1.2 describes an updating of conditions related to technical traffic management in Norwegian internet service providers' networks. Chapter 1.3 describes how Norwegian providers communicate information about the internet access they offer. Chapter 1.4 describes the quality achieved for Norwegian internet access services, analysed on the basis of measurements using Nkom's Nettfart measurement tool.

## 1.2 Open internet access

Nkom's collection of traffic management information from internet service providers shows no significant changes compared to last year in terms of the internet access service, as well as the provision of specialised services in the market. This year, Nkom has focused on fixed wireless internet access and the TV and video streaming applications offered as a package together with this type of internet access. At this year's dialogue meetings concerning net neutrality it emerged that these supplementary services are treated on a par with internet traffic.

### 1.2.1 The right to an open internet access service

End-users have the right to an open internet access service, where they can determine for themselves what the access is used for, in terms of which content is retrieved or delivered, and which applications are used or offered, based on Article 3(1) of the regulation. The internet service provider must transmit traffic in the network on a non-discriminatory basis, but has the opportunity for certain forms of traffic management, such as blocking traffic for security reasons.

Internet service providers may also offer specialised services, such as Voice over IP and IPTV, in parallel with internet access service, if these are subject to quality requirements that cannot be offered via the internet. Furthermore, specialised services may only be provided if the network capacity is sufficient to avoid degradation of the availability and general quality of internet access services for end-users (see Chapter 1.4).

### 1.2.2 Traffic management of internet access

As part of the data collection for the annual electronic communications statistics, Nkom obtained information from Norwegian internet service providers concerning the traffic management of internet access. The results for this year do not differ significantly from the results for last year.

According to the information obtained, typical traffic management measures include the blocking of domain names in DNS pursuant to a judicial order, the Kripos Child Abuse Filter, and blocking of TCP/UDP ports in connection with specific security measures (for example, to prevent DDoS (Distributed Denial of Service) attacks and other types of cyberattacks).

In the Norwegian market, speed-differentiated mobile internet access is offered. In its guidelines, BEREC describes how such subscriptions are in line with the regulation for as long as the subscriptions are application-agnostic, which means that all applications are treated equally.

### 1.2.3 Specialised services

Nkom has also collected information about specialised services, i.e. other services offered in parallel with the internet access service that fulfil specific criteria in the regulation. The most typical specialised service in fixed networks is Voice over IP. Similarly, VoLTE is commonly offered as a specialised service in mobile networks.

Nkom also asked how the providers ensure that the network capacity is sufficient to ensure that the specialised services are not to the detriment of the general quality of the internet service for end-users. The general response to this is that the traffic at the connections in the network is monitored continuously, and that capacity is expanded as needed.

Nkom has not undertaken more detailed assessment of the reported traffic management measures and specialised services, but assumes that these are provided in accordance with the regulation. In the future, Nkom will be able to initiate more detailed investigation of the measures.

### 1.2.4 Fixed wireless internet access

Fixed wireless internet access (FWA) was introduced in the Norwegian market in 2020, (see below about the speed of such services), and during 2021 Norwegian internet service providers launched TV and video streaming as bundled offers together with this form of internet access service.

In this context, it is relevant to assess whether these additional services are treated on a non-discriminatory basis on the broadband access to subscribers. At this year's dialogue meetings concerning net neutrality held by Nkom with the three Norwegian mobile network operators, it emerged that these supplementary services are treated on a par with internet traffic.

### 1.2.5 Net neutrality and security

Here, Nkom refers to the security exemption in Article 3(3)b of the Regulation, which states that traffic management measures beyond reasonable traffic management are not permitted, unless necessary to protect the security and integrity of the network. The application of the exemption must be based on a "strict interpretation" and relevant measures may not take place for longer than necessary. The exemption is further clarified in BEREC's guidelines (sections 83-87) and Nkom published a policy paper on net neutrality and security in November 2021.

On preparing the Annual Report, Nkom conducted an general investigation of the market, and finds that a number of security-related offers are still provided to consumers and businesses. Not all offers are relevant under the Open Internet Regulation. Nkom finds no basis for further follow-up of the offers as of today, but will continue to follow monitor the development closely in the future.

## 1.3 Transparency about the internet access service

Nkom observes that Norwegian providers provide satisfactory information about the internet access service and has not discovered any breaches of the regulations during its work on this report. At the same time, there is variation in how the information is provided. Some providers have a dedicated net neutrality webpage, with detailed information about regulations and terms, while others have more distributed information in several webpages and in contracts. Nkom recommends that providers make the information as easily accessible as possible for their customers.

### 1.3.1 Requirements concerning information

Requirements concerning information about the internet access service that providers are to make available to their end-users are set out in Article 4 of the Regulation. Article 4(1) sets out requirements for the transparency of agreements between provider and end-user, while Article 4(2) regulates the provider's obligation to ensure transparent, simple and effective complaints handling procedures.

Nkom has conducted a review of relevant providers' websites and assessed compliance with Article 4 of the Regulation. Below are some comments concerning the review.

### 1.3.2 Information concerning traffic management

Providers of internet access services are obliged to inform about which traffic management measures are used. Current traffic management measures are described further in subchapter 1.2.

According to the regulation, providers must give information about the measures in the agreement terms and make these publicly available, typically on the provider's website. Even if the providers can document that the information is made public, it is also relevant to assess the content and quality of the information.

Nkom's review shows that providers have a varying, but generally satisfactory, representation of traffic management information. It can be challenging to find the relevant information on some websites. Some providers have dedicated net neutrality webpages, where traffic management is one of several topics. Other providers inform more directly about traffic management in contracts and on webpages. Dedicated thematic net neutrality webpages provide end-users with more comprehensive information, but in Nkom's view both solutions referred to in this section are consistent with the regulation.

### 1.3.3 Information concerning speed

*Fixed internet access*

It follows from Article 4(1)(d) of the Regulation that the end-user must be informed of the speed which the provider is able realistically to deliver. Fixed internet access providers must specify the following parameters for both download and upload speeds:

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

"Normally available speed" is the speed that an end-user can expect to achieve for most of the time that they use the service. It is probably this parameter that provides the end-user with the most relevant information about the performance of the internet access.

With regard to the regulation's requirements of transparency, BEREC considers certain types of fixed wireless internet access (FWA) to be fixed internet access. This is, for example, the case where wireless technology (including mobile) is used for internet access at a fixed location with dedicated equipment, and uses either capacity reservation or dedicated frequency bands. In such cases, requirements concerning the availability of information in contracts and on the provider's website should be in accordance with the requirements that apply to fixed internet access.

Concerning fixed internet access, Nkom observes that providers generally disclose the various speed parameters required under the regulation.

*Mobile internet access*

In mobile networks, the speed normally available in a given cell is difficult to predict, due to the varying number of active users. For this reason, only fixed internet access providers are required to provide information about this speed parameter.

However, the regulation requires providers of mobile internet access services to specify the following parameters concerning speed:

- Estimated maximum speed
- Advertised speed

Mobile internet access services include both ordinary mobile subscriptions and dedicated internet access subscriptions, since both are services that provide access to the internet. Ordinary mobile subscriptions support both internet access and telephony/text messages, while dedicated internet access subscriptions solely support internet access. The former is often used via mobile phone, while the latter is often used via a router.

With regard to dedicated internet access subscriptions in the mobile network, a distinction is often made between "fixed wireless internet access" (FWA) offered at a fixed geographical location, often with a fixed outdoor antenna, and "dedicated mobile internet access" that can be used freely at different geographical locations within the coverage area. These differences can lead to varying conditions for the internet access speed achieved for the subscriptions.

For mobile internet access, Nkom observes that providers generally disclose the various speed parameters required under the regulation.

*Conclusion*

Nkom's review is that, to varying degrees, providers present the information about the internet access service on an easy-to-understand basis. On some websites, it can be challenging to find the relevant information. End-users should therefore be aware of what information they are looking for, or contact their provider for specific instructions on where the information is available.

## 1.4 Quality of the internet access service

It is positive to see that the speed of fixed internet access continues the favourable trend from the previous reporting period. The average download and upload speeds for fixed internet access have both increased by around 12% since the previous reporting period.
For mobile networks, we observe that measured speed shows better development than the forecast expected in the general quality of the internet access service. Nkom monitors the development via various sources, including Nettfart's measurement tool.

### 1.4.1 Requirements of the quality of the internet access service

Article 5 of the Regulation states that national regulatory authorities have monitoring and reporting obligations to ensure that providers of internet access services fulfil their obligations regarding open internet access. Furthermore, the regulator must promote non-discriminatory internet access with a quality level that reflects the technological development.

Recital 17 highlights that specialised services and the use of such services should not reduce the general quality of the customer's access to the internet. Concerning internet access via mobile networks, some of the requirements are eased due to the particular circumstances associated with

varying numbers of active users per cell, as well as non-homogeneous coverage. Yet over time, in this case too it is expected that the general quality of the internet access will be maintained.

### 1.4.2 Regulatory follow-up

A measure to follow up on Article 5(1) of the Regulation is to monitor the development in the quality of their internet access measured by end-users. In this report, Nkom has assessed the results of Nkom's Nettfart measurement tool, which can be used via web browser and/or mobile application. Nettfart is based on crowdsourcing whereby the users themselves actively perform measurements and thereby produce the data basis that Nkom analyses.

As for all forms of crowdsourcing, the statistical basis may not be fully representative. The measurement results nonetheless provide an indication of the quality of the internet access service experienced by the end-users. Review of the underlying data also shows that, over time, information is collected from a very large proportion of the Norwegian providers.

### 1.4.3 Measurement results

*Measurement results from nettfart.no*

In this subchapter, results from measurements made via nettfart.no are presented. For fixed internet access, the development in average speed across various subscriptions is presented.

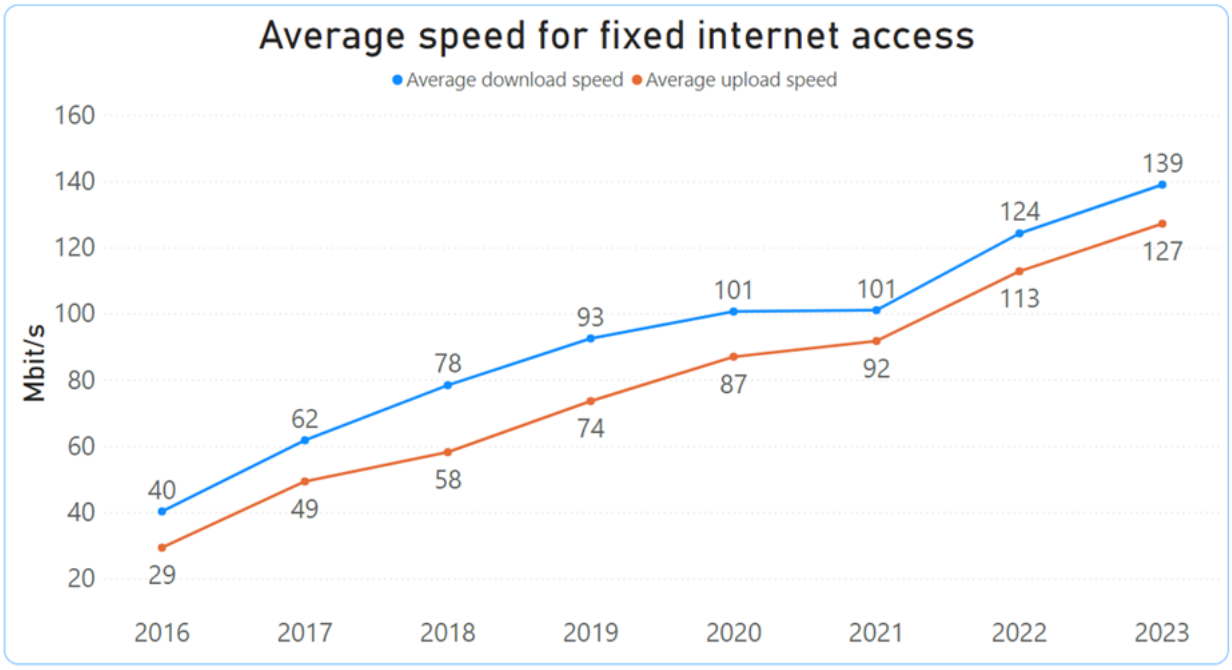



*Figure 1 – Average speed for fixed internet access (source: nettfart.no)*

Figure 1 shows that, so far in 2023, the average download speed measured across the end-users' various subscriptions is around twice as high as in 2017[4]. The growth appears to be continuing and stands at around 10-20 Mbit/s per year.

[4] This year's report uses a rather more extensive data base than was the case for last year's report. The trends are nonetheless the same.

*Measurement results from the Nettfart mobile app*

Here, results measured via the Nettfart mobile app are presented: first as average speed per technology (4G, 5G and WLAN), and then as key figures for measurements via 5G performed by customers in the mobile networks in 2022.

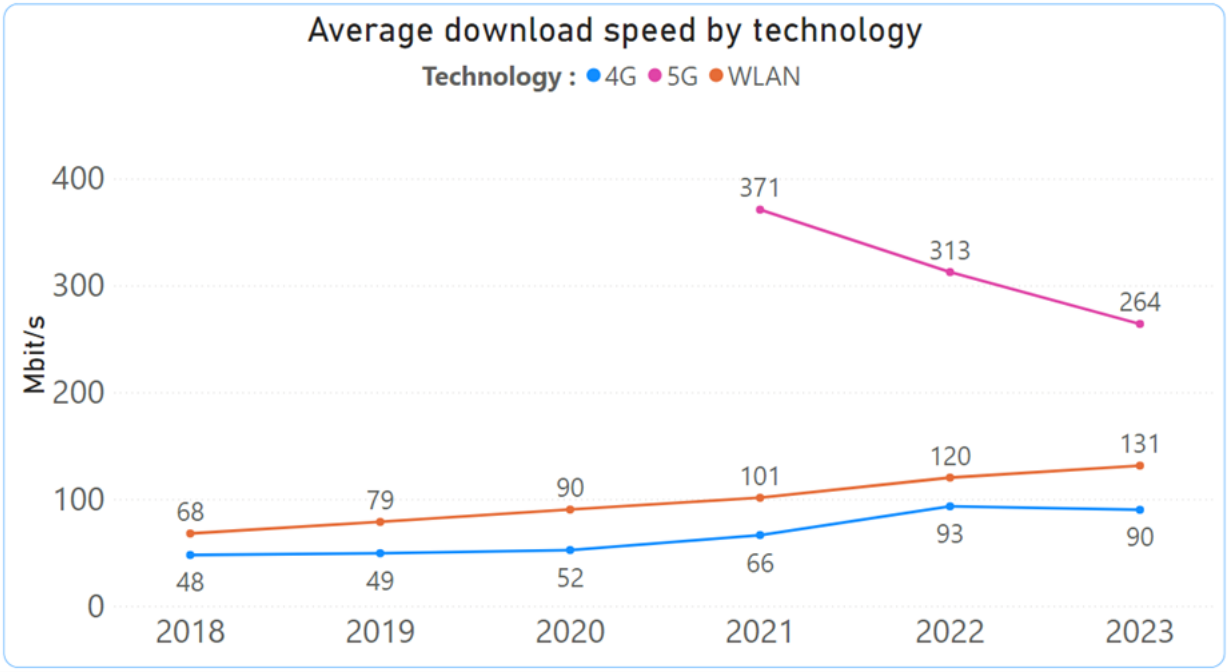



*Figure 2 – Average download speed by technology (source: Nettfart mobile app)*

Figure 2 shows the average measured download speed by technology. The figure shows that users of the Nettfart mobile app achieve significantly higher download speeds when measuring via 5G, compared to measurements via 4G and WLAN. For 5G, the figure shows a continuing downward trend, but it is difficult to say anything definitive about the reason for this. It could be a result of activating 5G in lower frequency bands, as providers also turn on this technology outside the major cities. It may also be due to the fact that the proportion of 5G phones is increasing sharply, which leads to an increased load on the providers' 5G network.

The average speed for WLAN is still increasing slightly. For 4G, we observe a slight reduction, but we emphasise that the trend may change when we have a more complete picture towards the end of the year. Concerning WLAN measurements, however, it is uncertain which transmission medium is used to and from the home for the individual measurements. This may be fibre, hybrid cable or fixed wireless internet access.

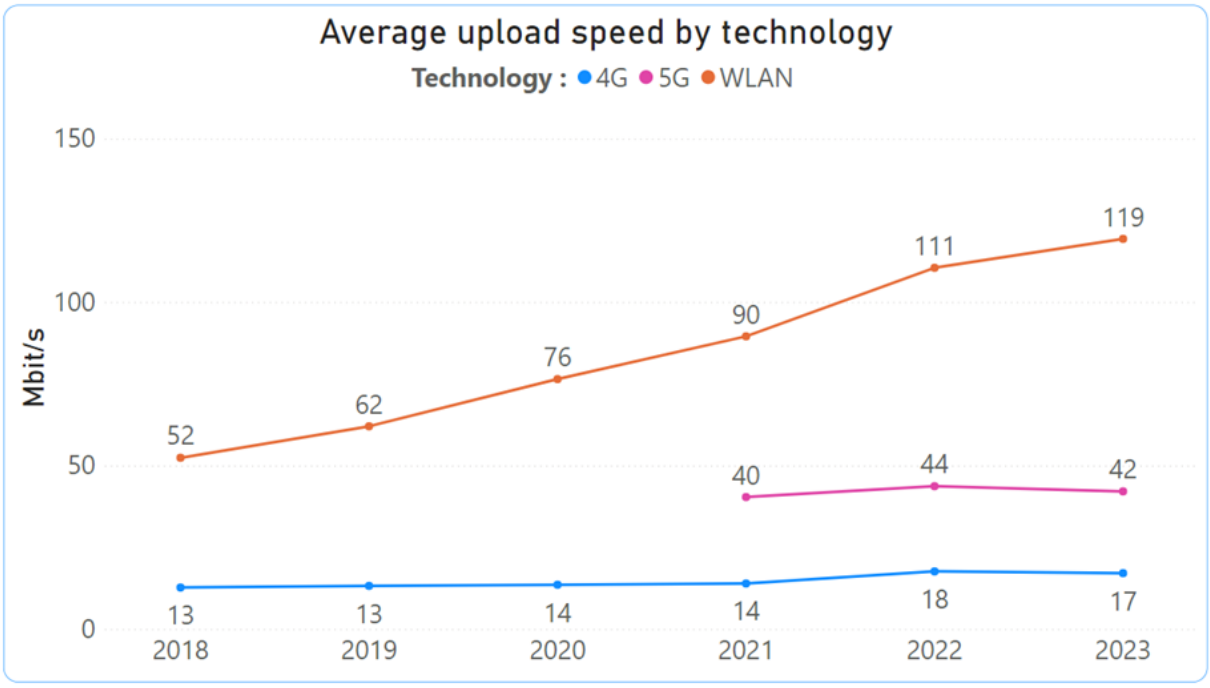



*Figure 3 – Average upload speed by technology (source: Nettfart mobile app)*

Figure 3 shows that for 4G and 5G there are greater differences between average measured upload speeds than are observed for measurements performed via WLAN. One possible explanation is that WLAN is more broadly connected to access lines with symmetrical properties, as offered by many fibre subscriptions.

The figure also shows that the average upload speed via the mobile networks is at a far lower level than in the case of download speeds (Figure 2). The explanation is probably that the mobile networks reserve a larger proportion of the available frequency range for download, since it can be assumed that this is the dominant direction of traffic between the internet and the individual customer.

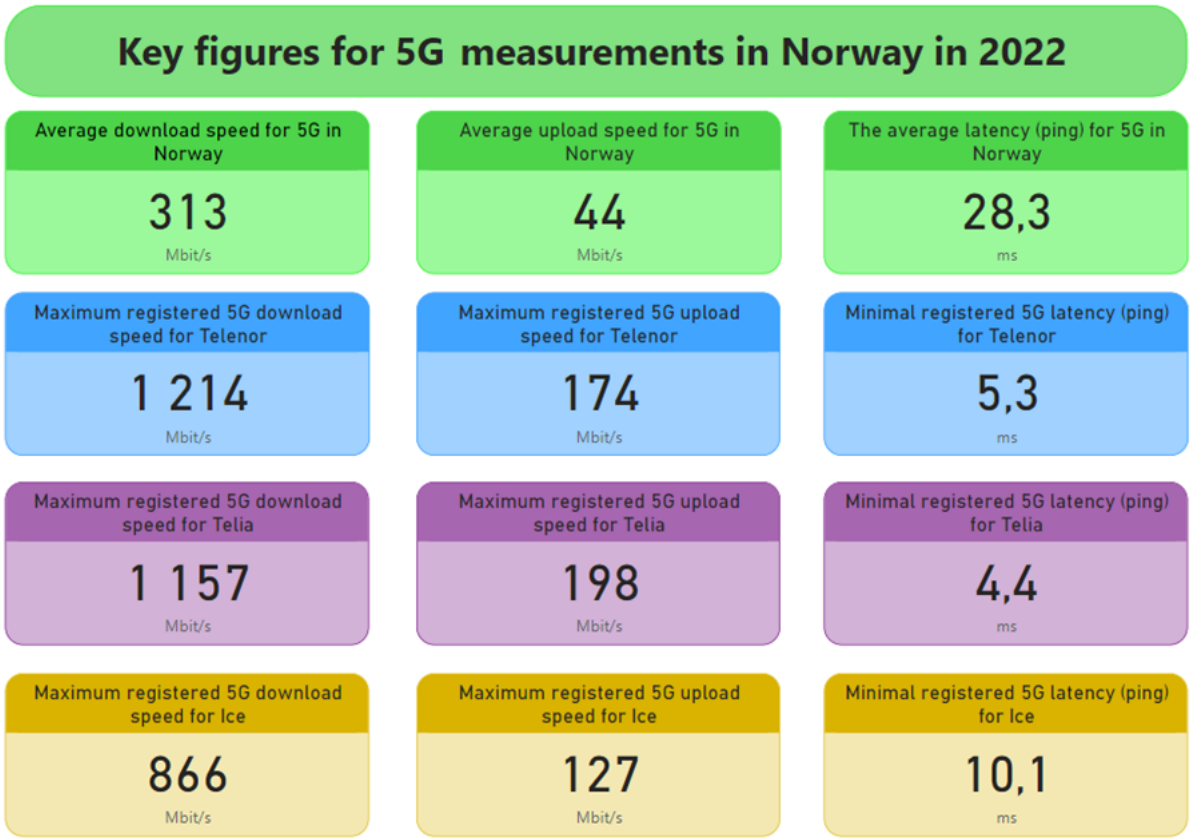



*Figure 4 – Key figures for 5G measurements in 2022 (source: Nettfart mobile app)*

Figure 4 shows selected key figures for 5G measurements in the mobile networks in 2022. The average download speed, upload speed and latency for the 5G networks in Norway in 2022 were 313 Mbit/s, 44 Mbit/s and 28 milliseconds (ms), respectively. Measurements from the Nettfart mobile app show the 5G technology's potential to offer internet access at high speeds and with low latency.

### 1.4.4 General quality of the internet access service

Nkom has applied BEREC's method of evaluating the general quality of the internet access service to the measurements made in the mobile networks. The method uses a forecasting function based on average download, upload and latency from the previous years and uses these to estimate expectations for subsequent years. Estimated and measured values can then be compared to see if there are large deviations in the results.

The figures below show forecast download and upload speeds, as well as latency, for measurements made in the mobile networks in Norway, aggregated for all mobile operators. The blue line shows the measured values and the pink dashed line shows the forecast for 2022.

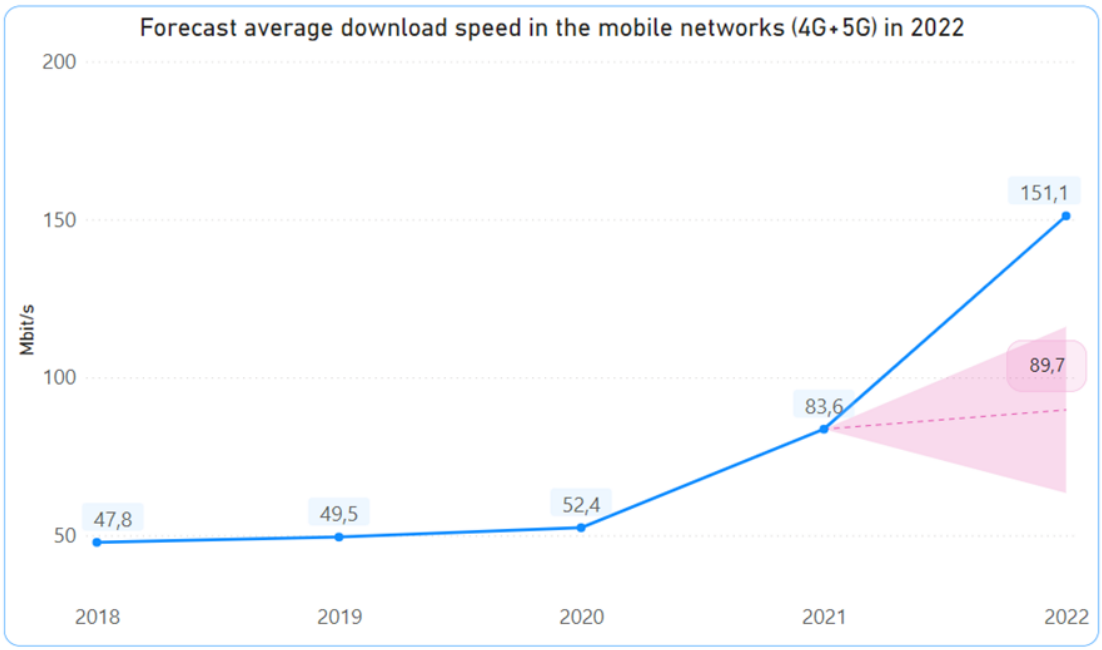



*Figure 5 – Forecast average download speed in the mobile networks in 2022*

Figure 5 shows the forecast average download speed for 2022 at 90 Mbit/s, while the average measured value was 151 Mbit/s. This shows that the download speed in the mobile networks has developed more positively than forecast estimates and that providers are expanding capacity as required.

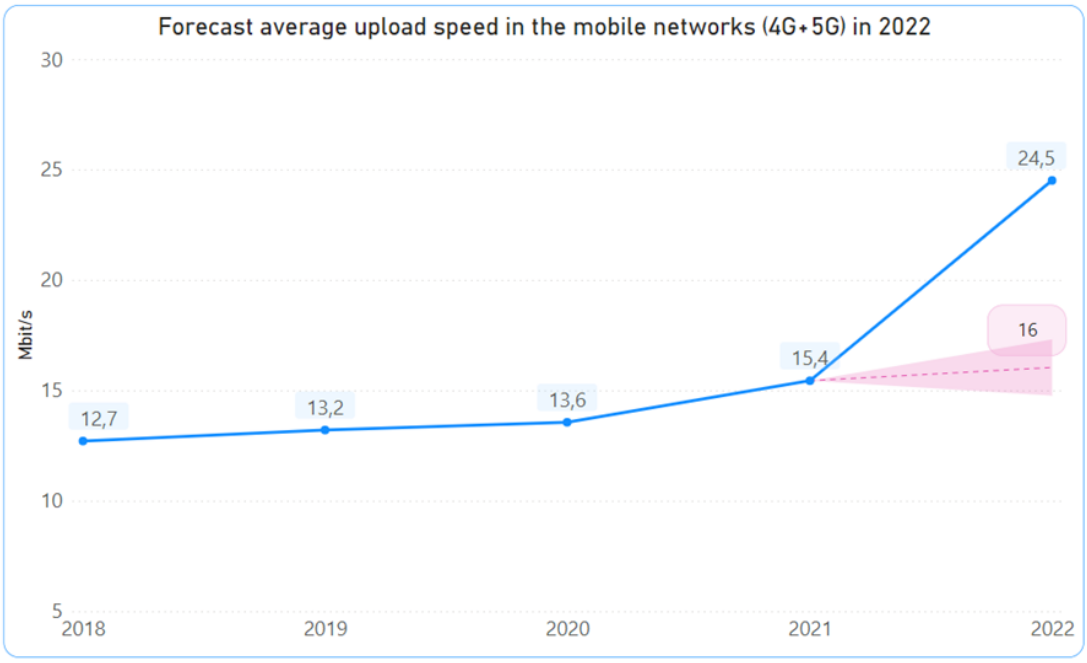



*Figure 6 – Forecast average upload speed in the mobile networks in 2022*

Figure 6 shows the forecast average upload speed for 2022 at 16 Mbit/s, while the average measured value was 25 Mbit/s. This shows that the upload speed in the mobile networks has also developed more positively than forecast estimates.

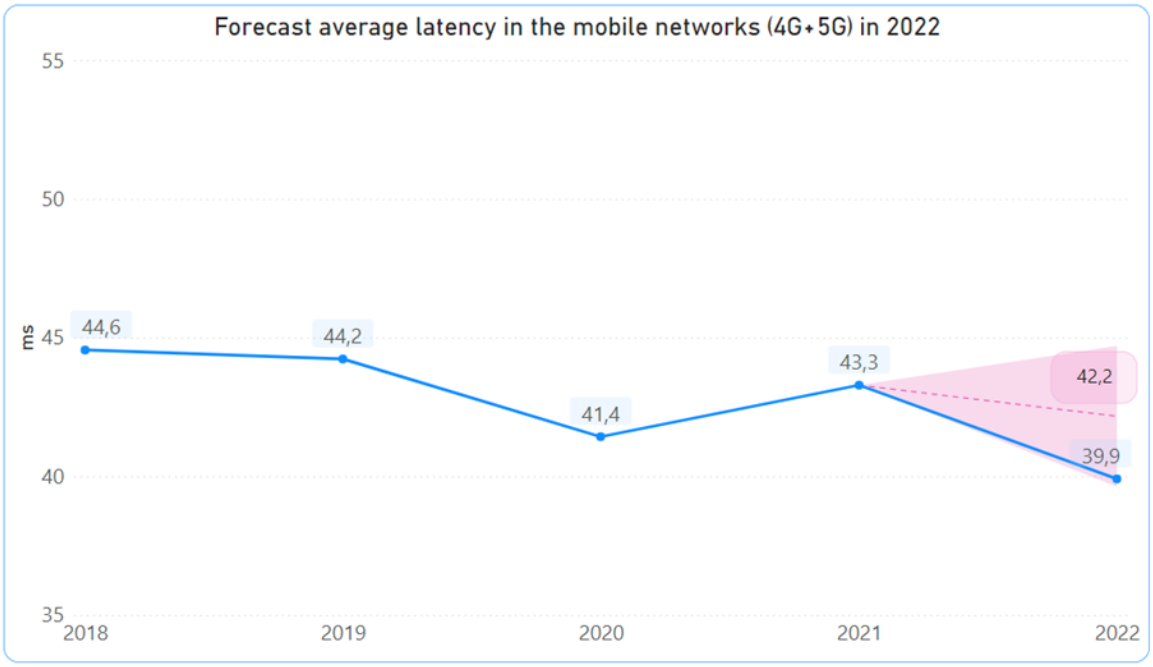



*Figure 7 – Forecast average latency in the mobile networks in 2022*

Figure 7 shows the forecast average latency for 2022 at 42.2 ms, and that the measured average value was 39.9 ms. Here, Nkom observes positive development in that measured latency is in line with the forecast and has even decreased somewhat compared to 2021.

# 2 Core functions of the internet in Norway

## 2.1 Introduction and background

Part 2 of the Annual Report describes the status of the core functions of the internet in Norway, a task commissioned by KDD (Norwegian Ministry of Local Government and Regional Development) from Nkom under *Report to the Norwegian Parliament 28 (2020-2021) Our common digital foundation – Mobile, broadband and internet services*[5].

Chapter 2.2 presents the status of infrastructure and traffic development in the Norwegian part of the internet, including the development for IPv6 and interconnection in the Norwegian market.

Chapter 2.3 presents the regulatory development for internet-based services, both as selected topics concerning the national development and various EEA-relevant legal acts from the EU.

Finally, Chapter 2.4 describes the geopolitical picture under topics such as the internet ecosystem, internet governance, internet security and the green transition within electronic communications.

## 2.2 Infrastructure and traffic development

### 2.2.1 Availability of the internet access service

In the first half of 2022, respectively 93.6% and 92.5% of all households in Norway were offered internet access with at least 100 Mbit/s, and 1000 Mbit/s in download speed. At the same time, baseline coverage for 5G was estimated at close to 82% in Norway.

The availability of the internet access service is generally consistent with the availability of broadband. Nkom's coverage survey for the first half of 2022 shows that 93.6% and 92.5% of all households had broadband offers with at least 100 Mbit/s, and 1000 Mbit/s in download speed[6]. This is mainly based on fibre or hybrid networks[7], although fixed wireless broadband also contributes to the coverage.

Virtually all households that have broadband offers with at least 100 Mbit/s download speed are also offered alternative connections. There are geographical disparities, but in overall terms most Norwegian residents have good opportunities to connect to the internet.

The rollout of the 5G network started in 2020. Nkom's coverage survey for the first half of 2022 shows that the basic coverage for 5G is estimated at almost 82% and that one year earlier it was estimated at around 23%. In other words: the basic coverage for 5G increased significantly in 2022.

The electronic communications statistics for 2022[8] show that Telenor, Altibox, Telia and GlobalConnect together held an estimated 84% of the market, when the private and business markets are combined.

[5] Report to the Norwegian Parliament 28 (2020-2021), Chapter 10, April 2021.

[6] https://ekomstatistikken.nkom.no/#/article/dekning_nasjonalt2022

[7] Hybrid fibre, which is also called HFC (Hybrid Fibre-Coaxial), refers to the way fibre and coaxial cables are used in combination within a cable network.

[8] https://nkom.no/statistikk/rapporter-og-analyser

In the mobile market, the concentration is even higher. Overall, Telenor, Telia and Ice have around 91% of customers.

By the end of November 2022, internet access via low earth-orbit satellites (LEO) from Starlink was available throughout Norway [9]. Other players, such as Oneweb, are also expected to offer internet access via LEO satellite in Norway in the coming years.

### 2.2.2 Development in Norwegian internet traffic

At aggregated level, Nkom can see annual growth of around 20-30% for internet traffic in both fixed and mobile networks. Streaming applications are the biggest traffic driver, accounting for around 70% of network traffic.

In 2022, internet traffic in mobile networks totalled 763 Petabytes (PB), an increase of 22% from 2021. 5G connections now account for around 27% of the total internet traffic in the mobile networks, and in the last three years, the share of FWA traffic has gone from 15% to 60% of total traffic.

In February 2023, Nkom issued a questionnaire to selected providers, in order to collect data on the development of internet traffic in fixed and mobile networks. The scope included the largest internet service providers in both of these categories. For the period from 2018 to Q1 2023, at an aggregated level we see annual growth of around 20-30% for internet traffic in both fixed and mobile networks.

In Q1 2023, network traffic production for the largest fixed network providers and the largest mobile operators was over 3 Tbit/s and 0.4 Tbit/s, respectively, in travel time (peak hour).

The distribution of internet traffic between different applications is relatively similar in mobile and fixed networks, with the exception of streaming, which is much larger in fixed networks. Streaming such as national broadcasters' internet-based TV, TikTok, YouTube and Netflix are the greatest traffic drivers, accounting for around 70% of traffic. Web browsing (HTTP-based communication) is still a major contributor. This is followed by social media such as Facebook, Instagram and Snapchat.

*Internet traffic on the mobile networks*

During the past two years, traffic growth on mobile networks has been driven by the launch of fixed wireless access. Traffic development is affected by the technological development and accompanying increase in network capacity, as well as growth in number of customers and increased data allowances. Mobile subscription[10] data allowances have increased recent years without prices rising equivalently.

Figure 8 shows the development in internet traffic distributed on ordinary mobile subscriptions, dedicated internet subscriptions[11] and international roaming. The ordinary mobile subscriptions generate most of the internet traffic on the mobile networks (over 80%). In 2022, internet traffic on mobile networks totalled 763 Petabytes (PB)[12], an increase of 22% from 2021.

Internet traffic for international roaming almost trebled in 2022 compared to 2021, which may be due to the fact that normal travel routines are in place again after the pandemic and that the principle of Roam Like At Home (RLAH)[13]has been retained in the regulation.

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

[10] The largest group still have data allowance of between 1 GB and 5 GB included. The biggest increase in 2022 was for subscriptions with data allowances of between 10 GB and 20 GB (source: Nkom's electronic communications statistics).

[11] Dedicated internet subscriptions concern products that offer a dedicated data service using their own SIM card. The user gains a clean data connection between the terminal and the mobile network and, via this, access to the Internet.

[12] A Petabyte (PB) is 1,000 Terabytes or 1,000,000 Gigabytes.

[13] Roam Like At Home: no additional charge for mobile data usage in the European Economic Area.

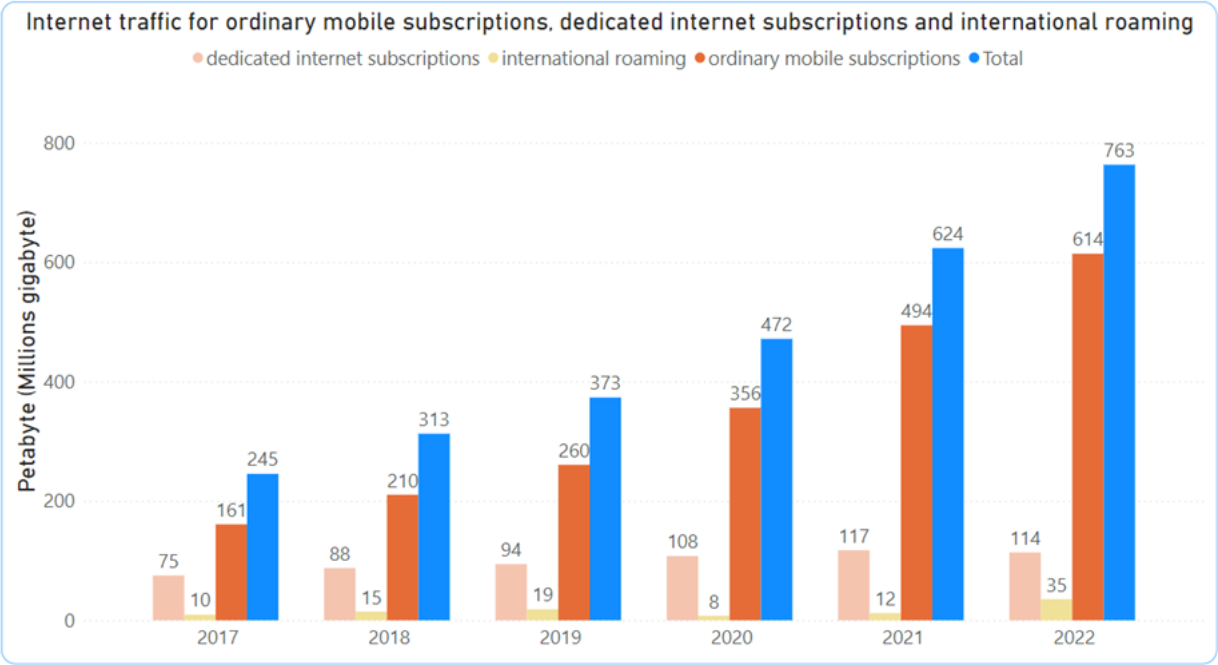



*Figure 8 – Internet traffic for ordinary mobile subscriptions, dedicated internet subscriptions and international roaming (source: Nkom electronic communications statistics)*

Mobile providers are now rolling out 5G on a large scale. In Q1 2023, around 50% of the connected handsets are ready for this technology generation, and the number of 5G-ready handsets has doubled during the past year.

5G connections now account for around 27% of total internet traffic on mobile networks. Compared to the 2022 figures, this represents more than a fivefold increase so far in 2023. 5G traffic is increasing as mobile providers enable 5G in more and more places, and older handsets are being replaced with newer ones that are ready for 5G. Another observation is that the availability of fixed wireless internet access (FWA) is the biggest driver of traffic growth in the mobile networks, and over the past three years, the share of FWA traffic has increased from 15% to 60% of the total traffic[14].

### 2.2.3 Adoption of IPv6

In 2023, Norway has an IPv6 adoption of 36.6%, thereby ranking 24th in the world, up 11 places from its previous ranking. In the course of one year, IPv6 adoption in Norway has increased from 24,2% in April 2022 to 36.6% in April 2023. At European level, Norway advanced four places, to 10th place, in the course of a year.

It is positive to see that internet service providers in Norway are increasing the availability of IPv6 for end-customers. Nkom is monitoring the further development and emphasises the importance of operators in the Norwegian market facilitating the use of IPv6 to the greatest possible extent.

[14] The number of accesses for fixed wireless access has increased from 104,000 in the first half of 2021 to 140,000 in the first half of 2022 for private subscriptions, and from 9,000 to 13,000 for business subscriptions in the same period (source: Nkom's electronic communications statistics).

*About the transition from IPv4 to IPv6*

IP (Internet Protocol) is the basic protocol used to transmit traffic on the internet. Public IP addresses are unique worldwide identifiers for computers connected to the internet. The IP protocol exists in two versions: IPv4 and IPv6.

There is a need to increase the use of IPv6 on the internet. The reason is a lack of available IPv4 addresses. The complexity of today's internet entails that the transition from IPv4 to IPv6 must take place gradually, starting with a period of co-existence with IPv4.

*IPv6 adoption in Norway*

Figure 9 below shows the status of IPv6 adoption in Norway. The data basis is taken from the four main sources of publicly available information on IPv6 adoption (Google, Akamai, Facebook, Apnic)[15], and the data collection took place in April 2023.

Norway moved from 35th place to 24th place on the list of countries with the highest adoption of IPv6 worldwide. In the course of one year, IPv6 adoption in Norway increased by 12.4 percentage points, from 24.2% in April 2022, to 36.6% in April 2023. At European level, Norway advanced four places, to 10th place, in the course of a year.

The figures show that the adoption of IPv6 is increasing and that Norwegian internet service providers are aiming to increase the availability of IPv6 to customers. Several providers have increased the activation of IPv6 in their network, such as Telia, which announced the important step of activating IPv6 gradually for all its customers in the mobile network.

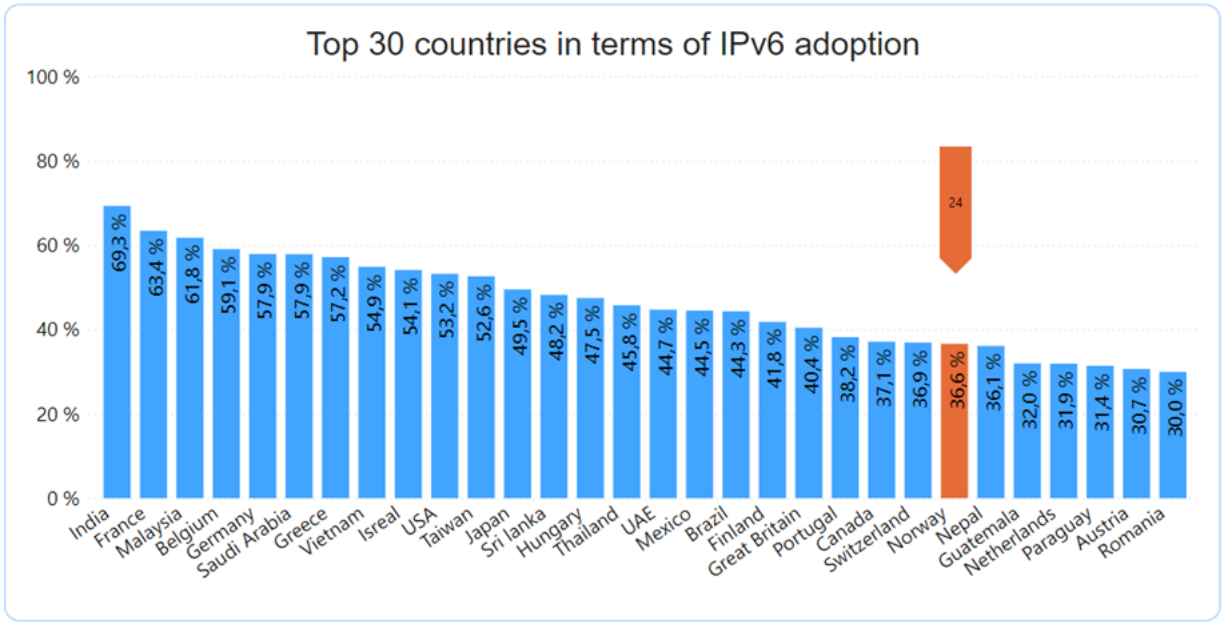



*Figure 9 – Top 30 countries in terms of IPv6 adoption*

[15] Based on the median for "Google IPv6 adoption", "Akamai IPv6 adoption", "Facebook IPv6 adoption" and "Apnic IPv6 adoption" data from April 2023. The median of the five sources is calculated for each country, and the statistics apply solely to the 100 countries with the most internet users (source: Wikipedia, data as at April 2023).

Figure 10 below shows how Norway is positioned among the Nordic countries when it comes to the use of IPv6. Norway is in second place, behind Finland and ahead of Sweden, Iceland and Denmark.

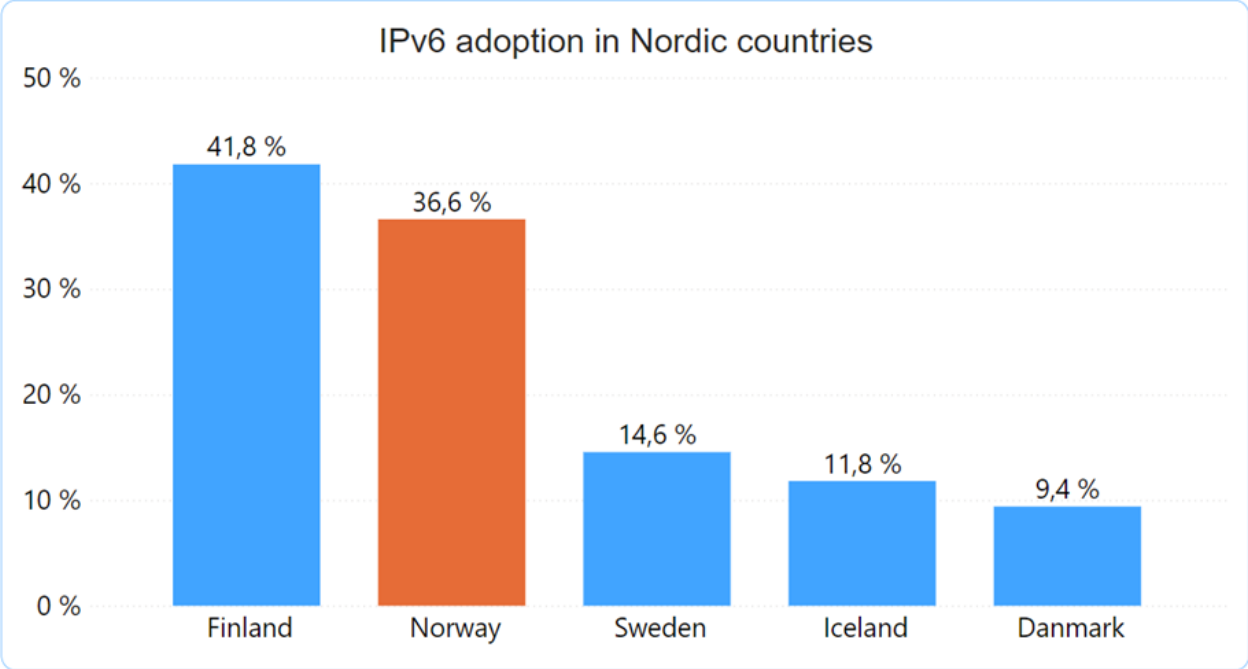



*Figure 10 – IPv6 adoption in Nordic countries*

Figure 11 below shows the annual average for IPv4 and IPv6, respectively, at vg.no for both fixed network providers and mobile operators. The statistics[16] were obtained in April 2023. The figures show that Telenor is at the top of the list when it comes to mobile networks.

Concerning the major fixed network providers, Telenor comes in 1st place and Altibox in 2nd place, while Telia is at the bottom of the list with less than 1% of IPv6 traffic volume at vg.no.

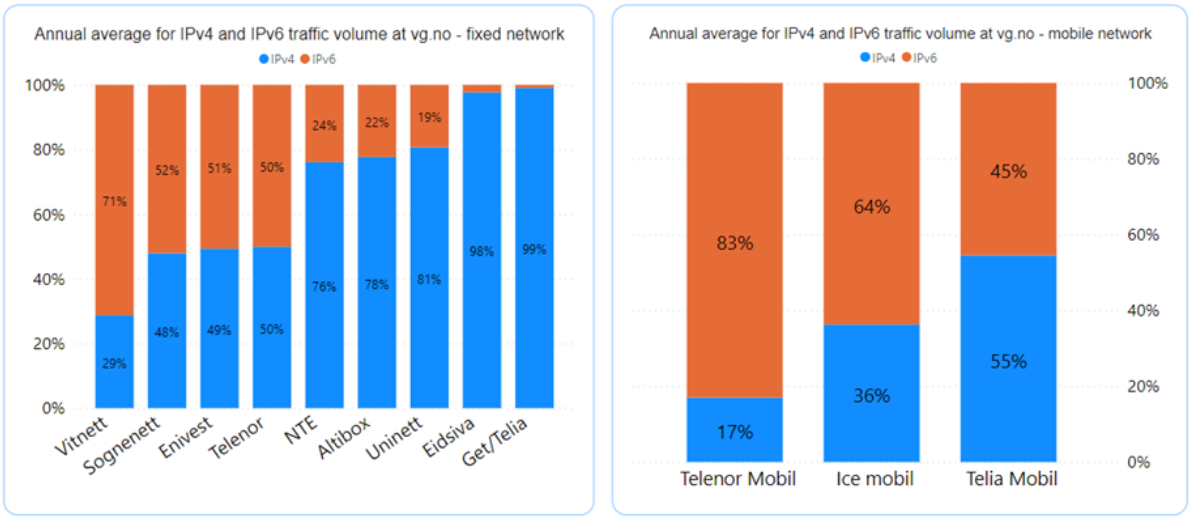



*Figure 11 – Annual average for IPv4 and IPv6, respectively, at vg.no*

[16] https://munin.fud.no/per_isp-year.html

*Regulatory follow-up*

Nkom has held dialogue meetings concerning IPv6 with the largest internet service providers in the Norwegian market, to stimulate the transition from IPv4 to IPv6. Nkom presented a proposed escalation plan for IPv6 over the next 2-3 years, and the Norwegian internet service providers (ISPs) have expressed that they are in many ways aligned with the proposal.

Nkom encourages Norwegian internet service providers to intensify their efforts to increase the use of IPv6 for the internet access services that are offering. These efforts are in parallel with the trend for equipment providers and software providers to introduce IPv6 in end-user equipment.

Nkom's recommended escalation plan for increasing use of IPv6 in the Norwegian market:

1. By 30 April 2024, Norwegian ISPs will activate IPv6 for all their internet subscribers, possibly with the exception of subscriptions that require physical replacement of home routers.
2. By 30 April 2025, Norwegian ISPs will have activated IPv6 for all their internet subscribers, and replaced any home routers that could not be upgraded via software.
3. However, home routers based on DSL technology connected to the copper network do not need to be replaced until the decommissioning of the copper network has been completed.

Nkom will follow the development in IPv6 use in the Norwegian market closely during the transition period.

- Nkom will publish tertiary statistics on active availability of IPv6 from Norwegian ISPs, as well as statistics on the use of IPv6 in the Norwegian market that are available from external sources.
- Based on the stepwise development (by the end of 2025), Nkom will assess whether there is a need to introduce national regulation to make IPv6 mandatory among Norwegian ISPs.

### 2.2.4 Internet interconnection in Norway

The annual average for inbound/outbound internet traffic across the entire NIX infrastructure is 94 Gbit/s in 2022, with NIX1 and NIX2 in Oslo accounting for 88 Gbit/s (93% of the total traffic on the NIX infrastructure) and other NIX interconnection points together accounting for 6 Gbit/s.

All the major internet service providers in Norway have currently installed CDNs from players such as Akamai, Google, Netflix, Apple and Facebook, and the internet service providers report that caching efficiency is 75-90%.

Most of the international internet traffic is conveyed via the international transit providers Arelion and Lumen, and the major Norwegian internet service providers Telenor, Telia, GlobalConnect, Telia and Altibox.

Interconnection is the process whereby various networks exchange traffic with each other. This is an important core internet function. Where and how this exchange of traffic occurs is of significance to response time, quality and security – and also has an economic aspect.

Most of the interconnection between Norwegian internet service providers is geographically centralised in Oslo, at private interconnection points. In addition, the public NIX – Norwegian Internet

eXchange – interconnection points are used[17]. NIX is a common term for public interconnection points in Oslo, Stavanger, Bergen, Trondheim and Tromsø.

Figure 12 shows the location of the interconnection points, and the size of the circles illustrates the relative difference in traffic volume in 2022.

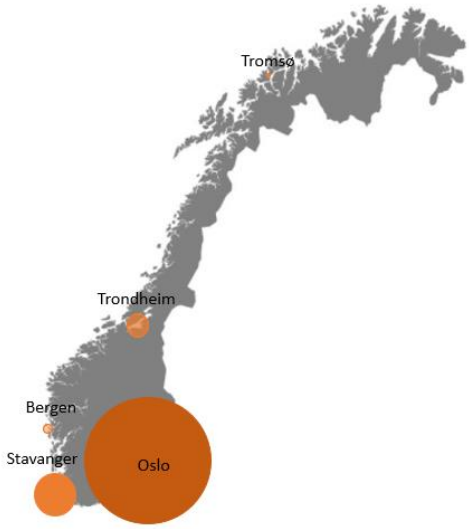



*Figure 12 – Location and traffic volume for the NIX interconnection points*

Annual average for inbound/outbound internet traffic across the entire NIX infrastructure is 94 Gbit/s in 2022[18], with NIX1 and NIX2 in Oslo accounting for 88 Gbit/s (93% of the total traffic on NIX). The volume in Oslo has seen a significant reduction of around 9% during the past year. The reason for this may be that some providers moved traffic to private interconnections, or other commercial operators.

Interconnection via the public interconnection points is particularly important for smaller internet service providers and is an opportunity to meet the major providers and exchange traffic with them. The larger internet service providers also use NIX, to supplement their private interconnection. As of Q1 2023, NIX had 70 domestic and international customers (connected networks), and most major international operators are present in NIX, such as Amazon, Microsoft, Akamai, Cloudflare, Dropbox, Huawei Cloud and NORDUnet[19].

Stavanger (SIX) is the second largest public interconnection point in Norway, with an annual average of 5 Gbit/s. SIX is located in Green Mountain's data centre, where both content providers and Content Delivery Network (CDN) providers are also located.

Other than SIX, there is a limited degree of regional interconnection, and some of the small providers regret that data traffic from their networks and customers must be sent to Oslo, to be connected to the largest providers' networks. However, all providers emphasise the importance of regional peering and see a need for local interconnection points in order to optimise traffic flow. Nkom has registered an increased interest among several network owners in exchanging traffic in Tromsø (TIX) and Stavanger (SIX), which could also have an impact on robustness and diversity in a national context.

[17] www.nix.no

[18] https://www.nix.no/statistics, the data was obtained in April 2023.

[19] NORDUnet connects the Nordic national research and education networks.

*Data centres*

Data centres are an increasingly important part of the internet ecosystem. This also applies to the internet ecosystem in Norway. In line with the national data centre strategy from 2021[20] in recent years the Norwegian authorities have worked offensively to facilitate the establishment of data centres and data centre industry in Norway.

In autumn 2022, the Ministry of Local Government and Regional Development announced that they were starting work on updating the data centre strategy. This was partly due to radical changes in framework conditions driven by the war in Ukraine, such as the strained power situation and a more demanding security policy picture. An updated data centre strategy is expected during 2023.

The data centre industry has experienced significant growth in recent years. The largest Norwegian data centre agreement to date was announced in March 2023. Data centre operator GreenMountain will build a dedicated data centre for TikTok outside Hamar, with a capacity of up to 150 MW.[21]

*Caching services*

CDNs are geographically distributed networks of caching servers that offer high availability and performance by moving content closer to end-users. The introduction of these services has resulted in a "flatter" internet with a shorter distance between consumer and content, since users retrieve cached content in CDN servers that are located in their own provider's network, instead of data centres further away. This has resulted in reduced bottlenecks in the network, and a reduced transit volume for internet service providers.

All the major internet service providers in Norway now have CDNs installed from operators such as Akamai, Google, Netflix[22], Apple and Facebook. Internet service providers report that caching efficiency is 75-90%, which means that many requests for content from their customers are serviced internally, and in high quality. Another effect is that the internet service providers can reduce the need for transit, in return for ensuring optimal conditions for the deployed servers.

On-network CDN traffic accounts for a large proportion of internet interconnection. Internet service providers in Norway reported that on-network CDN traffic accounts for more than half of the total interconnection volume in the network infrastructure today and this explains the decline in internet transit for internet service providers, which accounts for 5-10% of the total interconnection volume.

*International internet interconnection*

Most of the internet traffic between Norway and other countries is exchanged on private interconnection points in Oslo with the major international interconnection points in Stockholm, Frankfurt, Amsterdam and London.

This traffic was previously routed through a limited number of connections from Oslo via Sweden. In the period from 2020 to 2022, however, several new international submarine fibre connections were established. These connections facilitate a growing data centre industry and an increased need for capacity and exchange of internet and data centre traffic between Norway and abroad.

[20] "Norske datasenter – berekraftige, digitale kraftsenter" (Norwegian data centres – sustainable digital power centres), Norwegian Ministry of Local Government and Modernisation, 2021.

[21] MW will refer to how much power capacity the IT infrastructure has access to.

[22] Netflix stores up to 100% of the content in CDN.

In 2022, Altibox's submarine cable NO-UK from Stavanger to Newcastle (UK) was put into operation. The same applied to Bulk's submarine cable, Havsil, from Kristiansand to Hanstholm (Denmark). Havsil is used, among others, by Arelion (formerly Telia Carrier), an operator that transmits a significant proportion of the internet traffic between Norway and abroad.

In early May 2023, German interconnection operator DE-CIX[23] also put two interconnection points in Norway (Oslo and Kristiansand) into operation. DE-CIX is one of the world's largest interconnection operators with a global presence. They offer public and private interconnection and a range of other services to, among others, internet service providers, cloud service providers and major international companies.

International internet interconnection is important for national security and preparedness. This rapid development is related to the development of internet-based services and platforms, and the data centre industry in Norway. Nkom therefore continuously follows up the players involved in exchanging traffic between Norway and abroad, including interconnection operators.

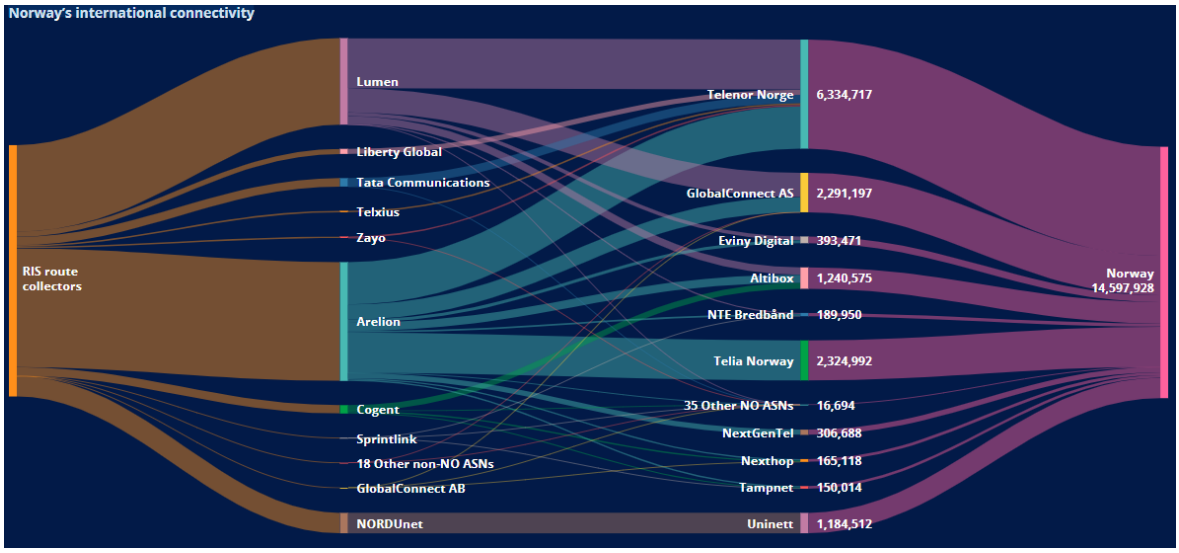



*Figure 13. Actors involved in Norway's international internet interconnection (source: RIPE NCC[24])*

Most of the international internet traffic measured by RIPE is conveyed between the international transit providers Arelion and Lumen, and the major Norwegian internet service providers Telenor, GlobalConnect, Telia and Altibox.

## 2.2.5 Domain Name System

The Domain Name System (DNS) is a critical component for the functioning of the internet. Technical and market-related changes affect important features of DNS, such as integrity, availability, confidentiality and the regulator's supervision of the internet access service. Nkom is monitoring the development and working to maintain a robust DNS infrastructure for Norwegian internet users.

[23] www.de-cix.net

[24] "RIPE NCC – Internet Country Report: The Nordic Region", RIPE NCC (www.ripe.net), December 2022.

The Domain Name System (DNS) is a basic function that is necessary for the internet infrastructure to function. When a user contacts an internet-based service using a domain name, this triggers a series of lookups in DNS to find the relevant IP address for the service.

Traditionally, DNS lookups are handled by the individual internet service providers, which often have DNS functions integrated into their networks. In recent years, however, there has been a shift towards increased use of open (and global) DNS lookup services, offered by e.g. Google and Cloudflare.

The European Union Agency for Cybersecurity (ENISA) points to various drivers of this development[25]:

- Increased integrity/confidentiality – many open DNS services offer DNS lookup encryption to prevent fraudulent DNS responses that can trick the user into fraudulent websites.
- Increased availability – if there is an outage of the integrated DNS service at the internet service provider, users often move to an open DNS service.
- Avoid blocking – using open DNS lookup services can circumvent national statutory DNS blocking of illegal content.

DNSSEC is a mechanism for integrity protection of DNS responses. This was introduced for the Norwegian country code top-level domain .no in 2014. As of May 2022, around 61% of all .no domain names were signed with DNSSEC. A condition for DNSSEC is also that the DNS servers that retrieve the response to the domain lookup validate the response, so that answers with incomplete signatures are rejected. As of May 2022, around 86% of the domain lookups in Norway were validated, which is due to the fact that the major Norwegian internet service providers such as Telenor, Telia and Altibox have enabled validation.[26]

*DNS4EU*

In response to the increasing use of US-based open DNS lookup services (e.g. from Google, Cloudflare), the EU has implemented the DNS4EU initiative to strengthen DNS lookup services within European jurisdiction.

DNS4EU was established as a project by the European Commission at the end of 2021. The project has members from many countries and is under the leadership of the Czech company, Whalebone. DNS4EU primarily offers DNS lookups, but also provides protection against unwanted websites in accordance with the EU's own regulations. The rollout of the service will start with a functionally limited version that, over a 3-year period, will be used by 100 million people, according to the EU's goals.[27]

### 2.2.6 Internet of Things (IoT)

IoT devices continue to grow steadily from previous years. This is an increase of 30% active SIM cards from 2021 to 2022 in Norway. The 5G rollout is well underway and this can probably increase the number of IoT devices even more in the coming years.

Around 1.4 million active SIM cards are connected to the 2G network, and after the decommissioning of the 2G network by 2025 these SIM cards will not be able to use this network. Nkom recommends affected users to implement newer technology well in advance of the decommissioning.

[25] Security and privacy of public DNS resolvers, ENISA, February 2022.

[26] More secure Norwegian domain names with DNSSEC, https://www.norid.no/no/om-domenenavn/veiledere/sikrere-norske-domenenavn-med-dnssec/

[27] EU is building its own DNS service. What's in it for the everyday user? https://adguard-dns.io/en/blog/dns-eu-project-secutity.html

IoT devices can be connected via wired or wireless connectivity. For wireless connectivity, an overall distinction is made between technologies that use unlicensed frequencies and technologies using mobile technology (licensed frequencies).

The number of IoT devices has increased in recent years and the trend seems to continue, but not necessarily at the same pace. Figures from analytics company IoT Analytics estimate that there were around 12.2 billion IoT devices in the world in 2021[28]. They now estimate that there will be 27 billion connected devices in 2025.

In Norway, IoT is used in a number of areas, such as metering systems, alarm systems, payment solutions, transport and smart house systems. In recent years, the use of IoT has also accelerated in municipalities across Norway, where they have the opportunity to use sensors for the aforementioned areas. These are often IoT devices that use unlicensed frequencies and therefore have no cost associated with the use of frequencies.

*IoT via unlicensed frequencies*

In this category there are a number of protocols with different range and bandwidth. The best known are Wi-Fi, Bluetooth/BLE (Bluetooth Low Energy), ZigBee, Z-wave, LoRaWan and Sigfox. The two last-mentioned go under the common designation LPWAN (Low-Power Wide-Area Network).

The number of connected devices in unlicensed frequencies is increasing. However, it is difficult to estimate this development accurately since a lot of equipment does not need to be registered. Many municipalities in Norway use LoRaWAN or similar technologies for different applications, to streamline or provide services to residents. LoRaWAN provides good coverage with low power consumption, and is widely used in water meters, agriculture, motion sensors and temperature sensors.

*IoT via licensed frequencies*

Machine-to-Machine communication (M2M) is mobile communication between machines, cars or other objects. In other words, M2M is a term that refers to mobile communication between non-human subscribers (IoT devices)[29].

2G (GSM) was originally developed for communication between people and not as a carrier for IoT. However, SMS was adopted for simple IoT communication and is still in widespread use. The 2G networks have limitations in terms of transmission capacity and the number of connected devices.

In 4G (LTE), two IoT-specialised standards were introduced: LTE-M and NB-IoT. LTE-M allows for higher speed and mobility than NB-IoT. NB-IoT is a simpler protocol with lower power consumption that is well suited for frequent communication and good indoor coverage. This has led to increasing interest in and use of mobile IoT from business and industry.

During the last three years, mobile providers have rolled out 5G networks in Norway. 5G supports a large number of simultaneously connected devices in the network, with the ability to handle multiple application areas. Today's 5G network does not support dedicated M2M technology, but this is expected to become available with the introduction of 5G Stand Alone and network slicing that will be added during 2023/2024.

Figure 14 shows the number of active SIM cards for M2M in mobile networks in Norway. The statistics show that the number of active SIM cards in 2022 had almost doubled since 2019 and that the number of devices has increased faster in the last two years, at a rate of around 30%.

[28] https://iot-analytics.com/number-connected-iot-devices/

[29] https://en.wikipedia.org/wiki/Machine_to_machine

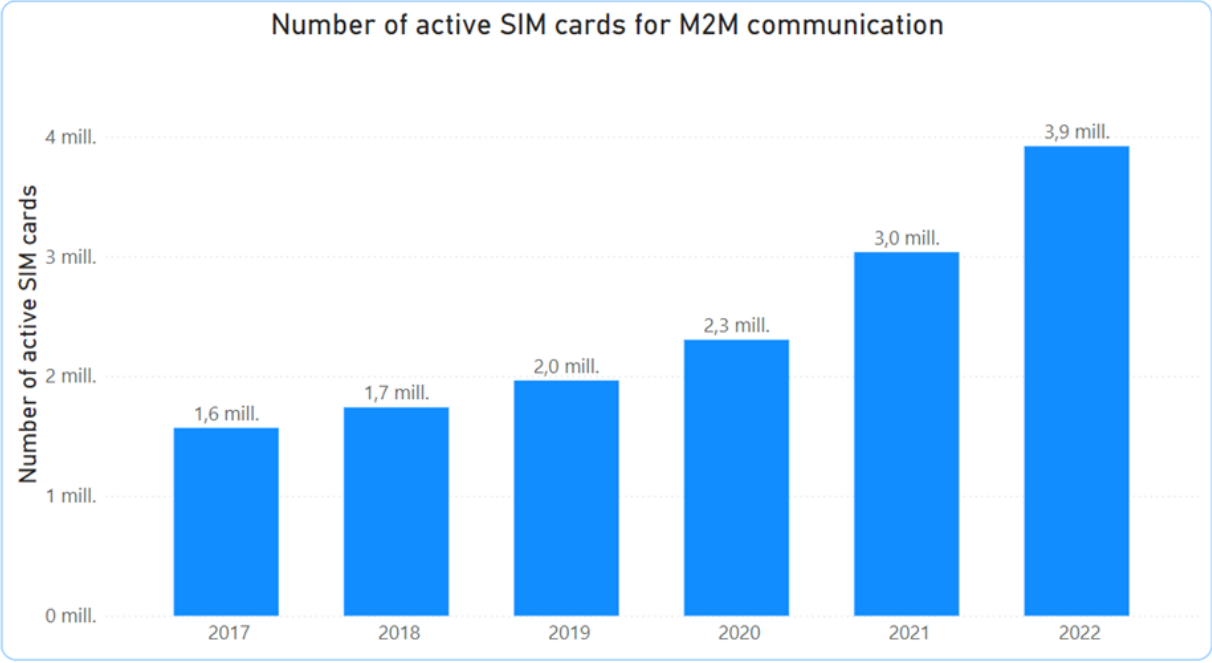



*Figure 14 – Number of active SIM cards for M2M communication*
*(source: Nkom electronic communications statistics)*

Nkom has urged all sectors to start planning the phasing-out of devices operating solely on 2G as the date of providers' planned decommissioning of the 2G network approaches[30]. There are still close to 1.4 million IoT devices connected to the 2G network. This will have consequences for those who do not switch to new technology. Up to the decommissioning date in 2025, Nkom will continue to survey the use of and reliance on 2G, to ensure responsible discontinuation that observes relevant user considerations.

[30] https://www.nkom.no/fysiske-nett-og-infrastruktur/informasjon-om-slukking-av-2g-i-2025#nr_legges_2gnettene_ned

## 2.3 Regulatory development

Nkom notes extensive development in the number of European legal acts and national legislation that will greatly influence the internet of the future. This applies to internet-based services and platforms, including cloud-based services, and to regulation related to internet security. If the regulatory development is to benefit internet users, it is vital to ensure the effective exercise of authority at international and national levels. To that end, Nkom expects to play an active role as national regulator of electronic communications.

### 2.3.1 Status and overview

Recent years we have seen rapid development in the number of legal acts and other regulations that have an impact on the internet area. At the international level, this takes the form of new EU legislation, while the national development is through consultation processes and legislative amendments. Below, Nkom presents regulations and processes that particularly affect the national electronic communications authority.

First, selected topics regarding national development are identified under section 2.3.2, before individual EU legal acts are presented in section 2.3.3 et seq. The overview is not exhaustive, but illustrates both the scope and how the regulatory context is relevant for Norwegian consumers and businesses on the internet.

### 2.3.2 National development

One of the key EU regulations for the electronic communications sector is Directive (EU) 2018/1972 of 11 December 2018 laying down a European regulatory framework for electronic communications (the Electronic Communications Directive). The Directive revised and amended the European framework for electronic communications and is intended to stimulate investment in and the rollout of very high-capacity networks, strengthen the internal market and strengthen end-users' rights. The Directive also expands its scope to include number-independent interpersonal communications services, i.e. person-to-person communications services delivered via the internet. The Ministry of Local Government and Regional Development has conducted a consultation process on the proposal for a new Electronic Communications Act, which, among other things, will implement the Directive in Norwegian law.

The Norwegian data centre industry is growing, and the use of data centres is increasing. The data centres are a key element of the digital infrastructure, and it is therefore important to also ensure adequate security for these. The Ministry of Local Government and Regional Development has consulted proposals for legislative amendments to the Electronic Communications Act that will set requirements for the data centres' security and preparedness.

Protection of electronic communications is also changing, both within the EU and nationally. The new ePrivacy Regulation is still under consideration in the EU/under negotiation in the EU (trilogue negotiations). The European Commission has proposed a regulation on the prevention and combating of child sexual abuse (CSAM). The proposal requires relevant internet-based service providers to detect, report, prevent and remove material depicting sexual abuse of children from their services, as well as the establishment of a EU Centre on Child Sexual Abuse. The Norwegian Ministry of Justice has been consulted on the proposal and will assess the proposal on the basis of the consultation input.

*Rules on IP address retention*

As from 1 January 2023, internet access service providers are subject to a statutory obligation under Section 2-8 a of the Electronic Communications Act to retain the information necessary to identify their subscribers based on public IP addresses, time of communication and, if applicable, port number if shared IP addresses (NAT solutions) are used. The retention obligation is for 12 months and the retention of destination information is explicitly prohibited. Under Section 2-8 b of the Electronic Communications Act, providers must disclose such information to the police and prosecuting authority upon their request. The disclosure obligation is limited to investigation of cases concerning serious crime and certain penal provisions, where IP address information is of particular importance to the investigation. Sections 7-6 and 7-7 of the Electronic Communications Act contain supplementary provisions to the statutory obligations. The retention and disclosure obligations are based on the need to establish an effective tool for fighting crime.

### 2.3.3 Digital Services Act (DSA)

The regulation entails essential new regulation of internet-based services and platforms, such as providers of online platforms, hosting services, caching services and mere conduit. The regulatory enforcement of DSA at the national level is particularly relevant, as a national Digital Services coordinator will be appointed who will have formal responsibility for all regulatory enforcement of the regulation. In addition, one or more national competent authorities may be appointed, with responsibility for sectoral supervisory tasks. At the international level, the European Commission will supervise the very large online platforms (VLOPs) and very large online search engines (VLOSE).

The DSA was published in the Official Journal on 27 October 2022 and took effect on 1 November 2022. The regulations formally entered into force on 16 November 2022, and on 25 April 2023, the first very large platform providers in the single market were designated by the European Commission.[31] The next major milestone is 17 February 2024. The obligations under DSA will then enter into force in full, and within this deadline all member states must have appointed a national Digital Services coordinator and competent authorities.

Nkom is the relevant authority for fulfilling the role of Digital Services coordinator, and as one of the competent authorities. In the preparations for the introduction of DSA in Norway, Nkom contributes actively to several areas, including as part of the inter-ministerial cooperation at national level, and extensive dialogue with other sectoral regulatory authorities, as well as international participation in working groups administered by the European Commission, and other networking and meeting points with European regulators of electronic communications. Nkom is also national representative in the Digital Services Expert Group.

### 2.3.4 Digital Markets Act (DMA)

DMA, like DSA, is an essential new regulation of internet-based services and platforms. The purpose of DMA is to designate gatekeepers on the internet who provide core platform services. Examples of such services are search engines, video-sharing platforms, operating systems and web browsers. The designation of gatekeepers follows an assessment of a set of qualitative and quantitative criteria, including annual turnover and the number of active users in the European market. The regulatory enforcement of DMA will mainly take place at European level, with the European Commission as the regulatory authority. At the same time, an important aspect of the regulation will be contact with national regulatory authorities and cooperation within the High-Level Group consisting of representatives from European regulatory bodies.

[31] DSA: Very Large Online Platforms and Search Engines (europa.eu) (Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando).

DMA was published in the Official Journal on 12 October 2022 and took effect on 1 November 2022, at the same time as DSA. Since the regulation entered into force, the European Commission has held several technical workshops on various regulatory issues, such as interoperability[32], self-preferencing own services[33] and app stores.[34] Furthermore, the High-Level Group was formally appointed by the European Commission on 23 March 2023.[35]

Nkom expects a role in the European enforcement of DMA, primarily through active participation in BEREC, which is represented in the High-Level Group. DMA is in practice an ex ante regulation of the gatekeepers, which has several similarities with today's market regulation of mobile and broadband markets. Several terms and conditions in DMA are thereby closely related to other regulations whereby Nkom is or will become a competent authority in the Norwegian market.

### 2.3.5 Data Act (DA)

DA is one of the legislative initiatives following-up the European Commission's 2020 Data Strategy. The purpose of DA is mainly to regulate who can access which types of data, and on what terms. Consumers and businesses will thereby more easily access data generated by their connected products and services, and public agencies will more easily access data in crisis situations. It will also be easier to move data between providers (data portability) and use data across multiple sectors (interoperability).

A DA proposal was announced by the European Commission on 23 February 2022. The proposal has been considered by both the European Parliament and the Council of the EU, which submitted their legislation proposals in the spring of 2023. Trilogue negotiations are expected to start during Q2 2023.

The Act has thereby not been adopted and has not entered into force. Nkom nevertheless expects to be the competent authority for elements of the regulation. Based on the proposal from the European Commission, issues concerning portability between providers and interoperability may be relevant regulatory tasks for Nkom in the national market. The interoperability obligations in DA are also related to the requirements in DMA, cf. above. It may thus be important to see these two regulations in context, even though, as mentioned, DMA will be enforced by the European Commission.

### 2.3.6 Artificial Intelligence Act (AI Act)

On 21 April 2021, the European Commission presented a legislative proposal concerning artificial intelligence. The proposed regulation is now being considered by the European Parliament and the Council, and a new EU body (European Artificial Intelligence Board) will be established to assist the European Commission and also cooperate with national supervisory authorities in monitoring follow-up of the regulation. Formal approval of the regulation by the European Parliament and the Council is expected before the end of 2023. If the Artificial Intelligence Act is adopted at EU level, it will probably be deemed to be EEA-relevant, and will thereby have to be incorporated directly in Norwegian law.

The concern that spread particularly in the spring of 2023 about the rapid and sometimes uncontrollable launch of more user-friendly AI systems is partly due to a lack of transparency, regulation and enforcement. The purpose of the AI Act is to establish a European legal framework for the use of artificial intelligence. In order to achieve this, an agreed definition of "AI systems" is a necessary prerequisite. Attempts have been made to make the proposed definition as technology-neutral and future-oriented as possible, in order to take account of the rapid development in artificial intelligence. The key elements are that, for a given set of human-defined goals, either machine

[32] Interoperability workshop (europa.eu)

[33] Self-preferencing workshop (europa.eu)

[34] App stores workshop (europa.eu)

[35] Digital Markets Act: Commission creates High-Level Group to provide advice and expertise in implementation | Shaping Europe's digital future (europa.eu)

learning or a logic- and knowledge-based approach is used to generate various outputs, such as content- or decision-making.[36]

The proposed regulation is built on a risk-based approach. This means that AI systems that pose an unacceptable risk must be prohibited, while specific requirements will apply to AI systems that entail a high risk to life and health, safety or fundamental rights.[37] Operators of such AI systems must also be subject to strict obligations with regard to, among other things, documentation, transparency and human supervision. The European Commission will establish a system for the registration of high-risk stand-alone AI systems in an EU-wide public database.

Norway has a tradition of avoiding regulation of specific technologies, but instead regulating unwarranted use, and has therefore supported the EU's approach to the regulation of artificial intelligence.[38] It will be important to find the right balance in the regulation. On the one hand, there must be agreement on the minimum requirements necessary to address the risks and challenges of artificial intelligence, while on the other hand there is no wish to limit or impede technological development and innovation.

For AI systems that only present a limited or minimal risk, certain transparency obligations will apply, and in cooperation with the member states, the EU will develop various industry standards. The proposed regulation calls for operators to ensure that AI systems intended to interact with humans are designed in such a way that the physical person is informed about the interaction with the AI system. Furthermore, the EU proposes requiring users of AI systems that generate or manipulate image, audio or video content to disclose that the content has been artificially generated, if the content noticeably resembles existing people, objects or events, and incorrectly appears authentic.

The Norwegian government has recently started work on a new digitalisation strategy that will discuss, among other things, the need for better regulation of new technologies, such as artificial intelligence, and the relationship with the big tech companies. The Ministry of Local Government and Regional Development will coordinate the work, and it is scheduled to be ready during the first half of 2024.

### 2.3.7 The Cyber Resilience Act (CRA) and the Radio Equipment Directive

On 15 September 2022, the European Commission presented a proposal to regulate cybersecurity requirements in products with digital elements and software (the Cyber Resilience Act, CRA). The scope of products covered by the proposal is very broad and will apply to everything from smartwatches and toys to routers and firewalls, as well as software used in the products.

The bill aims to reduce vulnerabilities in products placed on the market in the EU/EEA and ensure that manufacturers are responsible for the cybersecurity of their products throughout the product life cycle. In the proposal, the European Commission points out that it is important to set requirements that will apply to the entire life cycle of products, as vulnerabilities in software increasingly serve as a channel for cybersecurity attacks and generate significant societal and economic costs. The regulation will apply to all products connected either directly or indirectly to another device or network. The regulatory initiative is being considered by the Council of the EU and the European Parliament.

At the same time, cyber security requirements have also been laid down in the Radio Equipment Directive (RED), which will apply from 1 August 2024. The CRA proposal calls for the requirements in CRA to replace the cybersecurity requirements in RED.

Nkom supports the regulation proposal and believes that the introduction of cybersecurity requirements in products and software will contribute to increased cybersecurity.

[36] See proposed definition in Article 3(1) of the Artificial Intelligence Act.

[37] See examples of already defined "high risk" AI systems in Annex III to the Artificial Intelligence Act.

[38] Norwegian Position Paper on the European Commission's Proposal for Artificial Intelligence Act.

### 2.3.8 The NIS Directives

The NIS2 Directive (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a common high level of security in network and information systems throughout the Union and repealing Directive (EU) 2016/1148)) was adopted by the EU in December 2022, and its implementation deadline is 18 October 2024. The Directive replaces the NIS Directive. A proposal for a Digital Security Act that will implement the NIS Directive in Norwegian law, and a consent proposition, were sent to the Norwegian Parliament (Stortinget) on 5 May 2023.

The NIS Directives will ensure a high common level of security in network and information systems throughout the EU. A new feature in NIS2 is, among other things, that the range of sectors falling within the scope of the Directive is expanded, so that e.g. electronic communications networks and services fall within the scope of the Directive. In addition, the requirements concerning security and notification to the providers covered are strengthened, and a risk management method based on a minimum list of security elements is established, as well as, among other things, addressing security in the supply chain. The Directive will strengthen cooperation between authorities.

Digital infrastructure is one of the sectors of particularly critical importance, and includes interconnection point providers, DNS service providers (excluding root name servers), top-level domain name administrators, cloud service providers, data centre providers, content delivery network providers (CDNs), trust service providers and providers of public electronic communications networks and services.

For some of the providers of digital infrastructure, the Electronic Communications Act will already set out security requirements that to a great extent correspond to the requirements pursuant to NIS2, which Nkom is responsible for supervising. This currently applies to providers of electronic communications networks and services, and equivalent security requirements have been proposed for data centre providers.

### 2.3.9 eIDAS

The EIDAS Regulation is intended to increase confidence in electronic services and transactions in the internal European market. It consists of two parts, of which the first part regulates electronic identification (eID) and the second part regulates trust services, such as electronic signature and time stamping.

In June 2021, the European Commission presented a proposal for a revised version. They published a report concluding that the regulation had not met the requirements set when the regulation was drafted, and a number of changes were proposed. In addition to new trust services, a closer link to other European regulations, such as the new NIS2 Directive, has been established.

The biggest change is the introduction of a digital wallet to be offered free of charge to all citizens. This solution is intended to function across member states, regardless of where it is issued. The digital wallet is intended to contain a number of electronic attributes and documentation, which must be usable throughout the EU.

Nkom is designated as a supervisory body pursuant to the Electronic Trust Services Act and currently carries out a number of activities related to this role. It is to be expected that there will be additional supervisory tasks associated with the introduction of the revised regulation.

## 2.4 The geopolitical picture

### 2.4.1 Introduction

The internet plays an important geopolitical role. This applies to how large platform and content providers influence the internet ecosystem, how the international rules for governance of the internet are formulated, and how the internet is exploited in war and conflict. Last but not least, the internet and digitalisation are of great importance for how the Sustainable Development Goals can be achieved. These matters are examined further in this chapter.

### 2.4.2 The internet ecosystem

The internet architecture and ecosystem are constantly evolving, and there is a close interdependence between content and platform providers and internet service providers. In 2021/2022, ETNO's members launched the "fair share" proposal, which has led to a new debate on the charging for interconnection between platform providers and internet service providers. The European Commission's consultation on this issue in the spring of 2023 will take the debate a step further.

Concerning conditions in the Norwegian market, in the spring of 2023, Nkom held dialogue meetings with the major internet service providers, which showed that the status of the Norwegian market is more reconciled. The interconnection regime in Norway today functions with relatively few conflicts.

The internet architecture and ecosystem have gradually evolved in recent years and in December 2022, BEREC published a new report on the internet ecosystem[39]. The report presents a model of the internet ecosystem that illustrates the interdependencies between the various players in the ecosystem, such as electronic communications providers and platform providers.

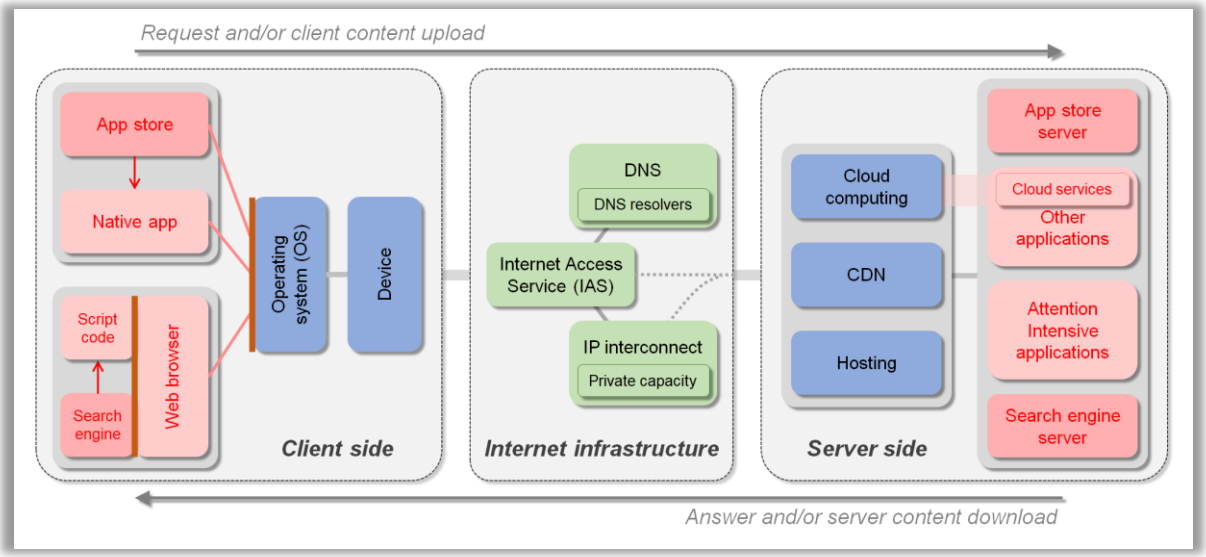



*Figure 15 - The internet ecosystem (source: BEREC[39])*

[39] BEREC Report on the Internet Ecosystem, BoR (22) 167, 12 December 2022

The global internet comprises tens of thousands of networks in a hierarchical architecture. For communication over long distances, traffic will be sent through many networks on the way from sender to receiver. This can lead to latency, which is a disadvantage, especially for real-time traffic.

Technological improvements to address this are increasingly being used, including caching and the establishment of private, dedicated capacity in parallel with internet's public, shared infrastructure. This has resulted in a more "flat" internet with a shorter distance between users and content.

The introduction of CDN, cloud services and data centres has given new players in the market. Furthermore, the establishment of private, dedicated capacity contributes to intensified competition between internet service providers and content providers. The platform providers have built extensive transmission capacity in parallel with the internet infrastructure, to interconnect their geographically distributed data centres.

Interconnection between platform providers and internet service providers is at the heart of the "fair share" debate. In 2021/2022, the members of ETNO (European Telecommunications Network Operators' Association) launched the "fair share" proposal[40] proposing that large platform providers should pay more for interconnection with internet service providers.

BEREC has presented a number of counterarguments[41]: It is not the platforms that generate traffic, but rather the internet service providers' own customers who control the downloading of traffic. Without the content of the platforms, internet service providers would offer "empty" services, and internet service providers would be reimbursed for their costs on the basis of their customers' subscription payments. As the model of the internet ecosystem illustrates, there is therefore an interdependence between internet service providers and content providers.

The European Commission's consultation on this issue[42] will take the debate a step further. Concerning conditions in the Norwegian market, in the spring of 2023, Nkom held dialogue meetings with the major Norwegian internet service providers. This show that the status of the Norwegian market is more reconciled, and that today's interconnection regime functions with relatively few conflicts.

### 2.4.3 Internet governance

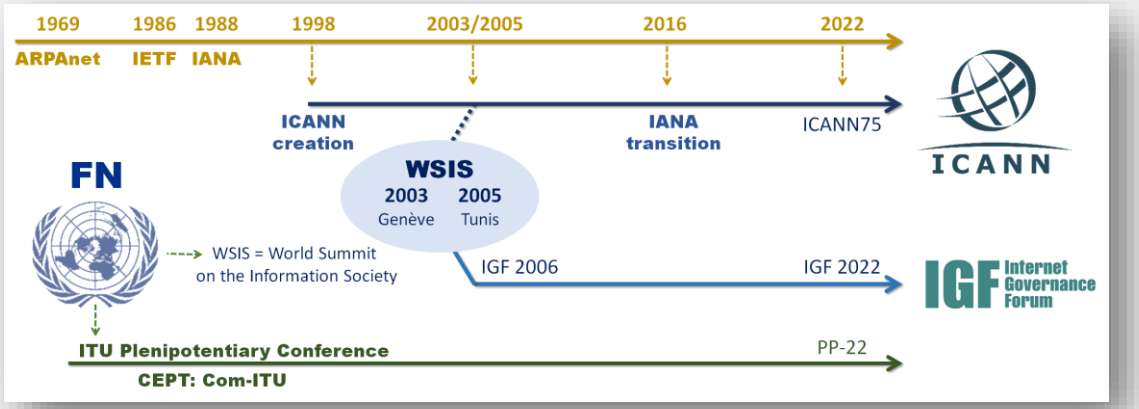
Nkom assists KDD with Norway's participation in international internet governance within organisations such as ITU and ICANN. During the ITU's Plenipotentiary (PP-22), history was made when Doreen Bogdan-Martin of the USA was elected as the ITU's first female secretary general in October 2022. Changes are also on the way at the top of ICANN. At the ICANN meeting in March 2023, ICANN Board gave a briefing on the commencement of the process related to the appointment of a new CEO of ICANN org.

The internet requires international coordination to function. This coordination is referred to as internet governance. Nkom assists KDD with Norway's participation in international internet governance in order to safeguard Norwegian interests. In 2022, KDD and Nkom attended the ITU's Plenipotentiary, PP-22. Nkom also participates as a representative for Norway in the Governmental Advisory Committee (GAC) at the regular meetings of ICANN.

[40] Joint CEO Statement, published on etno.eu, 29 November 2021

[41] BEREC preliminary assessment, BoR (22) 137, 7 October 2022

[42] Commission exploratory consultation, published 23 February, consultation deadline 19 May 2023.




How internet governance is organised reflects the historical development from the internet's origins as an American research network up to the current situation. In 1998, the USA established **ICANN** (Internet Corporation for Assigned Names and Numbers) to facilitate international participation in internet governance. ICANN currently manages IP addresses and top-level domain names.

In 2003 and 2005, the UN organised the **WSIS** (World Summit on the Information Society). The issue of internet governance was high on the agenda. At the 2005 meeting, it was agreed that ICANN would retain control of the technical internet coordination, but that a forum for internet governance within the UN, called the Internet Governance Forum (**IGF**) would be established.

In line with the increasing importance of the internet, the UN International Telecommunication Union **(ITU)** has become increasingly concerned with the internet in its work. This is also reflected in the Plenipotentiary held every four years, where discussion of internet governance is high on the agenda.

*Figure 16 - Timeline for international internet governance*

*ITUs Plenipotentiary (PP-22):*

Doreen Bogdan-Martin of the USA made history at the ITU Plenipotentiary (PP-22) when she won the battle for the top post against her Russian opposing candidate and became the ITU's first female secretary general. The Plenipotentiary is the highest body of the ITU and is held every four years, this time from 26 September to 24 October 2022 in Bucharest, Romania. Over 3,000 delegates attended, comprising 184 member states, over 60 sector members and other UN agencies. Norway's delegation was led by KDD with representatives from Nkom, UD, Norid, Telenor and RIPE.

Internet governance is an important topic in the ITU context. The internet resolutions, which include networks, the transition from IPv4 to IPv6 and domain names, were characterised by a great distance between the different regions of the world. This resulted in long and demanding negotiations. The wish of other countries and regions to strengthen the ITU's role in internet governance, in contrast to Western countries' opposition to this, made the negotiations polarised and at times stagnant.

Nonetheless, the negotiations during PP-22 proceeded better than expected. The overall result only entailed minor changes that were considered acceptable from a European standpoint.

*ICANN and Governmental Advisory Committee*

At the ICANN meeting in March 2023, ICANN Board gave a briefing on the process related to the appointment of a new CEO of ICANN org, the administrative organisation of ICANN. American Sally Costerton is currently the acting CEO after Sweden's Göran Marby's resignation at the beginning of the year. ICANN Board wants a transparent and inclusive appointment process, in which all ICANN stakeholder groups will be consulted. Then a selection of Board members will form a recruitment group, which will assist in the process of appointing a new CEO. The process is expected to be completed at the turn of the year 2023/24.

The preparations for a new round of applications for generic top-level domains (.com, .net, .shop, etc.) are entering a final phase. At its March meeting, the ICANN Board endorsed the majority of the recommendations of the Generic Names Supporting Organization (GNSO). The last outstanding points are scheduled to be presented to the Board at the next ICANN meeting in June. The recommendations from GNSO have been prepared in cooperation with other groups under ICANN, including GAC.

DNS abuse is also high on the agendas at the organisation's meetings. At the meeting in March, the focus was on development trends and competence development to combat DNS abuse. Among other things, information was shares about contract negotiations with registries and registrars for generic top-level domains, with the aim of increasing protection against DNS abuse. A new tool (acidtool.com) for identifying the relevant contact person for reporting abuse related to generic top-level domains was also presented.

### 2.4.4 Internet security in a global context

The internet is exploited for security attacks, digital sabotage and impact operations, and plays an important role in a global security policy. From the war in Ukraine, for example, we have seen rerouting of internet traffic in occupied areas, and how DDoS attacks against Norwegian targets have been used by pro-Russian hackers to generate media attention in Norway. For its part, the Norwegian government has implemented several measures to strengthen national control and digital resilience in the face of an escalating threat picture.

In a digitalised world, technology and technology development are high on the security agenda. Here, the internet plays a central role, as most of the digitalisation is based on the internet infrastructure and the internet ecosystem.

More and more assets important to national security are managed in the digital space. In December 2022, the government presented a report to the Norwegian Parliament[43] on digital resilience to safeguard national security. A key aspect of the government's strategy is to strengthen *national control* in the face of digital cross-border and international infrastructure, services and market participants.

The report points to regulation as a key instrument, cf. the Security Act, the incorporation of data centre operators into the Electronic Communications Act, and the new Digital Security Act (see Chapter 2.3). Other measures mentioned in the Report to the Norwegian Parliament are the investigation of cloud services under national control for processing and retention of public administration data, the establishment of an expert committee to investigate safeguarding national control of critical communications infrastructure, and a scheme to identify threats to submarine fibre cables.

In its latest threat assessment[44] PST points to how the war in Ukraine has fundamentally changed relations between Russia and other Western countries, including Norway. This also affects the Russian

[43] Report to the Norwegian Parliament no. 9 (2022-2023) - *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet* (National Control and Digital Resilience to Safeguard National Security).

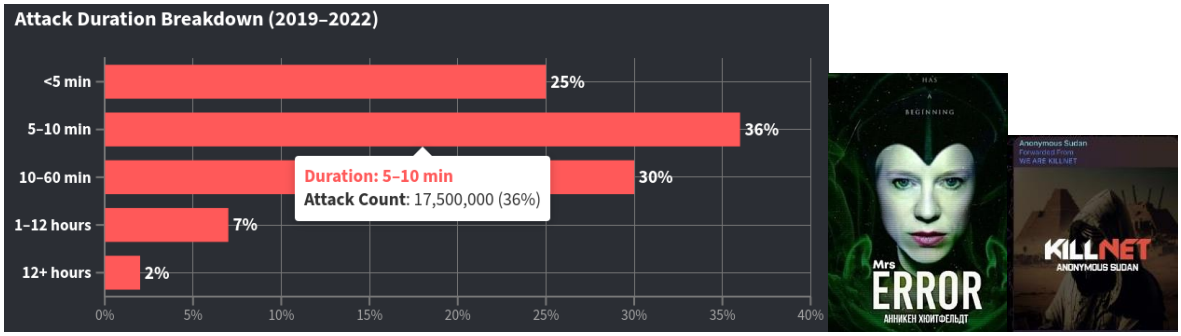
[44] *Nasjonal trusselvurdering 2023* (National threat assessment, 2023), Norwegian Police Security Service, 2023.

intelligence threat to Norway. The threat from other countries is assessed to be stable. Several of the relevant intelligence methods and instruments are internet-based in the form of network operations, digital sabotage and impact operations. Below are some examples from 2022.

*Denial of Service (DDoS) as an impact method*

The introduction of "DDoS-for-hire" services around a decade ago led to a fundamental shift in the threat landscape. For the first time, attackers could relatively easily, on a risk-free basis, "order" DDoS attacks on specific networks, organisations and individuals. This has resulted in significant downtime for many websites.

Since then, the ability of businesses to defend themselves has increased. At the same time, DDoS attacks have continued to increase both in size and number. The frequency is estimated to have increased by over 800% in the period, yet over 90% of the attacks last for less than an hour.




*Source: https://www.netscout.com/threatreport/ddos-threat-intelligence-report/#attack-timeline*

Pro-Russian hacker groups have been active in the media during the past year. The groups carry out DDoS attacks against well-known businesses. The feature of these attacks is that they are advertised on the hacker groups' telegram channels together with the method of attack to be used. The direct consequences of the attacks are therefore limited. The key motive seems to be the impact, since media reports on the incidents contribute to spreading fear and uncertainty in the population.

In Norwegian media, we initially saw major stories when Norwegian businesses were affected, such as in the summer of 2022, when the police, NAV and Digdir were attacked. The Minister of Foreign Affairs was depicted as a Maleficent mask from the Disney movie of the same name. There have been similar attacks against pro-Ukraine targets around the world, including attacks against healthcare institutions and critical government functions. The press has gradually toned down reports of such attacks.

*Routing of internet traffic in war zones*

The war in Ukraine has affected how internet traffic is routed, including the assignment of IP addresses and registration of ownership of the IP addresses. One of the biggest changes after the outbreak of the war came in the form of new rules for the transfer of address blocks between actors. For Europe, the allocation of address blocks is administered by RIPE.

An early concern at the outbreak of the war was whether internet service providers operating within occupied territory could be forced to transfer blocks of addresses to the occupying forces. The possibility of temporary administrative locking of address resources registered in RIPE database was therefore introduced at an early stage. When enabled, the lock will prevent transfer to another administrative unit through a "policy transfer". The lock remains active for six months and cannot be removed until that time has passed.

Correct, up-to-date registration of IP address ownership information is important. This reduces the possibility of misinterpretations and misunderstandings that can escalate the level of conflict. When address resources are clearly associated with the registered entity, it will also be easier to determine whether a transfer of the resources is legitimate or not. This helps to avoid situations where resources might be unlawfully taken over or misused during conflicts.

This became evident during the invasion, when a Russian-owned ISP terminated an agreement to lease an address block to a Ukrainian ISP. The reversal led to speculation as to whether the transfer was legitimate or was a means to re-route traffic via Russia.

The war has also brought increased focus on the use of RPKI to increase security related to routing on the internet. RPKI is a security mechanism to cryptographically verification that routing information as advertised by the networks is legitimate and authorised. In recent years, both advertising and verification of such signatures have increasingly been adopted by internet service providers.

| | 2020 | 2021 | 2022 | 2023 |
|---|---|---|---|---|
| **World** | 18% (23%) | 26% (30%) | 29% (33%) | 37% (35%) |
| **Norway** | 30% (43%) | 43% (55%) | 48% (55%) | 51% (58%) |
| **Ukraine** | 12% (23%) | 40% (42%) | 47% (49%) | 47% (61%) |

*Table 1 - Proportion of RPKI-signed routes for IPv4 (IPv6) at the beginning of each year.*[45]

### 2.4.5 Sustainability and the green transition depend on access to the internet

The green and digital future, also referred to as the twin transitions, is a major upheaval currently taking place and that in combination could help reduce global greenhouse gas emissions from heavy greenhouse-gas emitting industries by up to 20% before 2050.

For this to be achieved, the technology must be connected to the internet in some form. The digital foundation is becoming an increasingly important infrastructure. The EU and the UN, among others, emphasise the importance of understanding the connections between digitalisation and sustainability, in terms of own emissions, as well as the benefits that can be reaped in the green and digital future.


As described earlier in the report, Norway had growth of around 20-30% in internet traffic on both fixed and mobile networks. Streaming services are the biggest traffic driver, accounting for around 70% of network traffic. This growth is expected to continue in the years ahead. We live in a time characterised by major changes and geopolitical unrest. Digitalisation is a premise for achieving major efficiency gains that are expected to result in significant reductions of greenhouse gas emissions.

Several studies[46] show that increased digitalisation can help reduce greenhouse gas emissions from heavy greenhouse-gas emitting industries, such as energy, materials and transport industries, in the order of 15-20%. Accenture, together with the World Economic Forum, has compiled several research reports showing how digitalisation can be used to reduce greenhouse gas emissions.

[45] Route Origin Authorisation (ROA) statistics by APNIC, 2020, 2021, 2022 and 2023

[46] Europe's green commitment indicates around a 15% reduction. GSMA studies estimate up to 20%. https://www.weforum.org/agenda/2022/05/how-digital-solutions-can-reduce-global-emissions/

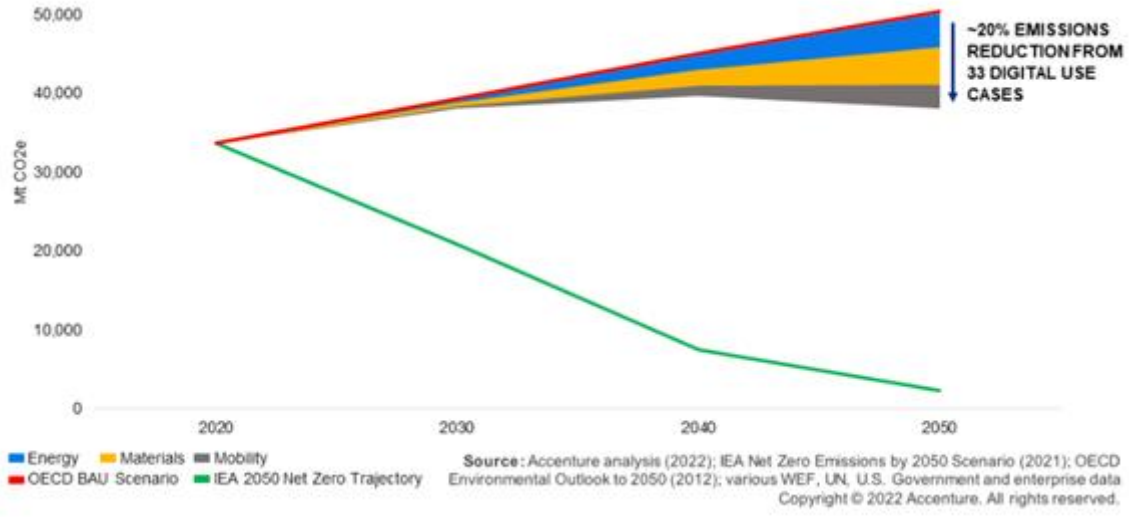



*Figure 17 - Digital solutions can accelerate net zero in high emission industries (source: WEF[47])*

The figure below shows how the various different types of technologies have different roles in reducing greenhouse gas emissions. All of these technologies must be connected to the internet in some form or other.

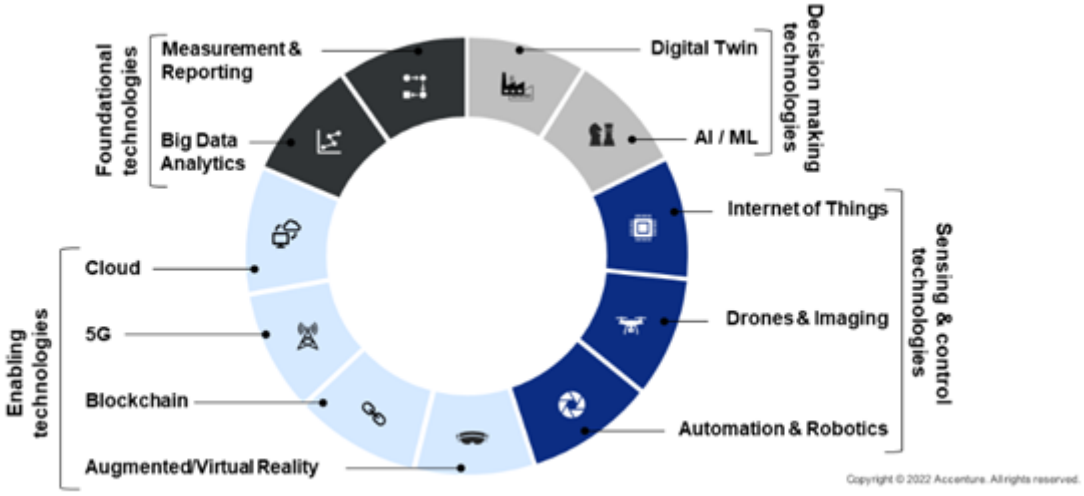



*Figure 18 - Four clusters of digital technologies that could drive decarbonisation (source: WEF[47])*

On the other hand, the digital sector's own climate and environmental footprint is increasing. An increasingly more connected world is leading to huge growth in internet traffic, which in turn generates a demand for more energy. Cabling routes must be established, the number of base stations must be increased, data centres must be established, and equipment and backup power must be produced, while access to rare metals and minerals will be more difficult to obtain.

[47] World Economic Forum, https://initiatives.weforum.org/digital-transformation/climate-scenarios

> *"Demand for digital services is growing rapidly. Since 2010, the number of internet users worldwide has more than doubled, while global internet traffic has expanded 20-fold. Rapid improvements in energy efficiency have, however, helped moderate growth in energy demand from data centres and data transmission networks, which each account for 1-1.5% of global electricity use."*[48]

Gains related to energy efficiency from new and less energy-intensive technologies and equipment can limit the increase in energy consumption and thereby also associated greenhouse gas emissions. One example is the use of artificial intelligence that can reduce energy consumption in 5G mobile networks by 40%[49].

As described earlier in the report, much of the data processing that industry and business depend on to create value, as well as virtually everything we do on a PC or a smartphone, will pass through a data centre or CDN. Together with electronic communications networks, data centres account for a large proportion of greenhouse gas emissions from the ICT sector's global footprint[50].

Norway markets green data centres as most of the energy comes from renewable resources such as hydroelectric power. It is also important to be able to recover waste heat produced by cooling and to use AI to optimise power consumption and design circular products[51].

Understanding the connections between digitalisation and sustainability is crucial if we are to succeed in achieving the climate goals. But being sustainable must also be balanced, so that it does not compromise the security of the networks. The complexity of the value chains in the internet ecosystem, and understanding their environmental impact, robust assessment methods and common sustainability indicators based on standardised data, are required by the industry.

It is therefore important to have a good understanding of the impact that electronic communications networks and the digital sector can have, and which measures can be taken to balance the footprint. Promoting sustainability in the ecosystem requires greater responsibility to be taken by all relevant parties in the digital value chain.

---

[48] Data Centres and Data Transmission Networks, IEA report, published September 2022.

[49] New research project demonstrates AI reduces energy consumption in Tele2's 5G network.

[50] Devices contribute the largest share (60-70%) to the ICT sector's global footprint, while networks (12-24%) and data centres (15%) contribute less. The partition should not omit interdependencies between these bricks. Source: BEREC Report on Sustainability: Assessing BEREC's contribution to limiting the impact of the digital sector on the environment.

[51] Examples from GlobalConnect, Leva Martinkenaite, head of Telenor Research & Innovation, and Energy Valley: Building data centres with up to 90% less energy consumption.