Norwegian
Communications
Authority

Internet in Norway – Annual report 2022

June 2022

Table of Contents

Summary – Internet in Norway 3

1 Status of net neutrality in Norway 5

1.1 Introduction and background 6

1.2 Zero-rating in Norway 7

1.3 Traffic management and specialised services 10

1.4 Net neutrality and security 11

1.5 Transparency about the internet access service 13

1.6 Quality of the internet access service 15

2 Core functions of the internet in Norway 21

2.1 Introduction and background 22

2.2 Infrastructure and traffic development 22

2.3 Adoption of IPv6 27

2.4 Domain name system 30

2.5 Internet of Things (IoT) 34

2.6 Internet security 36

2.7 Internet-based services and platforms 39

2.8 Internet governance 41

Summary – Internet in Norway

"Internet in Norway – Annual Report 2022" is the first edition of the Annual Report.

Part 1 of the report describes the state of net neutrality in Norway. Net neutrality is the principle that all internet communications must be treated equally, regardless of sender, recipient, equipment, application, service or content. Annual reporting on net neutrality is a statutory task for Nkom based on the Open Internet Regulation.

Part 2 of the Annual Report describes the status of the core internet functions in Norway, covering such functions as infrastructure, traffic development, interconnection and the transition from IPv4 to IPv6, as well as the domain name system's resolvers and authoritative servers. This year's Annual Report establishes a basis to map the development of the internet's core functions in the years ahead.

Zero-rating in Norway

During the five years in which the Open Internet Regulation has applied, Nkom has followed the development of zero-rating closely. In the first few years, the scale of the practice increased year-by-year, while this year there is a decrease. Meanwhile the proportion of end-users with a large data allowance has increased in recent years, which limits the effect of zero-rating. Based on an overall assessment, Nkom believes that the zero-rating does not have significant adverse effects in the Norwegian market today.

BEREC's open internet guidelines used by Nkom for the regulatory assessment of zero-rating are being revised this year on the basis of new rulings from the European Court of Justice. As a consequence, zero-rating will be phased out of the market by the end of 2022.

Net neutrality and security

Nkom observes that the provision of security protection for internet access is increasing. This development is predictable, in view of the extent of malware, fraud and other security threats on the internet. In addition to the two specific service offerings: Telenor "Nettvern" and GlobalConnect "SafeSurf", Nkom will monitor this development going forward. In November 2021, Nkom published a memorandum of principle which discusses the trade-off between net neutrality and DNS blocking, with further guidance for the internet service providers.

Quality of the internet access service

Nkom monitors the development in the quality of the internet access service in the Norwegian market. Clear positive development in the speed of fixed internet access can be seen. The average download and upload speeds for fixed internet access have increased by 19% and 22%, respectively, since last year. The speed of internet access via the mobile network also shows positive development. The mobile providers appear to be able to meet demand.

For 4G, the average download speed has increased by 34% since last year, while the upload speed has shown a marginal increase. For 5G in Norway in 2021, the average download speed was 365 Mbit/s (4G: 65 Mbit/s), and the average upload speed was 39 Mbit/s (4G: 14 Mbit/s), while the average latency was 28 ms (4G: 44 ms). So far, 5G traffic accounts for a small proportion of the total, and it will be interesting to see whether the networks keep step as coverage is expanded and more customers have 5G-ready handsets.

Internet interconnection

An important core function of the internet is interconnection. In Norway, internet service providers exchange traffic between their networks at interconnection points that are mainly located in Oslo. Most of the traffic is exchanged at private interconnection points. In addition, the Norwegian Internet Exchange (NIX) public interconnection infrastructure interconnects more than 70 small and large internet service providers.

Internet interconnection in Norway is evolving. As the deployment of closed solutions driven by large data centre and platform providers expands, Nkom considers it important to further develop open, neutral and regional interconnection solutions. This has both competitive and security advantages.

Transition from IPv4 to IPv6

In 2022, Norway has an Pv6 adoption of 22.2%, thereby ranking 35th in the world. In October 2020, Norway was in 29th place with an adoption of 18.1%. Norway has thus dropped 6 places on the list in the course of one and half years. Meanwhile, the percentage IPv6 adoption has improved and increased by around 4 percentage points. At European level, Norway is in 14th place.

This means that providers in a number of other countries are increasing their IPv6 adoption faster than the Norwegian market. Nkom is monitoring the further development and emphasises the importance of providers in the Norwegian market facilitating the use of IPv6 to the fullest possible extent.

Development of the domain name system

New domain name resolution methods, called "encrypted DNS", have recently been adopted. One of these methods is DoH (DNS-over-HTTPS). Today's providers of DoH resolvers are mainly located outside Norwegian jurisdiction. There are several regulatory consequences of increasing use of open resolvers, including that public enforcement based on filtering of DNS resolution is enforced to a lesser extent.

The EU has launched the DNS4EU initiative to establish a European alternative to the major open American DNS resolvers. Nkom will continue to monitor the development of DNS4EU as the solution becomes available and will assess the possibility of Norwegian involvement and facilitation of the use of the service for Norwegian residents. In the longer term, this approach could contribute to strengthening the position of DNS resolvers within European jurisdiction.

Internet-based services and platforms

Greater use of internet-based services and platforms challenges existing legislation and requires legislation to be adjusted. Within the EU, a package of regulations, including the Digital Services Act and the Digital Markets Act, is currently being established. These are relevant to the EEA and could thereby be implemented in Norwegian legislation. New regulations will set the terms for consumers' and businesses' use of the internet.

The regulation of internet-based services and platforms requires cross-sectoral cooperation between government bodies. This is to ensure effective and consistent exercise of public oversight towards resourceful providers who play a dominant role within the internet ecosystem. Nkom will play an active role in this collaboration in view of our expertise as a regulator of electronic communication services in general, and net neutrality and predefined markets in particular.

1
Status of net neutrality in Norway

tech
BUSINESS
CULTURE
GADGETS
FUTURE
STARTUPS
Hot List
Facebook's Russia problem: What we know
4 ways the White House says tax reform will put money in workers...
North Korea oil embargo: Trump's plan is a long shot
SpaceX launches mysterious Air Force space plane ahead of Irma's...
Disney's dark side Stock tanks on earnings warning
Most Popular Videos
How a Rolls-Royce might look in 2114
Front camera
Dot projector

1.1 Introduction and background

Part I of the Annual Report describes the status of net neutrality in Norway. This is the first 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 2021 to 30 April 2022.

Net neutrality was codified by law in Norway with effect from March 2017 in connection with the introduction the Open Internet Regulation, in accordance with Regulation 2015/2120[1]. The purpose 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."[2]

The regulatory supervision of net neutrality is also based on BEREC's open internet guidelines, which have been established pursuant to Article 5(3) of the Regulation. In accordance with recital 19 of the preamble, the national regulatory authorities must "take utmost account" of relevant guidelines from BEREC in their application of the Regulation.

Part 1 of the Annual Report has the following structure: Chapter 2 describes access to an open internet via Norwegian providers' internet access services, and reports on assessments of existing zero-rating offers. Chapter 3 describes conditions related to technical traffic management in Norwegian providers' networks. Chapter 4 describes conditions related to security measures for the internet access that is provided. Chapter 5 describes how Norwegian providers communicate information about the internet access they offer. Chapter 6 describes the quality achieved for Norwegian internet access services, analysed on the basis of measurements using Nkom's Nettfart measurement service.

[1] | Regulation (EU) 2015/2120 of the European Parliament and of the Council.

[2] | First recital of the preamble to Regulation 2015/2120.

1.2 Zero-rating in Norway

In the Norwegian market, there is no indication of the introduction of zero-rating for new application categories. The proportion of end-users with large data allowances continues to increase, which limits the effect of zero-rating. The scale of zero-rating declined during the reporting period. At the same time, zero-rated music is increasingly streamed by users with relatively large data allowances. Based on an overall assessment of these development trends, Nkom believes that zero-rating in the Norwegian market does not have significant adverse effects.

BEREC's open internet guidelines used by Nkom for the regulatory assessment of zero-rating are being revised this year on the basis of new rulings from the European Court of Justice. As a consequence, zero-rating will be phased out of the market by the end of 2022.

Zero-rating is a form of price discrimination of selected applications compared to other applications. A typical example is that music streaming can be used without using the end-user's agreed data allowance. The internet service provider decides which applications are zero-rated.

Regulatory assessment of zero-rating is performed as an overall assessment based on the criteria set out in BEREC's open internet guidelines. As the guidelines are revised this year, future assessment of zero-rating will be based on criteria other than those that have been used in recent years.

1.2.1 Market position of the internet service providers

Nkom has previously assessed zero-rating offers from both Telenor[3] and Telia[4]. Both are called "Music Freedom", and include zero-rating of select providers of music streaming. In these instances, Nkom has expressed concern that the offers might have adverse effects, due to the two internet service providers' significant market position and potential influence.

The national electronic communication statistics for 2021 show that the duopolistic situation is continuing, since Telenor and Telia together have around 79% of the subscribers in the market for telephony-connected mobile services. In terms of revenue, the companies together have around 84% of the private market and 91% of the business market.

1.2.2 Impact on the content providers

Nkom generally believes that the zero-rating offers may affect the competitive conditions in the content market. This is because the positive price discrimination entails that using selected music applications may seem more advantageous to users than other applications for which content transmission "eats up" the data allowance.

[3] | Nkom report on Telenor's zero-rating of 29 June 2017

[4] | Nkom report on Telia's zero-rating of 18 December 2017

Telenor and Telia's offering of the zero-rated "Music Freedom" service includes music streaming services from Spotify, Tidal, Beat, Apple Music, Deezer and Audiomack. SoundCloud is also included in Telenor's offering. Nkom maintains our previous assessment that the number of content providers that are actually included in the zero-rating schemes is relatively limited, and that this mainly includes large, well-established providers.

Regarding the development of zero-rating of music streaming in Norway in recent years, the number of music streaming applications is relatively stable. Nkom has not received enquiries about issues with inclusion in the zero-rating schemes during the current reporting period.

1.2.3 Impact on end-users

Nkom believes that the zero-rating offers can affect end-users' real freedom of choice, in particular because data allowances in Norway are relatively small and relatively highly priced, compared to our neighbouring countries. When the data allowance included becomes relatively small, zero-rating will be more problematic than would have been the case with larger data allowances.

Nkom can observe that for several years, Norwegian mobile subscribers have had the lowest data consumption, according to Nordic-Baltic statistics. In countries where inclusion of unlimited data has a higher adoption, zero-rating will be less problematic. Below, total data consumption for mobile internet access in Norway compared to Sweden and Denmark is presented:

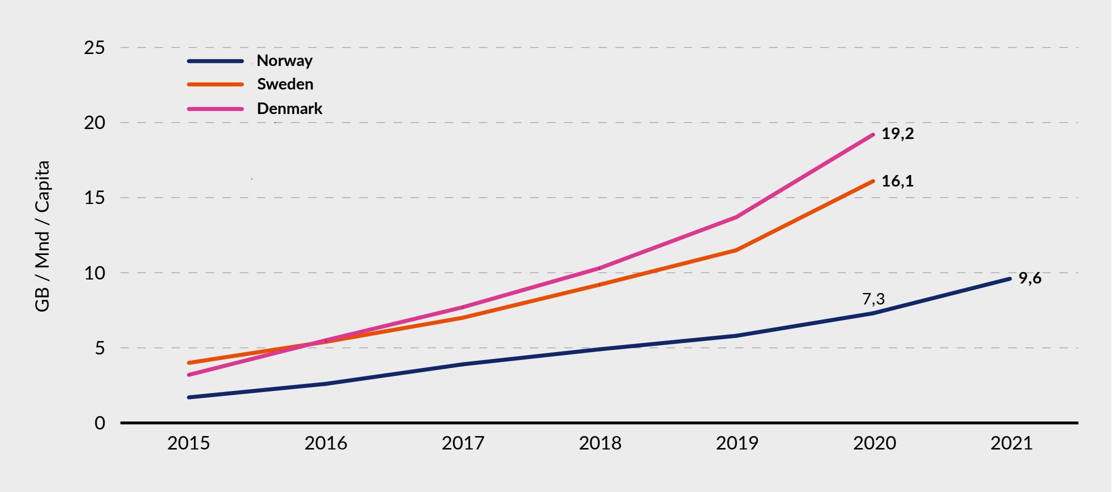

Figure 1: Total data consumption in mobile networks per month per capita measured in gigabytes (GB)

Norway is among the countries with relatively low data consumption in mobile networks, and also relatively high prices for subscriptions with unlimited data allowance. This implies that zero-rating is more problematic in Norway. When the data allowances are large enough, offers of zero-rated services will have a small impact on the choices made by users.

Mobile subscriptions with a higher data allowance have higher adoption in several other countries than in Norway. Table 1 below shows the proportional distribution of the total customer base (in the private market) per data allowance in Norway at the end of each year during the period from 2017 to 2021.

Allowance size	2017	2018	2019	2020	2021
No data included	23,1 %	19,3 %	16,5 %	14,0 %	14,2 %
From 0 to 1 included	7,2 %	7,6 %	6,0 %	6,4 %	5,1 %
From 1 to 5 included	45,6 %	43,7 %	45,2 %	41,2 %	33,0 %
From 5 to 10 included	16,2 %	16,3 %	16,6 %	17,5 %	15,6 %
From 10 to 20 included	6,5 %	6,6 %	7,5 %	9,9 %	14,8 %
Over 20 included	1,5 %	6,4 %	8,2 %	–	–
From 20 to 100 included	–	–	–	5,3 %	7,7 %
Over 100 included	–	–	–	5,7 %	9,6 %

Table 1: Distribution of total customer base (private) by monthly data allowance

The largest group of Norwegian end-users still have subscriptions with a data allowance of between 1 GB and 5 GB. The proportion of end-users with a data allowance in this interval has fallen significantly from 2020 to 2021, however. The trend indicates that the proportion of end-users who have allowances greater than 10 GB per month is increasing. The increase in 2021 is somewhat greater than the increase in the preceding years. The biggest increase in 2021 was for subscriptions with data allowances of between 10 GB and 20 GB.

During the past year, subscriptions with "free" data usage, i.e. allowances exceeding 100 GB, have had a higher adoption. Nkom can also observe that the market trend shows that large data caps have become less expensive since last year's net neutrality report. Nkom views this as a possible consequence of the regulation of the mobile market that came into force on 14 May 2020.

1.2.4 Scale of zero-rating

The increasing scale of zero-rating increases the number of end-users who are encouraged to use certain selected content providers. In last year's Annual Report, the scale of zero-rating was assessed to be limited, however. This was the main reason that Nkom, according to an overall assessment, found that there was no basis to give a mandatory order to rectify the zero-rating offers in the market. It is still the case that zero-rated services solely include Telenor and Telia's offer of "Music Freedom".

- Telia's "Music Freedom" zero-rating service is included in Telia X subscriptions, and for Telia Mobil customers who are aged under 29 (excluding Barn (Child) subscriptions). "Music Freedom" is also included in the Mobile Broadband 50 GB, 100 GB, 200 GB and 500 GB subscriptions. Other customers can purchase the service for NOK 29 per month. The service solely applies to streaming of music and downloading of playlists[5].
- Telenor's zero-rating service is also called "Music Freedom" and is included in the Fleksi, Yng and U18 subscriptions. The product can be purchased separately for NOK 49 per month by holders of Next, Original, Medium, Trygg (Safe) or Trygg Start (Safe Start) subscriptions.

[5] | https://www.telia.no/mobilabonnement/music-freedom/

During the reporting period, the proportion of private subscriptions with "Music Freedom" decreased from around 34% to 32%. Even though both Telenor and Telia offer the opportunity to buy "Music Freedom" separately (for NOK 49 and NOK 29, respectively) for certain other subscriptions, this only makes a small contribution to the customer base that has "Music Freedom". Telia reports that around half of the customers with "Music Freedom" have Telia X subscriptions. Telia X is a "free data use" subscription, which therefore makes zero-rating less relevant.

Overall for Telenor and Telia's customer base, the proportion of private subscriptions with zero-rating per monthly data allowance has developed as shown in the following table:

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

Table 2: Proportion of private subscriptions with zero-rating per monthly data allowance

As the above table shows, an increasing proportion of private customers with "Music Freedom" have a subscription with a monthly data allowance of 10 GB or more. To some extent, this trend offsets the negative effects of zero-rated services.

According to information from Telenor and Telia concerning the average consumption of zero-rated content, end-users with data allowances greater than 10 GB per month have the highest average data consumption of "Music Freedom". This also contributes to reducing the negative effects of zero-rated services.

1.3 Traffic management and specialised services

Nkom's collection of information from internet service providers shows no significant changes compared to last year in terms of traffic management of the internet access service, as well as the provision of specialised services in the market. Nkom has not performed any detailed scrutiny of the reported traffic management measures or specialised services, but assumes that these are offered in accordance with the Regulation. In the future, Nkom might initiate more detailed scrutiny of the measures.

1.3.1 Traffic management of internet access

As part of the data collection for the annual electronic communication statistics, Nkom obtained information from Norwegian internet service providers concerning the traffic management of internet access. This is in line with BEREC's recommendation. The results for this year do not differ significantly from the results for last year.

[6] On purchasing data packets of 10, 15 or 20 GB, subscriptions with no data allowance included, such as prepaid cards, will be included in the figures for the calendar month in which the data packets were purchased.

According to the information obtained, typical traffic management methods 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 cyber attacks).

In the Norwegian market, speed-differentiated internet access was observed for the first time, on Telenor's launch of "Next" in March 2021. In December 2021, Telia launched equivalent services with "Telia X". 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 with equal traffic management.

1.3.2 Specialised services

Nkom has also obtained information on specialised services. This concerns other services that are offered in parallel with internet access services and that fulfil specific criteria in the Regulation. The data shows that typical specialised services in fixed networks are voice over IP and IPTV. In mobile networks, it is relatively common to offer VoLTE. This is in line with typical examples of specialised services in BEREC's open internet guidelines.

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 access service for end-users. The general response to this is that the traffic at the links in the network is monitored continuously, and that capacity is expanded as needed.

Nkom has not undertaken detailed scrutiny of the reported traffic management measures and specialised services, but assumes that these are provided in accordance with the Regulation. In the future, Nkom may initiate more extensive scrutiny of services offered in the Norwegian market.

1.4 Net neutrality and security

Nkom observes an increasing provision of security protection for internet access services. This development is predictable, in view of the extent of malware, fraud and other security threats on the internet. In addition to the two specific service offerings: Telenor "Nettvern" and GlobalConnect "SafeSurf", Nkom will monitor this development going forward and, if necessary, initiate dialogue with providers about the regulatory framework for such products. In November 2021, Nkom published a memorandum of principle which discusses the trade-off between net neutrality and DNS blocking, with further guidance for the internet service providers.

1.4.1 Security exemption in the Regulation

Article 3(3)b of the Regulation shows that traffic management measures beyond reasonable traffic management are not permitted, unless necessary to protect the security and integrity of the network. The exemption is often referred to as the "security exemption" and the application of the exemption must be based on a "strict interpretation", see recital 11 of the Regulation. Moreover, relevant measures may only take place for as long as necessary.

The security exemption is further defined in sections 83 to 87 of BEREC's guidelines. Among other things, the guidelines describe which security threats it is relevant to protect against, and how national regulators can move forward in assessing whether safeguards are warranted. It is emphasised in the guidelines that the security exemption might be used as a basis for circumvention of the regulations and that in their assessment of relevant products and services in the national markets regulators should therefore consider carefully whether the Regulation is fulfilled.

Prior to and during the work on the Annual Report, Nkom has focused on DNS-based security measures at Norwegian internet service providers. These are measures that actualise the question of whether the security exemption in the Regulation is to be applied and whether in such case the measures are lawful under the provisions of the Regulation and BEREC's guidelines. Below, two relevant services offered by internet service providers in the Norwegian market are presented.

1.4.2 Security filter in the Norwegian market

Telenor "Nettvern"

Telenor Norge AS offers the "Nettvern" (network protection) security service, which, according to the company, blocks websites that are infected or fake. This is by means of a filter that prevents the end-user from accessing websites containing viruses, or that are used for scam attempts or malware. Instead of being forwarded to this site, the end-user receives a warning that they are about to open a non-secure website.

"Nettvern" furthermore consists of a security filter that is enabled automatically in all fixed and mobile internet access services, but the end-user can turn it off as required. Filtering takes place by blocking in DNS.

Telenor has a more detailed description of the service on its websites.

GlobalConnect "SafeSurf"

GlobalConnect AS offers the "SafeSurf" security service, which, according to the company, protects users and systems from contact with malicious websites that contain viruses or are used for scam attempts, called phishing. When the service is enabled, it automatically blocks access to malicious sites and domains, and sends the user on to a secure site.

According to GlobalConnect, "SafeSurf" is enabled automatically for customers who currently have internet via fibre (with a fixed IP address) or xDSL (either with a fixed IP address or the additional Wi-Fi Connect service). The service can also be offered for other subscription types, or where DNS is configured by end-users themselves.

GlobalConnect has a more detailed description of the service on its websites.

1.4.3 Guidance for internet service providers

Based on the knowledge held by Nkom as of the reporting date, there is not assessed to be any basis for mandatory orders or other interventions in the market. Nkom nonetheless wants to provide a general guide for how DNS-based security measures should be offered to Norwegian end-users.

For ordinary internet users, a pre-enabled DNS filter is a reasonably effective security measure. This is because most internet communication performs DNS resolution before the communication takes place. But there is also a risk of over-blocking/"false positives" because domains with lawful content can be blocked in their entirety due to infected or other malicious individual sites.

Nkom believes that here a distinction must be made between pre-activated DNS filter, optional DNS filter and security software installed on the end-user's PC. The two last-mentioned solutions could be adopted immediately without being in conflict with the security exemption in the

Regulation. However, pre-enabled filters require particularly good transparency and information to the end-user about what the service does. Providers must also have a good and verifiable overview of blocking lists and which blockings present a real threat according to the requirements in the Regulation.

Here, Nkom wants to clarify that it may request information about which specific assessments the provider has made for its specific blockings, cf. Article 5(2) of the Regulation.

Nkom published a memorandum of principle on DNS-based security measures in November 2021, which elaborates on the elements mentioned above. The memorandum is available on our website.

1.5 Transparency about the internet access service

Nkom's assessment is that Norwegian providers generally provide good information about the internet access service, in terms of both traffic management and the speed of fixed and mobile internet access. Nkom has not undertaken a detailed review of all providers' websites and contract terms, but assumes that information is published in accordance with the requirements of the Regulation and that providers make independent assessments when they change existing services or launch new services. In the future, Nkom might make more specific assessments in individual cases, for example relating to fixed wireless access and whether the provider is obliged to inform about normally available speed.

1.5.1 Information requirements

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

1.5.2 Information concerning traffic management

Providers of internet access services are obliged to notify which traffic management measures are used. Current traffic management measures are described further in subchapter 1.3.

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 in conjunction with the Annual Report shows that providers have a varying, but generally satisfactory representation of traffic management measures. Some providers have dedicated pages on net neutrality, where traffic management is one of several topics. Other providers inform more directly about traffic management in terms and on their websites. Dedicated thematic pages provide end-users with more comprehensive information about net neutrality, but in Nkom's view both solutions referred to in this section are consistent with the regulations.

1.5.4 Information concerning speed

Fixed internet access services

It follows from Article 4(1)(d) of the Regulation that the end-user must be informed of the speed which the provider is realistically able of delivering. Fixed internet access providers must specify the following measurement 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 measurement parameter that provides the end-user with the most relevant information about the performance of the internet access.

With regard to the Regulation's openness and transparency requirements, BEREC considers certain types of fixed wireless access to be fixed internet access. This includes cases where wireless technology (including mobile) is used for internet access at a fixed location with dedicated equipment, using 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. As far as Nkom is aware, as at the end of April 2022 capacity reservation or dedicated frequency bands for fixed wireless access are not used by Norwegian internet service providers.

Nkom also observes that it is becoming increasingly relevant to roll out new services via fixed wireless access. In individual cases, Nkom may therefore assess that a service is deemed to be fixed internet access on the basis of concrete implementation and the conditions for the specific service provision.

For fixed internet access, Nkom observes that providers generally disclose the various speed parameters required under the Regulation, including normally available speed.

Mobile internet access services

In mobile networks, the normally available speed 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 measurement parameters concerning speed:

- Estimated maximum speed
- Advertised speed

Mobile internet access services include both ordinary mobile subscriptions and dedicated internet 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 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 subscriptions in the mobile network, a distinction is often made between "fixed wireless 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 different subscriptions.

Conclusion

Nkom's review shows that, to varying degrees, providers present the information about the internet access service in an easy-to-understand and accessible manner. 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. For speed-differentiated subscriptions, improved transparency is observed when it comes to differentiation/lacking differentiation of end-users in congestion situations in the provider's mobile network.

1.6 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 increased by 19% and 22%, respectively, since the previous reporting period.

The speed of internet access via the mobile network also shows positive development. Mobile providers appear to be able to meet the demand by expanding coverage and implementing radio technologies that effectively leverage the available range.

For 4G, the average download speed has increased by 34% since the previous reporting period, while the average upload speed has increased marginally. For 5G in Norway in 2021, the average download speed was 365 Mbit/s (4G: 65 Mbit/s), the average upload speed was 39 Mbit/s (4G: 14 Mbit/s) and the average latency was 28 ms (4G: 44 ms). Currently, 5G traffic accounts for a small proportion of the total and it will be interesting to see whether the networks hold their ground when the coverage is expanded and a larger proportion of customers get terminals that are 5G-ready.

1.6.1 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. Article 5(1) stipulates that national regulatory authorities have a duty to ensure providers' compliance with Articles 3 and 4.

Recital 17 highlights the importance of the fact that specialised services and the use of such services should not degrade the general quality of the customer's internet access service. 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.

As from autumn 2021, BEREC has been working to update its methodology for how national regulatory authorities can perform, evaluate and publish results from quality measurements in fixed and mobile networks. The updated method description was subject to public consultation at the start of 2022. An important change in the updated description is that it now provides guidance to national regulatory authorities on how to assess the development in the general quality of internet access services. Chapter 1.6.4 shows how the methodology can be adopted to analyse the general quality of internet access services.

1.6.2 Regulatory supervision

A measure to follow up on Article 5(1) of the Regulation is to monitor the development in the quality of their internet access services measured by end-users. In this report, Nkom has assessed the results of Nkom's Nettfart measurement service, which can be used via web browser and/or mobile application. Nettfart is based on crowd-sourcing whereby the users themselves actively perform measurements and thereby produce the data basis that Nkom analyses. Nettfart.no has around 100,000 measurements per month, and the Nettfart mobile app has around 20,000 measurements per month.

As for all forms of crowd-sourcing, 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.

1.6.3 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.

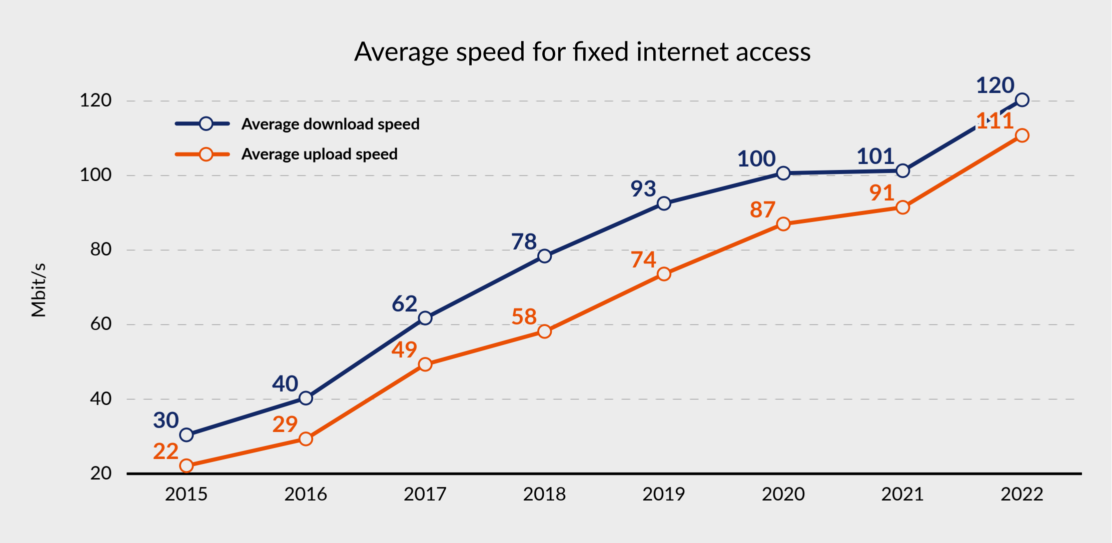

Figure 2: Average speed for fixed internet access (source: nettfart.no)

Figure 2 shows that, so far in 2022, the average download speed measured across the end-users' various subscriptions is around three times as high as in 2016[7]. The growth appears to be continuing, and stands at around 10-20 Mbit/s per year.

[7] 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 of Telenor and Telia in 2021.

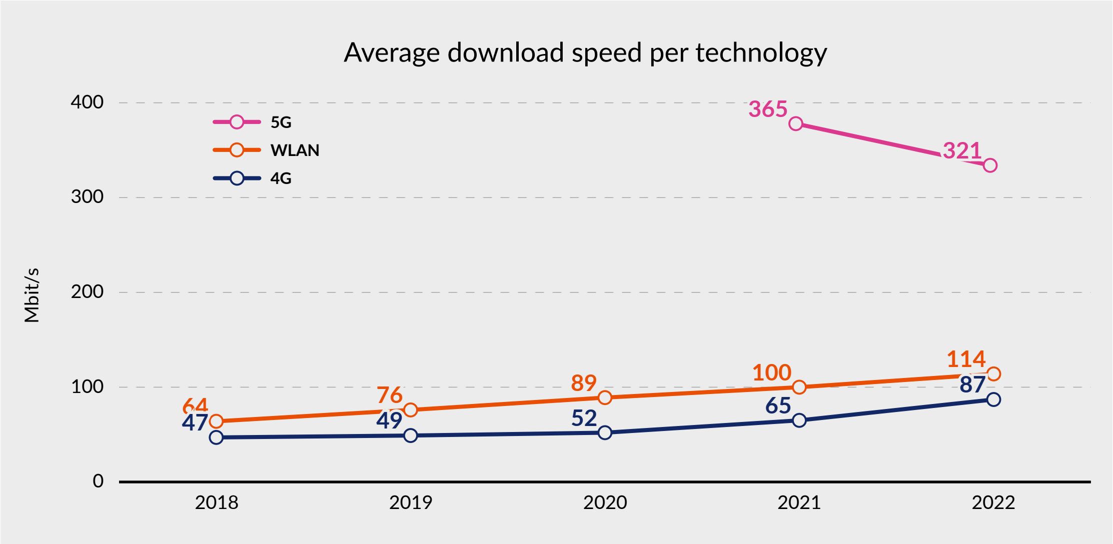

Figure 3: Average download speed per technology (source: nettfart mobile app)

Figure 3 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 downward trend, but it is difficult to say anything for certain 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.

The average speed of 4G and WLAN is increasing slightly. It would appear that most recently 4G has recovered some of the difference in relation to WLAN. This may be related to the ongoing modernisation of the mobile networks at the same time as 5G is activated. 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 access.

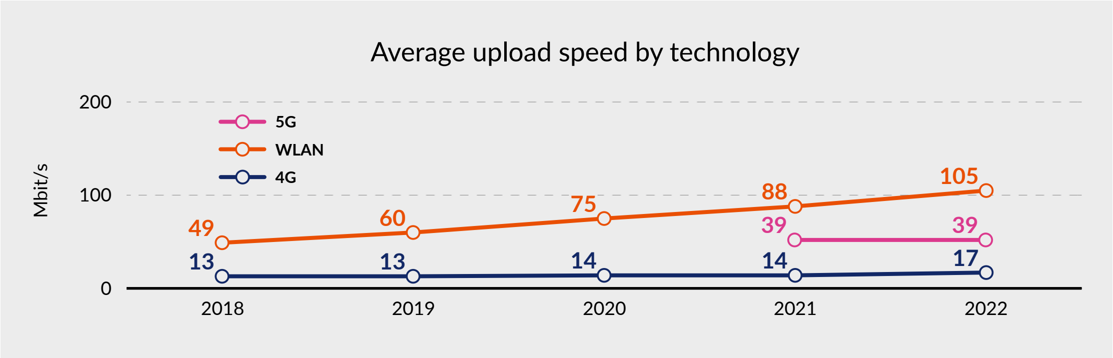

Figure 4: Average upload speed by technology (source: nettfart mobile app)

Figure 4 shows that there are greater differences between average measured upload and download speeds in the mobile networks 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 3). 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.

Key figures for 5G measurements in Norway for 2021 (Telenor and Telia)

Average download speed for 5G	Average upload speed for 5G	Avarage latency for 5G
365,00 Mbit/s	39,00 Mbit/s	28,27 ms
Maximum registered 5G download speed for Telenor	Maximum registered 5G upload speed for Telenor	Minimum registered 5G latency for Telenor
907,43 Mbit/s	137,44 Mbit/s	9,95 ms
Maximum registered 5G upload speed for Telia	Maximum registered 5G upload speed for Telia	Minimum registered 5G latency for Telia
921,20 Mbit/s	159,04 Mbit/s	5,21 ms

Figure 5: Key figures for 5G measurements in 2021 (source: Nettfart mobile app)

In Figure 5: Key figures for 5G measurements in 2021 (source: Nettfart mobile app) we present selected key figures for 5G measurements in the mobile networks of Telenor and Telia in 2021. The average download speed, upload speed and latency for the 5G networks in Norway in 2021 were 365 Mbit/s, 39 Mbit/s and 28 milliseconds (ms), respectively. The measurements recorded in Nettfart's databases show that Telia has somewhat higher values with regard to the three parameters mentioned. Measurements from the Nettfart mobile app nonetheless show the 5G technology's potential to offer internet access at high speeds and with low latency.

1.6.4 General quality of the internet access service

Nkom has applied BEREC's new method of evaluating the general quality of the internet access service to the measurements made in the 4G networks. The method uses a forecasting function based on average download speed, upload speed 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 discrepancies in the results.

Figure 6 shows forecast download and upload speeds, as well as latency, for measurements made in the 4G networks in Norway; in this case aggregated for all mobile providers. The upper part of the figure shows the forecast and the lower part shows the measured values.

The forecast average download speed for 2021 was 54 Mbit/s, while the measured value was 65 Mbit/s. This shows that the download speed in the 4G network has developed more positively than forecast estimates and that providers are expanding capacity as needed.

The forecast average upload speed for 2021 was 13.7 Mbit/s, while the measured value was 13.9 Mbit/s. This shows that the upload speed in the 4G network has shown development very close to the forecast function's estimate.

The forecast average latency for 2021 was 40.9 ms, and the measured value was 44.6 ms. It can be observed that measured latency has increased somewhat compared to the forecast function's estimate. For Nkom, it will be interesting to see whether this trend continues next year or whether we will see an improvement.

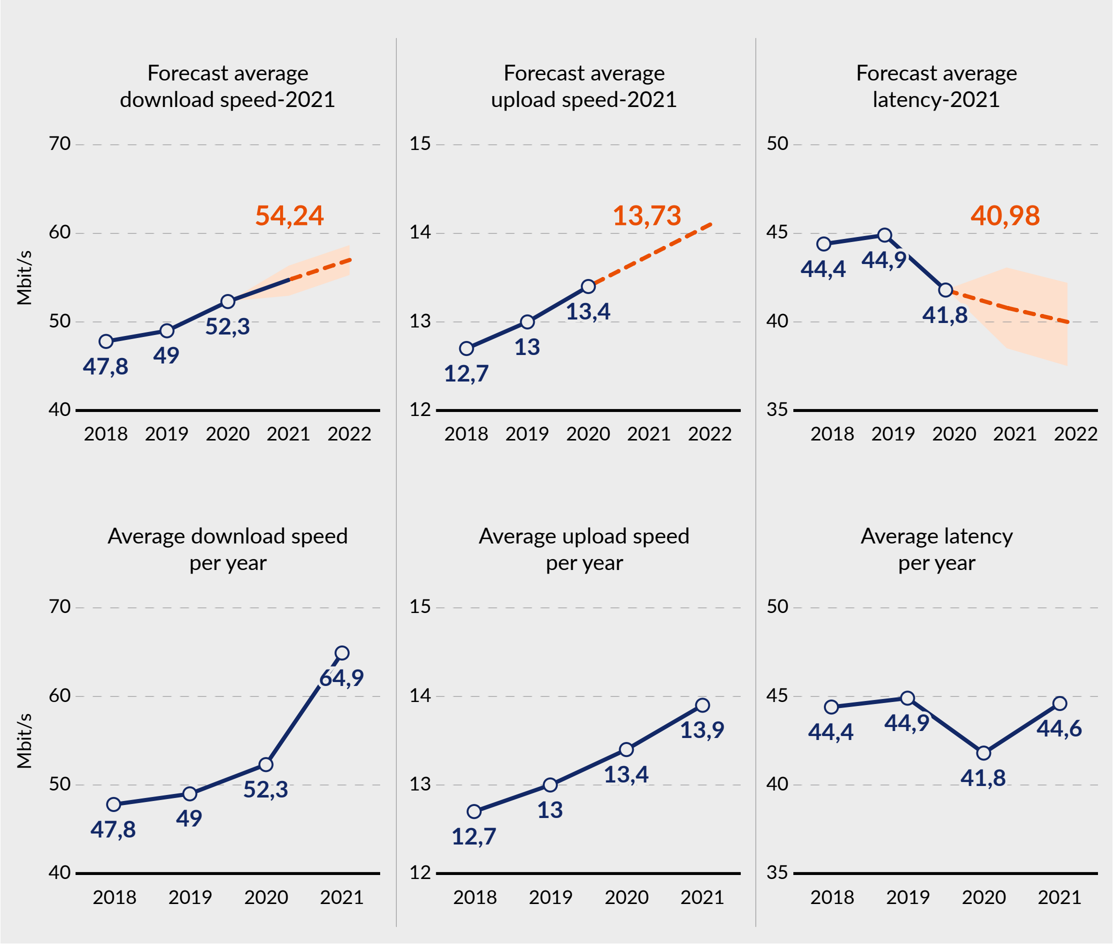

Figure 6: Forecasts of general quality of the internet access service in the 4G mobile networks in 2021. The upper part of the figure shows the forecasts, while the lower part shows the achieved result. (source: Nettfart mobile app)

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.

The report is an assignment given by KDD (Norwegian Ministry of Local Government and Regional Development) to Nkom under Report to the Norwegian Parliament 28 (2020-2021) *Vår felles digitale grunnmur – Mobil-, bredbånds- og internettjenester (Our common digital foundation — Mobile, broadband and internet services)*.
Chapter 10.8 of the Report to the Norwegian Parliament states, among other things, that
“The government requires:

- The Norwegian Communications Authority to publish an annual status report on *internet in Norway*.
- Continued work to ensure that the core functions of the Norwegian internet are secure and forward-oriented.”

Furthermore, the report describes how “Nkom reports annually on net neutrality in Norway, and this status report should be further developed to include information on the development of the core functions of the Norwegian internet, internet management, and internet-based services and platforms, as well as any regulatory reviews in this context.”

Part 2 is structured as follows: Chapter 2 describes infrastructure and traffic development for the internet in Norway. Chapter 3 discusses the adoption of IPv6 for the internet in Norway. Chapter 4 describes the status of the domain name system and encrypted domain name resolution.

Chapter 5 describes the applications of the Internet of Things, including security for the Internet of Things. Chapter 6 discusses internet security for its core functions, as well as general security trends. Chapter 7 reviews legislation relating to internet-based services and platforms.

Chapter 8 describes the development in international internet governance and Norwegian participation in this work.

2.2 Infrastructure and traffic development

An important core function of the internet is interconnection. In Norway, internet service providers exchange traffic between their networks at interconnection points that are mainly located in Oslo. Most of the traffic is exchanged at private interconnection points. In addition, the Norwegian Internet Exchange (NIX) public interconnection infrastructure interconnects more than 70 large and small internet service providers.

Internet interconnection in Norway is subject to development. As the deployment of closed solutions driven by large data centre and platform providers expands, Nkom considers it important to further develop open, neutral and regional interconnection solutions. This has both competitive and security advantages.

2.2.1 Availability of the internet access service

The national availability of the internet access service is generally consistent with the availability of broadband. Nkom's coverage survey for the first half of 2021 shows that close to 90% of all households had broadband offers with a download speed of at least 100 Mbit/s[8]. This is mainly based on fibre or hybrid networks, although fixed wireless access also contributes.

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

The 2021 electronic communication statistics[9] show that Telenor, Altibox, Telia and GlobalConnect together held an estimated 85% of the market, when the private and business markets are combined. In the mobile subscription market, the concentration is even higher. Overall, Telenor, Telia and Ice/Altibox have around 91% of customers. These three companies are also the three largest providers in the fixed broadband market, accounting for a predominant share of the services that give Norwegian users access to the internet.

2.2.2 Internet interconnection in Norway

Interconnection is the process whereby different networks (autonomous systems) 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 of service and security. These trade-offs also have an economic aspect.

Interconnection

There are two main interconnection methods: Peering and transit. In peering, two networks mutually exchange traffic with each other. This method is typically used between internet service providers that exchange large volumes of traffic between their networks. In the case of transit, an internet service provider pays one or more third-party providers to transfer traffic to and from the rest of the internet.

A distinction should also be made between national and international interconnection, and between traffic exchange occurring at private or public Internet eXchange Points (IXP).

Most 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[10]. NIX is a common term for public interconnection points in Oslo, Stavanger, Bergen, Trondheim and Tromsø.

Interconnection via the public interconnection points is particularly important for smaller internet service providers and is an opportunity to meet the larger providers and exchange traffic with them. The larger internet service providers also use NIX, to supplement the private interconnection agreements. As of Q1 2022, NIX had just below 70 customers (connected networks).

[8] Bredbåndsdekning 2021 – nkom.no

[9] Ekommarkedet helår 2021 – nkom.no

[10] nix.no

2.2.3 Internet interconnection with abroad

Most of the internet traffic between Norway and abroad is exchanged between interconnection points in Oslo and the major international interconnection points in Stockholm, Frankfurt, Amsterdam and London. However, most of this traffic passes through a limited number of connections from Oslo and via Sweden.

Since 2016, Nkom has pointed to the need to strengthen the geographical diversity of the routing of internet traffic to and from Norway, against the background of national security and emergency preparedness. This is becoming increasingly important as internet-based cloud services, which are often produced outside Norway's borders, constitute a more and more significant input factor for key functions in society.

In the period from 2020 to 2022, several new submarine fibre connections to abroad were established. These connections facilitate a growing data centre industry and an increased need for capacity and diversity. During the period, the Norwegian State contributed close to NOK 100 million to strengthen the security of the connections and to facilitate the increased diversity of internet traffic to and from Norway.

New submarine fibre connections to abroad established since 2020:

- Bulk, 2020: "Mermaid" from New Jersey (USA) to Blaabjerg (Denmark) and Kristiansand
- Altibox, 2020: "Skagenfiber West" from Larvik to Hirtshals (Denmark)
- Altibox, 2021: "NO-UK" from Stavanger to Newcastle (UK)
- Bulk, 2022: "Havsil", from Kristiansand to Hanstholm (Denmark)

These are in addition to the existing submarine fibre connections to Tampnet between Vestlandet and the UK, and Statnett's "Skagerrak 4" between Kristiansand and Tjele in Denmark.

Going forward, Nkom will assess how these changes contribute to strengthening the geographical diversity and security of internet interconnection to abroad.[11] The traffic diversity will in this case also be linked to the development of internet-based services and platforms, and the role of the Norwegian data centre industry[12].

2.2.4 Development in Norwegian internet traffic

In February 2022, Nkom issued a questionnaire to collect data on the development of internet traffic in both fixed and mobile networks. The scope included the largest internet service providers in both of these categories. At aggregated level and for the period from 2017 to Q1 2022, we see annual growth of around 25-30% for internet traffic in both fixed and mobile networks.

[11] | Cf. target 4 of the report "Robuste transmisjonsnett for Norge mot 2030" (Robust transmission networks for Norway towards 2030), Nkom – 2022.

[12] | Norske datasenter – berekraftige, digitale kraftsenter (Norwegian Data Centre – sustainable digital power centre) – regjeringen.no

Internet traffic in the mobile networks

During the past two years, traffic growth 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 the number of customers and increased data allowances. Mobile subscription data allowances[13] have increased in recent years without prices rising proportionately.

Figure 7 shows the development in internet traffic distributed on ordinary mobile subscriptions, dedicated internet subscriptions[14] and international roaming. The ordinary mobile subscriptions generate most of the internet traffic in the mobile networks (over 80%). In 2021, internet traffic in mobile networks totalled 624 Petabytes (PB)[15], an increase of 32% from 2020.

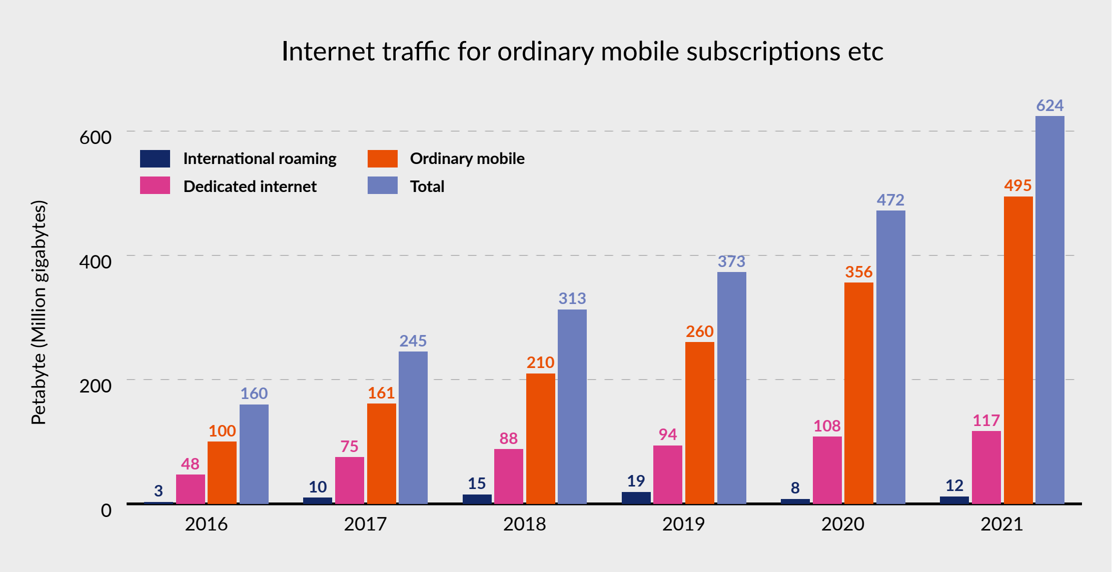

Figure 7 – Internet traffic for ordinary mobile subscriptions, dedicated internet subscriptions and international roaming.

Mobile providers are now rolling out 5G on a large scale. In Q1 2022, around 25% of connected handsets were ready for this generation of technology, and 5G connections account for around 5% of total internet traffic. 5G traffic is increasing in line with mobile providers' 5G rollout and phasing-in of new handsets ready for 5G technology.

Internet traffic in fixed networks

Also for fixed networks, there has been annual growth in internet traffic of around 25-30% since 2017. In Q1 2022, network traffic production for the largest fixed network providers exceeded 2 Tbit/s in peak hour.

Providers experienced a significant increase and a change in traffic pattern in conjunction with the coronavirus lockdown in 2020 and the subsequent increase in home office use and virtual meetings.

[13] The largest group of Norwegian end-users still have subscriptions with a data allowance of between 1 GB and 5 GB included. The biggest increase in 2021 was for subscriptions with data allowances of between 10 GB and 20 GB.

[14] 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.

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

Applications that produce the most internet traffic

The distribution of internet traffic between different applications is relatively similar in the mobile networks and fixed networks. Web browsing (HTTP-based communication) remains the biggest traffic driver. Streaming services such as internet TV, YouTube, Netflix and TikTok are major contributors. This is followed by social media services such as Facebook, Instagram and Snapchat.

Traffic development on NIX

As mentioned in Chapter 2.2, the interconnection between the different Norwegian networks and the interconnection between Norwegian and foreign networks mainly takes place in Oslo. Some of the Norwegian interconnection occurs at the NIX public interconnection points. Figure 8 shows the location of the interconnection points, and the size of the circles illustrates the relative difference in traffic volume in 2021.

Annual average for inbound/outbound internet traffic across the entire NIX infrastructure is 102 Gbit/s in 2021[16], with NIX1 and NIX2 in Oslo accounting for 96 Gbit/s (94% of the total traffic on NIX).

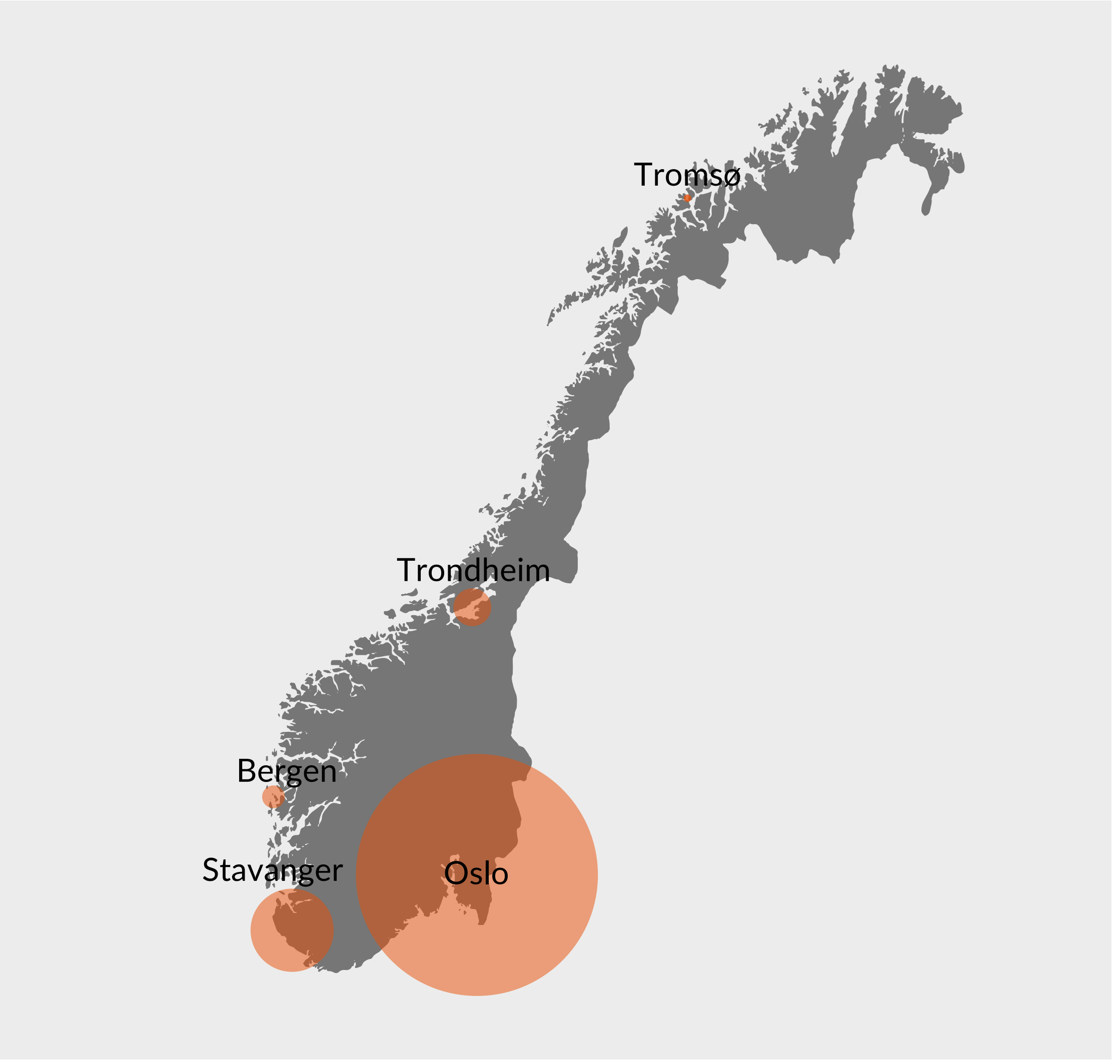

Figure 8 – Location and traffic volume for the NIX interconnection points

[16] | Statistics – nix.no, the data was obtained in April 2022.

Given that most of the private interconnection also takes place in Oslo, it is clear that in Norway there is very small degree of regional interconnection. One exception seems to be Stavanger (SIX) which had the greatest increase in 2021, with an annual average of 5 Gbit/s. SIX is located in the Green Mountain data centre, and the growth is due to new content providers and providers of CDN (Content Delivery Network), as well as an increase in the number of connected networks.

2.3 Adoption of IPv6

In 2022, Norway has an Pv6 adoption of 22.2%, thereby ranking 35th in the world. In October 2020, Norway was in 29th place with an adoption of 18.1%. Norway has thus dropped 6 places on the list in the course of one and half years. Meanwhile, the percentage IPv6 adoption has improved and increased by around 4 percentage points. At European level, Norway is in 14th place.

This means that providers in a number of other countries are increasing their IPv6 adoption faster than the Norwegian market. Nkom is monitoring the further development and emphasises the importance of providers in the Norwegian market facilitating the use of IPv6 to the fullest possible extent.

2.3.1 About the transition from IPv4 to IPv6

The government's objective is "*That the Norwegian Communications Authority in cooperation with relevant stakeholders must emphasize the work on the adoption of IPv6, so that Norway is at least at the level of comparable countries*". On this basis, Nkom will seek to survey the current status of the adoption of IPv6 in Norway, and monitor development over time.

IP (Internet Protocol) is the basic protocol used to transmit traffic on the Internet, and to identify devices connected to the internet (computers, phones, servers, etc.). Public IP addresses are unique global identifiers. The IP protocol exists in two versions, IPv4 and IPv6.

IPv4 has been used on the internet since 1983. The success of the internet, combined with the diversity of areas of use and the growing number of connected devices, has resulted in a gradual decline in the number of available IPv4 addresses, with some parts of the world being more severely affected than others by the greatly reduced availability.

The basic IPv6 specification was completed in 1998, and in the following years extensive standardisation work for the protocol has been conducted. IPv6 offers a very high number of IP addresses, which are considered to be sufficient for a long time to come. In addition, the protocol provides functions for increased basic security and optimised routing.

The complexity of today's internet entails that the transition from IPv4 to IPv6 must take place gradually. A prolonged period of coexistence between the two versions is required. IPv6 will not be able to fully replace IPv4 until all internet connected devices have migrated to the new version. Even though the transition began in 2003, the process is still in a co-existence phase.

On 25 November 2019, RIPE NCC announced17 that they had run out of IPv4 addresses. This could lead to acceleration in the transition from IPv4 to IPv6.

17 | RIPE NCC – the regional internet registry tasked with assigning IP addresses in Europe and the Middle East.

2.3.2 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)[18]. The data collection was carried out in April 2022. This first Annual Report on the internet in Norway is intended to be a reference point for observing the development of IPv6 adoption. Norway ranks 35th worldwide with an adoption of 22.2%. At European level, Norway is in 14th place.

Based on information from France's Internet Report[19] for 2021, where the data is from October 2020, Norway was in 29th place with an Ipv6 adoption of 18.1%. Norway has dropped back 6 places on the list of top countries in terms of Ipv6 adoption over one and a half years (from October 2020 to April 2022). But the percentage IPv6 adoption has nevertheless improved during the period, increasing by around 4 percentage points (from 18.1% to 22.2%). At European level, Norway was in 12th place at the same time (October 2020), which means that Norway dropped two places on the list in the course of one and a half years.

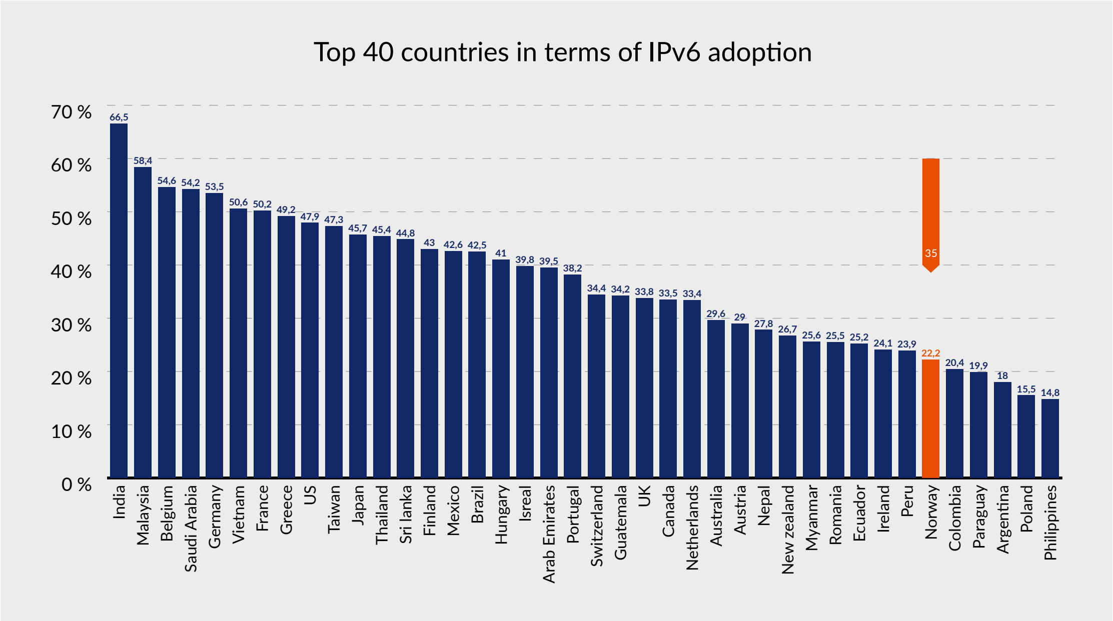

Figure 9 – Top 40 countries in terms of IPv6 adoption

Even though Norway has dropped down the list, IPv6 adoption has increased gradually among the Norwegian internet service providers. The fact that IPv6 adoption is increasing nationally while Norway's position on the list is moving downwards means that internet service providers in many countries are accelerating IPv6 adoption faster than internet service providers in the Norwegian market.

[18] Based on the median for "Google IPv6 adoption", "Akamai IPv6 adoption", "Facebook IPv6 adoption" and "Apnic IPv6 adoption" data from April 2022. 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 2022).

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

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

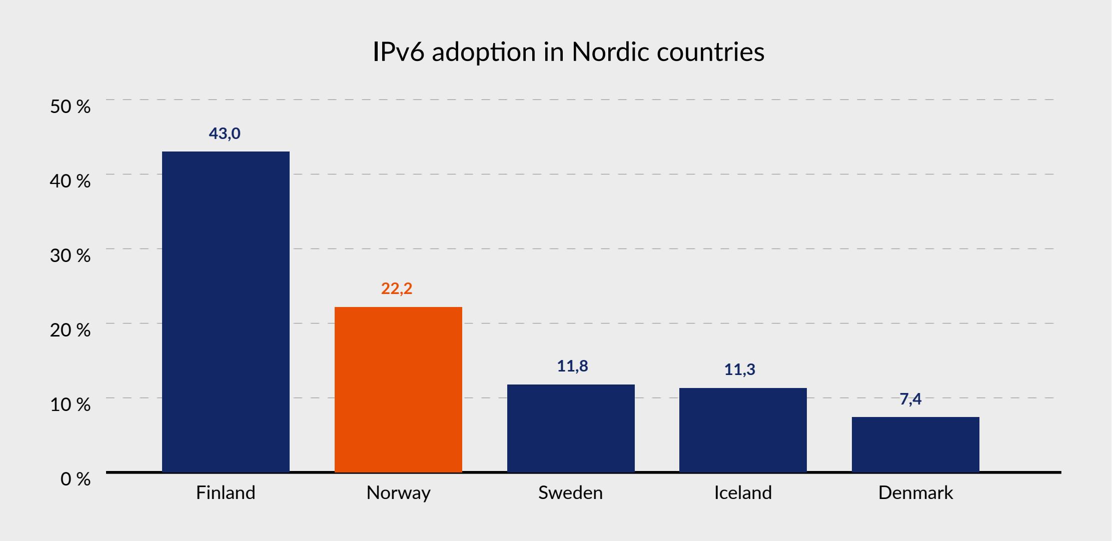

Figure 10 – IPv6 adoption in Nordic countries

Figure 11 shows the adoption as percentage median value obtained from the four main sources of publicly available information on IPv6 adoption (Google, Akamai, Facebook, Apnic). Facebook records the highest percentage IPv6 adoption among Norwegian end-users.

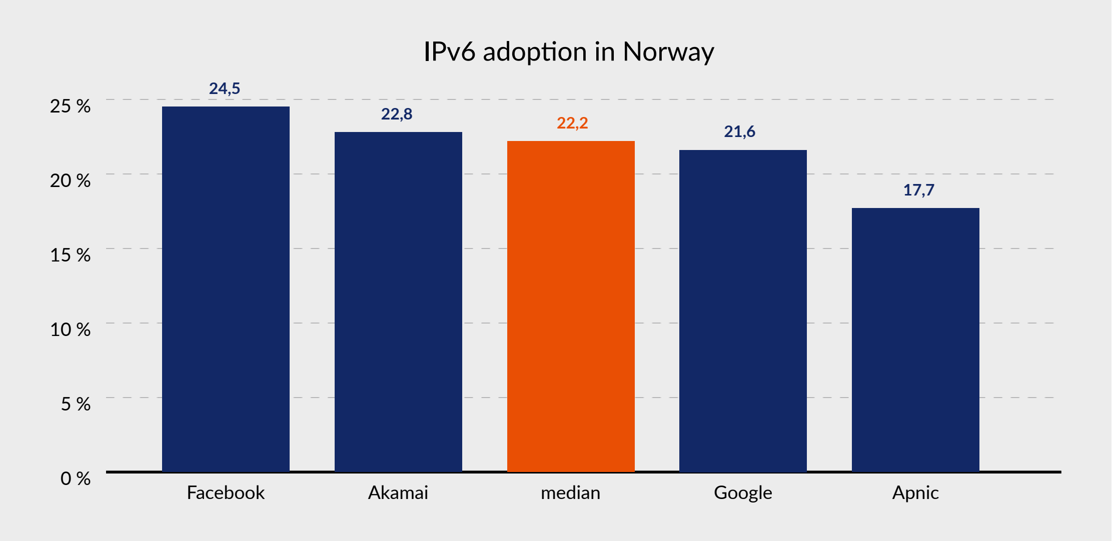

Figure 11 – IPv6 adoption in Norway

2.3.3 Status of Norwegian internet service providers

Nkom’s information collection shows that exclusively “dual stack” is offered to Norwegian customers. This means that IPv4 and IPv6 are run in parallel in both fixed and mobile networks’ infrastructure. The users of the vast majority of fixed and mobile network providers must themselves take the initiative (“opt-in”) to adopt IPv6, by enabling IPv6 on their routers and/or through the reconfiguration of their terminal.

In terms of internet *interconnection*, it appears that IPv6 has far greater adoption. All of the fixed and mobile network providers asked use IPv6, if this is also supported by their interconnection partners. Regarding the routing of traffic, stability, security level and performance for gaming in particular, no perceived difference between IPv4 and IPv6 is reported.

IPv6 in mobile networks

Two out of three mobile providers offer IPv6 in their networks, while the third will have this in place in the near future. A large proportion of voice traffic (VoLTE) goes via IPv6, depending on whether the handsets support this or not. Internet traffic in mobile networks (including fixed wireless access) currently uses IPv6 to a small extent.

Mobile providers seek to ensure that the most commonly used terminals are pre-configured to support IPv6, and that in the case of “dual stack” IPv6 is preferred.

IPv6 in fixed networks

Some fixed network providers have support for IPv6 enabled for all new installations, while other providers ask customers if they require this. Some of the providers can fully enable/disable IPv6 from their side, while in other cases the customer is also required to configure the customer equipment themselves. This is most often determined by whether the customer uses equipment delivered by the provider or acquires equipment themselves.

Fixed network providers have a limited overview of IPv6 usage. Among private customers, generally those who are “particularly interested” will choose IPv6. In the public and business markets, there is somewhat greater use of IPv6. Fixed network providers must also provide some customers with new equipment if IPv6 is to be used. The feedback indicates that IPv6 is promoted to a small extent, even though the infrastructure as such is often prepared for IPv6.

2.4 Domain name system

New domain name resolution methods, called “encrypted DNS”, have recently been adopted. One of these methods is DoH (DNS-over-HTTPS). Today’s providers of DoH resolvers are mainly located outside Norwegian jurisdiction. There are several regulatory consequences of increasing use of open resolvers, including that public enforcement based on filtering of DNS resolution is enforced to a lesser extent.

The EU has launched the DNS4EU initiative to establish a European alternative to the major open American DNS resolvers. Nkom will continue to monitor the development of DNS4EU as the solution becomes available and will assess the possibility of Norwegian involvement and facilitation of the use of the service for Norwegian residents. In the longer term, this approach will contribute to strengthening the position of DNS resolvers within European jurisdiction.

2.4.1 Status of DNS in Norway

The domain name system (DNS) links IP addresses to unique domain names, such as altinn.no. This is a basic function that is necessary for the internet infrastructure to function. When a user seeks to contact an internet service, this triggers a series of requests to DNS to find the relevant IP address. The system's hierarchical structure requires the interaction of several independent providers for the user's machine to get the response it needs.[20]

Norid AS is the registry for the Norwegian country code top-level domains of .no, .sj and .bv, and under the agreement with the Internet Corporation for Assigned Names and Numbers (ICANN) has the right to assign, manage and register domain names under these top-level domains. Only the .no domain is open for registration. As a registry, Norid manages the domain name service and registration service for the top-level domains.

A domain name arises when an organisation or private individual is assigned a subscription to the domain name. Norid's registration service processes applications for domain names in line with current allocation rules and maintains the register of user rights to the various domain names. To apply for a domain name, an applicant must contact a registrar, who submits the application and then manages the subscription on the subscriber's behalf. There are around 260 registrars that intermediate domain names ending in .no.

The domain name service for .no is part of the technical infrastructure of the domain name system. The service responds to which domain names are found under the top-level domain and which name servers each domain name is associated with. It has particularly high availability requirements, and has not been unavailable since the top-level domain came into use more than 30 years ago.

In 2014, Norid introduced DNSSEC for Norwegian domain names. DNSSEC is a security mechanism that cryptographically signs responses to domain resolution. This makes it possible to verify that responses to requests to DNS come from a correct source, and have not been changed during the process. As at May 2022, 60.8% of all domain names under .no are signed with DNSSEC, and the Norwegian top-level domain is a world leader in terms of proportion of secured domain names.

Even though .no has a very high proportion of secured domain names in total, there are major differences in the degree of security among the various registrars. Five of the ten largest registrars have signed more than 80% of the domain names they manage. The others have signed less than 5% of their portfolios, or do not offer such securing of customers' domain names.

A condition for DNSSEC to safeguard the individual user is that the computer that retrieves the response to the domain resolution checks (validates) the response, so that responses with false or inconclusive signatures are discarded. This is performed by special computers — resolvers — which are often operated by internet service providers, hosting providers and managers of corporate networks.

As at May 2022, around 86.2% of domain name requests are validated in Norway, which is also high in worldwide terms. This is because, among other things, major providers such as Telenor, Telia and Altibox, which together cover a large customer base, have turned on validation. However, there are still some major internet service providers that do not validate the domain name resolution.

[20] Subchapter 2.4.1 is a text contribution from Norid

2.4.2 Encrypted domain name resolution

What is “encrypted DNS”?

The domain name system consists of two main parts:

- authoritative servers, which are containing the global directory of domain names; and
- resolvers, that perform domain name resolution in this directory.

When we communicate via the internet and enter a domain address, our computer first sends a domain name request to a DNS resolver typically offered by our internet service provider. The resolver then asks the authoritative DNS servers on the internet to find the relevant IP address and return it to our computer.

Today, it has also become common for providers other than internet service providers to offer resolvers, while various content and application providers also offer “open” resolvers. This means that we can configure our web browser to use these resolvers instead.

Relatively recently, new domain name resolution methods have been adopted, called “encrypted DNS”. One of these methods is DoH (DNS-over-HTTPS), which performs domain name resolution as an integral part of web traffic. Today’s providers of DoH servers are mainly located outside Norwegian jurisdiction.

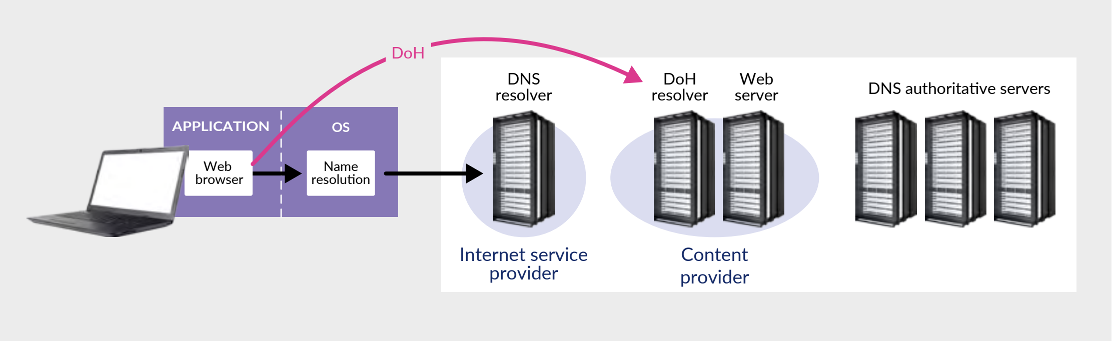

Figure 12 – Domain name resolution with traditional DNS and DoH, respectively

The use of DoH has different consequences for various categories of stakeholders. For ordinary internet users, encryption offers advantages in terms of confidentiality for the domain name resolution made. However, the organisation that runs the resolver service will have access to the requests that are made, then the question is whether one puts most trust in a national internet service provider or an international content provider.

The significance of these factors also depends on where one lives or stays, as well as who one is. For example, in the case of dissidents in an authoritarian country, the assessments will typically be different than for residents of Norway. The introduction of encrypted DNS also has various implications for other providers, which are further elaborated in the following subchapters.

The detailed functioning of encrypted DNS is still subject to development. The basic protocol itself has been standardised. Work is continuing on improving functionality in order to configure which DoH server is used by the web browser. Once this is in place, the opportunities to set up encrypted DNS in the preferred way will be improved significantly.

Status of DNS-over-HTTPS (DoH)

DoH is increasingly supported by the most popular web browsers and operating system. For example, DoH is supported by the Firefox, Chrome and Edge web browsers, and can also be found in operating systems such as Windows, MacOSX and Linux, as well as Android and iOS.

Standardisation of mechanisms related to the policy for selection of resolvers is developed by IETF in the "Adaptive DNS Discovery" working group. So far, selection of resolver is implementation-specific and varies between both web browser and operating system.

For several of the implementations, however, DoH is not turned on as the default mode. There is every reason to believe that this is development will change, and will be implemented as a quick update. For example, in 2021, DoH was turned on as default for all Firefox users in the US.[21]

Open resolvers have long been available to internet users. In recent years, several providers of these have also implemented the possibility of using DoH. For Norwegian consumers, it is optional which resolver service they use, even though this removes control of the user experience from the internet service providers. To date, Norwegian internet service providers do not offer DoH as a mechanism available to their customers.

DoH aims to protect communication between internet user and provider of the resolver service. Norwegian consumers are to a great extent protected by legislation from access to information about their use of DNS, and there is a great deal of trust between customers and internet service providers. This reduces the incentive to change current resolver services. Use of DoH also presents a number of technical challenges that are related to response time, scaling and access to and experience with implementations of DoH servers.

2.4.3 Regulatory consequences of DoH

The government's goal is to "*Work for Norwegian internet service providers to maintain DNS resolvers within Norwegian jurisdiction in case of introduction of new domain name resolution methods*".

There are several regulatory consequences of using open DNS resolvers in general and open DoH resolver services in particular, since public oversight based on limitations in DNS is no longer possible to implement based on a regulation.

Statutory facilitation obligations under the Norwegian Electronic Communications Act, for example related to interception, are impeded by the use of DoH where all traffic is encrypted. Furthermore, it is not possible to distinguish domain name resolution from other internet traffic. This makes it difficult to determine whether DoH is used, and to detect content in requests and responses.

DNS is also used for nationally imposed filtering, for example based on the Pirate Bay ruling. In cases where open resolvers with DoH are used, the opportunity to filter out illegal content disappears. Several of the popular open resolvers are run by large multinational companies over which it is difficult to exercise Norwegian authority.

Further liability under the Norwegian Electronic Communications Act's mandatory order on safe and responsible operation could also be disrupted by DoH. To a great extent the internet access service depends on the control and stability in DNS. On using international resolver services, internet service providers lose part of this control.

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

In connection with the increasing use of open resolver services from US providers such as Google and Cloudflare, the EU has implemented the DNS4EU initiative as a European alternative. On the deployment of DNS4EU, the service will provide an optional offer that supplements existing resolver services and supports up-to-date security requirements and privacy under the European standard, including support for filtering based on national court rulings.

Nkom will continue to monitor the development of DNS4EU as the solution becomes available and will assess the possibility of Norwegian involvement and facilitation of the use of the service for Norwegian residents. In the longer term, this approach could contribute to strengthening the position of DNS resolvers within European jurisdiction.

2.5 Internet of Things (IoT)

The number of IoT devices is increasing in both licensed and unlicensed frequency bands. The development of standalone 5G will start in 2023 and in the long run is likely to take over large amounts of IoT traffic. As from 1 August 2024, the European Commission's regulation on internet security for IoT equipment will apply to manufacturers of radio equipment.

There is still a lot of IoT equipment in Norway that is only connected to 2G networks. However, the 2G networks are planned to be closed down in 2025. Nkom encourages all sectors to start planning the phasing-out of devices that only work on 2G. Nkom will also survey the use and dependencies of 2G, and any challenges arising in the time up to the discontinuation of the 2G network, to ensure responsible decommissioning that takes relevant user considerations into account.

2.5.1 Use of the Internet of Things

The Internet of Things (IoT) consists of physical objects that communicate directly or indirectly via the internet. Communication between IoT devices without human interaction is referred to as machine-to-machine (M2M) communication. Depending on the data volume, communication pattern, coverage requirements, power consumption, mobility and number of devices, various technologies will be used.

IoT devices can be connected via wired or wireless access. For wireless access, an overall distinction is made between technologies that use frequencies regulated by the Free-Use Regulation (unlicensed frequencies) and technologies using mobile technology (licensed frequencies).

The number of IoT devices has increased sharply in recent years and the trend seems to continue. Figures from analytics company IoT Analytics estimate that there were around 12 billion IoT devices in the world in 2020[22]. This is projected to rise to 31 billion in 2025.

In Norway, IoT is used in a number of areas, such as alarm systems, payment solutions, smart home systems and measurement systems, e.g. power measurement. Within the transport sector, IoT is used for alarm systems and to monitor and track vehicles and containers, as well as electronic log-books. Within the healthcare sector, it is used for applications such as security alarms in homes and patient alerts in nursing homes. The trend is also for a number of traditional household products such as refrigerators, washing machines, tumble dryers, coffee makers and so on to become IoT products.

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

2.5.2 IoT as an electronic communications service

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).

Development in the use of unlicensed frequencies is increasing, and the number of connected devices is rising strongly. However, it is difficult to estimate this development accurately since a lot of equipment does not need to be registered. The Last Mile Solutions company reports very high growth during the previous three years and also expects strong growth in the next three years.

One of the most widely used wireless IoT protocols is LoRaWan which, with good coverage and low power consumption, is widely used. The technology can, for example, be used in water meters, motion sensors and temperature sensors. For unlicensed technologies with limited range, it may be necessary to supplement with licensed networks, such as 4G/5G.

IoT via licensed frequencies

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 two 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.

Figure 13 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 2021 has almost doubled since 2017 and that the number of devices is rising faster each year.

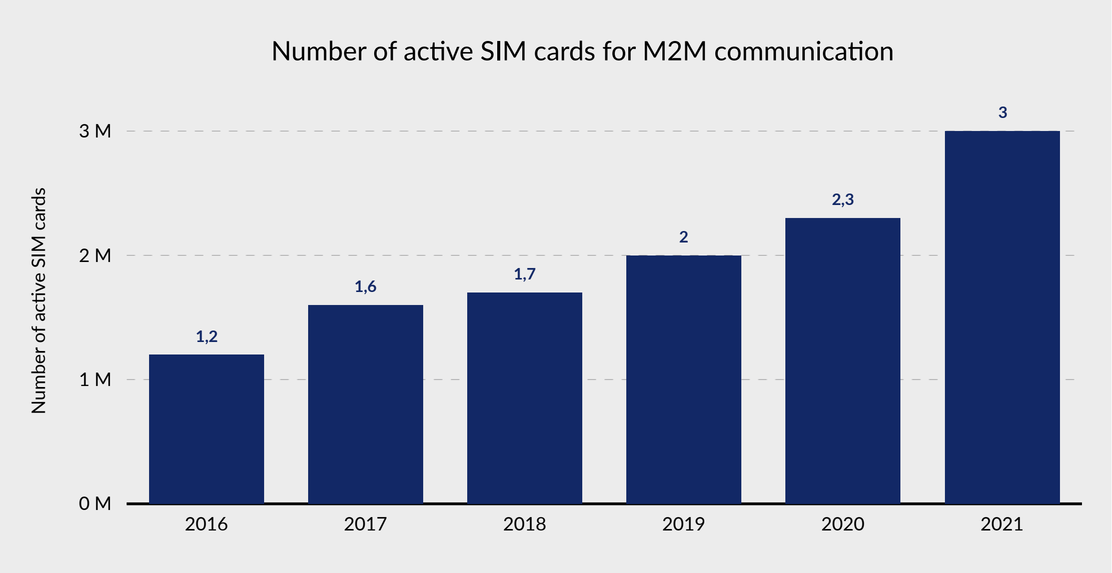

Figure 13 – Number of active SIM cards for M2M communication in the mobile network

Today, mobile providers use both 2G and 4G for M2M communication, but they plan to close the 2G networks during 2025. This will have significant consequences for sectors that still only use 2G for M2M. There are still over a million IoT devices connected to 2G networks.

Nkom has urged all sectors to start planning the phasing-out of devices operating solely on 2G as the date of providers' planned shutdown of the 2G network approaches[23]. Up to the shutdown date, Nkom will continue to survey the use of and reliance on 2G, to ensure responsible discontinuation that takes relevant user considerations into account.

2.5.3 IoT security

IoT devices can be exploited for cyber attacks and dissemination of malicious software. Devices themselves can also be targets of cyber attacks that manipulate mode of operation or steal personal data. There are currently no requirements for IoT equipment to have built-in security, and the responsibility to protect from such incidents is today mainly left to the users themselves.

The European Commission has concluded that this is such a major problem that the EU is establishing its own regulation in the area[24]. The requirements will apply to internet-connected radio equipment and require built-in data security, privacy, protection from fraud and integrity of the network. The regulation applies to equipment placed on the market after 1 August 2024.

European standardisation organisations are working to produce relevant harmonised standards in the field. For IoT equipment intended for consumers, a standard (EN303 645) has already been prepared to describe good practice for data protection and privacy. The standard is aimed at developers and manufacturers of IoT equipment.

2.6 Internet security

The press often spotlights the security of end-user devices such as computers, mobile phones, tablets and the like. For individual persons, poor security and successful cyber-attacks can have major consequences.

However, the attackers also exploit the internet's core functions such as DNS and BGP. The networks are often exposed to distributed denial-of-service attacks. The common denominator is that the end-users rely on the providers for protection against this form of security attack.

2.6.1 About internet security

The complexity of internet technology is increasing, and value chains are becoming longer and more complicated. When this is combined with increasing numbers of vulnerabilities in infrastructure and services, as well as an increase in malicious attackers, strong requirements are placed on internet service providers to contribute to secure and stable services.

Core functions of the internet are subject to exploitation. However, the protocols are continuously updated with new security features to counter the various threats. Norway has come far in adopting such security improvements.

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

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

2.6.2 Security for the internet's core functions

Domain name system

DNS is a critical core function of the internet that is exposed to security attacks. Hijacking and manipulation of DNS can result in users being routed to fake websites. These inherent vulnerabilities are associated with both operation and use of the DNS infrastructure.

Historically, greater vulnerabilities have been observed in both the DNS protocol and in implementations thereof. In several cases the DNS protocol has been used for distributed denial of service (DDoS) attacks that exploited basic functionality in DNS and how delegation and forwarding of requests functions.[25]

Operation of authoritative name servers is distributed and undertaken by the owners of the domains. This means that a large number of providers have to protect their systems, which they manage to implement to varying degrees. There are various technical solutions to protect domain name resolution, but these are not always adopted. For Norwegian domains, the status is relatively good in this area, where around 60% of the domains are signed on the basis of DNSSEC, cf. Chapter 4.1.

Even though DNSSEC is used to ensure that responses to domain name resolution are not manipulated by unauthorised persons, this does not ensure that ownership of the requested domain is correct. Attackers can exploit this by registering domains that are spelt almost the same, or are registered on alternative top-level domains. The possibility of registering this type of false domains depends on policy and safeguarding measures on the registration in the various top-level domains. For example, Norid has strict guidelines to safeguard brand and proper names under the .no zone, while this is applied to a lesser extent to generic top-level domains that are internationally available. Nkom EkomCERT reports weekly on events related to false domains.

Border Gateway Protocol

The Border Gateway Protocol (BGP) is the routing protocol used to bind the networks (autonomous system) together into a global internet. BGP allows the various internet service providers to announce the address segment used in their network, so that the various internet routers can learn the shortest path to other providers' networks and addresses.

There are technical solutions to verify ownership and ensure route announcements via BGP. One method used is Resource Public Key Infrastructure (RPKI) which confirms ownership cryptographically via esignature. Norwegian networks are increasingly protected by this type of signing, but still have some way to go. Verification is also performed to a greater extent, using the Routing Policy Specification Language (RPSL).

There is also work on the development and standardisation of corresponding protection mechanisms for entire network paths, announced via BGP. However, this work is not mature enough to be used extensively. In recent years, several major network owners have signalled that announcement must be protected with RPSL and/or RPKI and could be validated so that route announcements can be accepted.[26]

[25] | Examples of such vulnerabilities are tsuNAME and NXNSAttack.

[26] | Is BGP safe yet? No.

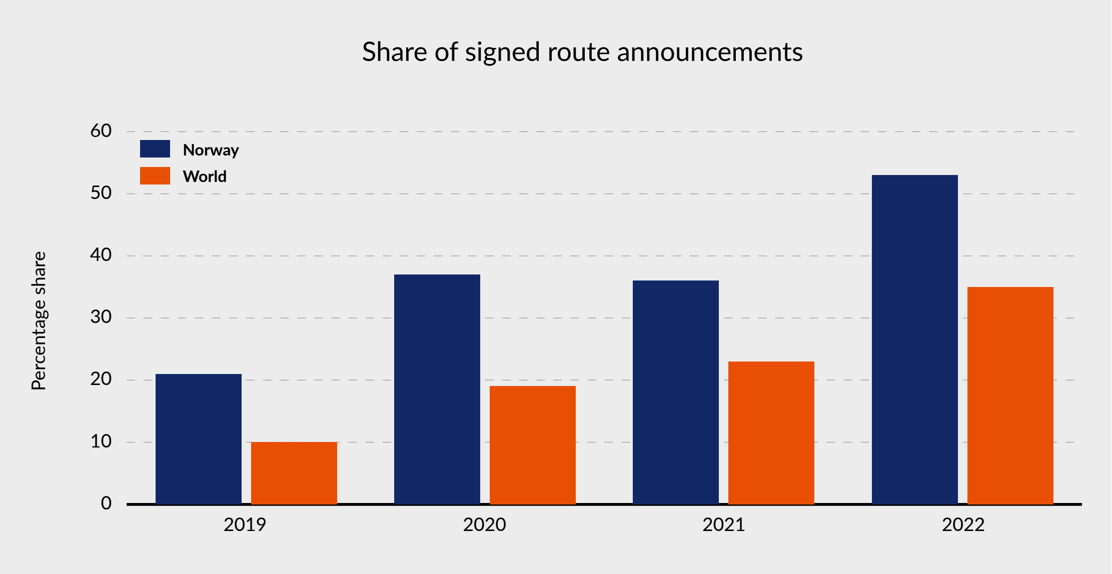

Figure 14 – Share of signed route announcements, source: https://observatory.manrs.org/#/overview

One method of attack using BGP is BGP hijacking, which entails a provider announcing an address segment they do not rightfully operate, causing internet traffic to be routed to or via the wrong network. The consequences of BGP hijacking are potentially very great, including that a attackers can perform denial of service attacks, intercept traffic or introduce counterfeit infrastructure and services.

BGP hijacking may also occur unintentionally as a consequence of misconfiguration of network equipment and BGP routing. On the outbreak of the war in Ukraine, there were several observations of BGP hijacking of Ukrainian route announcements.

2.6.3 Denial of service attacks and available bandwidth

Denial of service attacks are a persistent type of security attack handled by Norwegian internet service providers on a daily basis. There are several types of denial of service attacks. The most common concerns the internet's infrastructure whereby it is sought to overload the transmission capacity in the network by transferring large volumes of adverse traffic. The attacks often target end-customers or end-customers' services.

There are several countermeasures that can be used. For this to be effective, it is important to have an overview of which services or customers are often the targets of this type of attack. Technical information about the methods used is also important, as well as details of vulnerable services or botnets that can be used for such attacks.

The largest internet service providers currently have good countermeasures that can be used to handle denial of service attacks. For example, through the filtering of adverse traffic using equipment specially built and designed for this purpose. It is also possible for providers to work together to filter sections of traffic using signalling via BGP.

2.7 Internet-based services and platforms

Greater use of internet-based services and platforms challenges existing legislation and requires legislation to be adjusted. Within the EU, a package of regulations, including the Digital Services Act and the Digital Markets Act, is currently being established. These are relevant to the EEA and could thereby be implemented in Norwegian legislation. New regulations will set the terms for consumers' and businesses' use of the internet.

The regulation of internet-based services and platforms requires cross-sectoral cooperation between government bodies. This is to ensure effective and consistent exercise of public oversight in relation to resourceful providers who play a dominant role within the internet ecosystem. Nkom will play an active role in this collaboration in view of our expertise as a regulator of electronic communication services in general, and net neutrality and predefined markets in particular.

2.7.1 Regulatory development

In recent years, internet access has become the most widely used electronic communication service in Norwegian society. Furthermore, services that we use via the internet (often referred to as "over-the-top") have gradually taken over from traditional electronic communication services. Large computer systems that offer comprehensive internet-based services such as social media or app stores are often referred to as "internet-based platforms".

In the spring of 2022, the EU's legislative institutions have agreed on two new regulations that will help secure users' rights on using internet-based services (Digital Services Act) and establish ex ante regulation of the major internet-based platforms (Digital Markets Act), respectively. This legislation is part of a larger package of legislative proposals related to internet regulation that are EEA-relevant and are also likely to be implemented in future Norwegian legislation.

2.7.2 Digital Services Act (DSA)

The purpose of DSA is to modernise and clarify commitments for providers of internet-based services and platforms. The background is an increase in the scope of internet activities that are harmful to consumers. The current regulations are considered to be ineffective and insufficiently coordinated between member states to deal with this issue.

DSA encompasses all types of providers of internet-based services, and not just the major platforms as mentioned above. However, the degree of obligation under DSA depends on the size of the provider. Very large internet-based platforms will be subject to more requirements than smaller intermediate services, such as providers of internet access services, caching services, and hosting services.

Providers covered by DSA are subject to a number of liability rules and diligence obligations that supplement and complement the general provisions. Smaller providers may be exempt from some of the liability provisions of the regulations, stipulated as further terms. However, major providers must consider cumulative obligations related to, among other things, transparency, reporting and risk analysis.

The enforcement of the obligations under DSA will take place both nationally and internationally. Each country will appoint one or more national coordinators ("Digital Services Coordinators") who will be tasked with managing complaints against providers, and will cooperate via a European Board for Digital Services. The European Commission will oversee the largest platform providers.

Nkom supports the DSA proposal and believes that asymmetric commitments are the right approach, so that new and small/medium sized providers of internet-based services are not subject to an excessive regulatory burden. The oversight of very large platform providers requires the involvement of the European Commission, since this may also intersect with other internet-related regulations, while at the same time national coordinators will be important contributors to assessing national conditions and will contribute professional expertise concerning the internet.

The European Commission, the European Parliament and the Council reached political agreement on the DSA proposal on 22 April 2022. Formal approval by the European Parliament and the Council is expected during the second half of 2022. DSA will thereafter enter into force 15 months after formal approval, or from 1 January 2024, whichever date occurs first. However, the largest providers may be subject to oversight four months after they have been designated according to the procedure indicated by DSA.[27]

2.7.3 Digital Markets Act (DMA)

The purpose of DMA is to ensure fair treatment of business users that use the largest internet-based platforms. Another important consideration is to enable end-users and business users to use the platforms without facing undue conditions set by the provider. The expected effect is for the regulations to stimulate competition and innovation via the internet, so that consumers in the single market can benefit from a greater and better range of services on the internet, at affordable prices.

Several stakeholders will be regulated by both DSA and DMA, but the central provider term in DMA is "gatekeeper", which denotes influential, internet-based platforms with many customers and financial turnover of such a scope that the legislator has found regulation necessary. There are also several resolutions and court rulings at European level that have underpinned the regulatory requirement.

Gatekeepers can be designated in various business areas that are more closely defined in the regulations, such as internet-based intermediation services, search engines, social media and video sharing services. The designation itself is based on qualitative and quantitative criteria.

The European Commission will oversee DMA, which is important in view of the fact that the gatekeepers are very large and dominant players in the market. A Digital Markets Advisory Committee (DMAC), in which member states are represented, is also to be created. Furthermore, a High-Level Group will be created in which BEREC is represented together with other European organisations. Both bodies will assist the Commission in its oversight duties.

Nkom also supports the DMA proposal and the underlying goals of the regulations. Gateway providers restrict the openness of the internet in a similar way to internet access providers before net neutrality regulations were introduced. Regulation that can ensure the openness of the internet at the application layer is therefore crucial.

The European Commission, the European Parliament and the Council reached political agreement on the DMA proposal on 24 April 2022. Formal approval by the European Parliament and by the Council is expected during the second half of 2022. DMA will take effect six months after the regulations are adopted.

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

2.8 Internet governance

Nkom works in line with the Norwegian government's objective to "Participate actively in the debate on the development of the internet and, through the electronic communication authority, participate in international organisations dealing with internet governance, further development of internet technology and internet architecture". Nkom particularly closely monitors the development related to "New IP" and similar initiatives and believes that the standardisation of internet technology should be led by IETF, which has traditionally played the leading role in the further development of the internet's architecture.

2.8.1 About internet governance

International internet governance takes place along two different axes: The ITU (International Telecommunication Union), which follows the UN track based on multilateral processes, and the multistakeholder track whereby ICANN (Internet Corporation for Assigned Names and Numbers) has overall responsibility for coordinating internet resources such as domain names and IP addresses. Between these two organisations we find the IGF (Internet Governance Forum), which serves as a bridge between the two axes.

Norway participates in these international organisations through KDD (Norwegian Ministry of Local Government and Regional Development) and Nkom. Norwegian authorities emphasise European cooperation in the field of internet governance and participate in the COM-ITU for European coordination of ITU work, and in the HLIG for European coordination of the activities of the Governmental Advisory Committee (GAC) within ICANN.

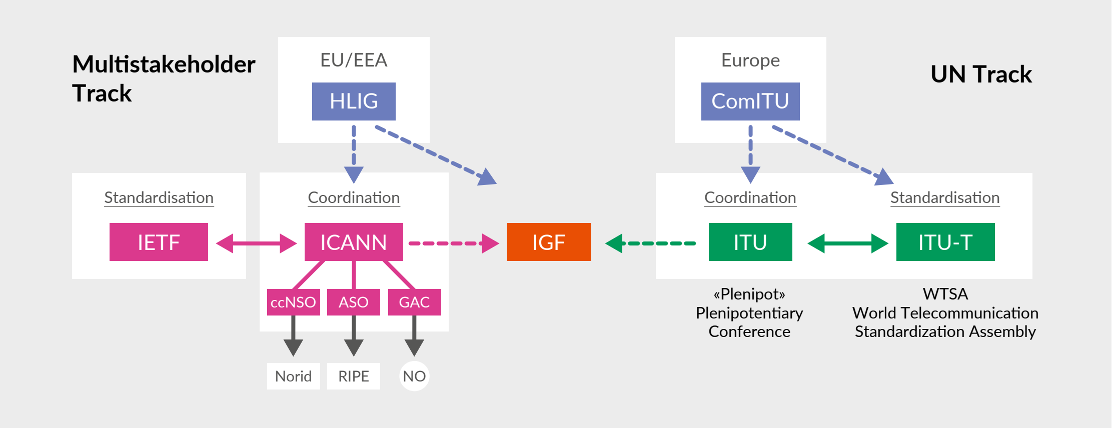

Figure 15 – Two axes of internet governance: the Multistakeholder Track and the UN Track

2.8.2 UN Track

ITU

Several of the ITU member states have for some time been working actively to give ITU greater influence on the resource management and development of the internet, specifically the administration and management of internet resources such as domain names and IP addresses. This is in conflict with the governance model used in ICANN, whereby the different stakeholder groups are equated.

Particularly the standardisation work related to the internet taking place within ITU-T challenges the interests of Norwegian and other Western countries in terms of internet governance. “New IP” and “Facial recognition” are two examples of standardisation work that can be seen as an element of the positioning of ITU as a major player in the internet’s development, at the expense of the Internet Engineering Task Force (IETF). The wish for increased public control of the internet is the goal.

The ITU Plenipotentiary Conference (PP) is held every four years and is the ITU’s supreme body. PP-22 will take place in Bucharest, Romania on 26 September – 14 October 2022. There are expected to be discussions of the resolutions relating to the internet.

WTSA-20

The World Telecommunication Standardization Assembly (WTSA) sets the direction and structure for the work within the telecommunication standardisation branch of the ITU (ITU-T) for the next four years. WTSA-20 was held in Geneva in March 2022, two years later than originally planned, as a consequence of the pandemic.

The war in Ukraine left its mark at the meeting and as requested by Ukraine there was consensus that candidates from Russia and Belarus should not be elected for leadership office in the ITU-T.

2.8.3 Multistakeholder Track

ICANN

During the reporting period for this Annual Report, three ICANN meetings were held. At these meetings, two main issues were a recurring theme: (1) New application round for generic top-level domains, and (2) Adaptation of WHOIS to GDPR.

The preparation for a new application round for generic top-level domains has been a recurring topic within ICANN for several years. After ICANN in 2012 conducted its first widescale expansion of the number of top-level domains, the organisation has commenced the preparation of a subsequent round.

ICANN Org has relatively recently started up the Operational Design Phase (ODP) for the project, and the result is scheduled for completion towards the end of 2022. It is indicated that the actual application round could start up in 2023-24.

Adaptation of WHOIS to GDPR

Traditionally, information about domain name owners has been openly available via the WHOIS database. Among other things, the database has been an important tool for identifying domain owners in combating crime and countermeasures against online fraud.

When GDPR came into force, the work of bringing WHOIS into line with the regulation commenced. A temporary scheme for shielding personal data was introduced, while providing access to non-public data for legitimate entities, typically government bodies.

ICANN then created a project to establish a permanent solution. Phase 1 of the project has prepared a principal model, while Phase 2 specifies a data system for processing data requests (System for Standardised Access/Disclosure, SSAD).

In this project, the Operational Design Phase (ODP) was recently concluded, with the conclusion that it will probably take 5-6 years before SSAD can be put into operation. The ICANN Board will now decide on the fate of the project, based on the ODP results.

N K
O M

Address for visitors: Nygård 1, Lillesand, Norway
Postal address: Postbox 93, NO-4791 Lillesand
Tel. no.: (+47) 22 82 46 00
nkom.no