Digital Information Literacy Guide

A DIGITAL INFORMATION LITERACY GUIDE
FOR CITIZENS IN THE DIGITAL AGE

FaktaBaari EDU

Kari Kivinen, Minna Aslama Horowitz, Pipsa Havula, Tiina Härkönen, Carita Kiili,
Elsa Kivinen, Harto Pönkä, Joonas Pörsti, Mikko Salo, Riina Vuorikari & Jukka Vahti

Digital Information Literacy Guide. A digital information literacy guide for citizens in the digital age

ISBN 978-952-69148-3-1 (EN)
ISBN 978-952-69148-2-4 (FI)

2022 Avoin yhteiskunta ry / Faktabaari EDU

Editor in chief: Kari Kivinen

Writers: Kari Kivinen, Minna Aslama Horowitz, Pipsa Havula, Tiina Härkönen, Carita Kiili, Elsa Kivinen, Harto Pönkä, Joonas Pörsti, Mikko Salo, Riina Vuorikari, Jukka Vahti

Illustrations: Lumi Pönkä

Language check: Elsa Kivinen & John O'Connor

Citations: Kivinen, K., Aslama Horowitz, M., Havula, P., Härkönen, T., Kiili, C., Kivinen, E., Pönkä, H., Pörsti, J., Salo, M., Vahti, J., & Vuorikari, R. (2022). Digital Information Literacy Guide, Faktabaari, Helsinki

Co-funded by:

NORdic observatory
for digital media and
information DISorders

Co-financed by the Connecting Europe
Facility of the European Union
Contract number: INEA/CEF/ICT/A2020/2394203

SITRA

Digital Information Literacy Guide

A digital information literacy guide for citizens in the digital age

Digital Information Literacy

Digital information literacy is the ability to access, manage, understand, integrate, communicate, evaluate, create, and disseminate information safely and appropriately through digital technologies.

It includes competences that are variously referred to as information literacy and media literacy, computer, and ICT literacy but also an ability to understand the functioning of the digital information landscape at large.

Digital Information Literacy involves a dimension of active and civic engagement with the digital world and promotes active citizenship.

PROLOGUE

Digital information literacy is a modern civic skill that underpins participation in democratic decision-making. Finland is renowned for its high literacy rate, and the teaching of multiple literacies has been integrated into current curricula from early childhood education onwards.

However, on digital platforms such as TikTok, YouTube, Instagram and Facebook, children and young people are confronted with a bewildering flood of information that they may not be able to filter out with the skills they have acquired in the school community and at home: claims about products by influencers, search results tailored by commercial algorithms, cleverly scripted propaganda and authorisations to track online behaviour or physical movement in urban space hidden behind countless 'yes' buttons.

It is therefore important to strengthen the digital information literacy of all the web users, especially young people, in order to identify how we are being influenced online.

JOONAS PÖRSTI, EDITOR-IN-CHIEF OF FAKTABAARI

Table of Contents

Executive Summary

Digital information literacy is a modern civic skill that underpins participation in democratic decision-making. It can be defined as a citizen's ability to access, manage, understand, integrate, communicate, evaluate, create, and disseminate information safely and appropriately using digital technologies.

Digital information literacy brings together various other literacy approaches. It includes competences that are referred to as information and media literacy, computer, and ICT literacy but also an ability to understand the functioning of the digital information landscape at large. This means understanding the role of the big platforms in social media and citizen's rights for privacy. Digital Information Literacy involves a dimension of active and civic engagement with the digital world and promotes active citizenship.

Faktabaari's Digital Information Literacy Guide includes 15 texts from 10 Finnish experts. Riina Vuorikari and Kari Kivinen introduce the newly published digital competence framework for citizens (DigComp 2.2.), which for the first time includes examples of media and information literacy knowledge, skills and attitudes.

Finns are frequent users of social media services and have a very positive attitude towards them. Harto Pönkä analyses Finns' use of social media through a wide range of studies and lists the latest social media trends.

Carita Kiili presents the latest online reading research projects of the Critical group and sheds light on what investigative, critical online reading can be like.

Kari Kivinen presents different working methods used by fact-checkers such as prebunking, debunking, sourcing, strategic ignorance and lateral reading, He also shares information about civic online reasoning strategies.

According to Minna Aslama Horowitz we should take our rights and responsibilities seriously as digital citizens and be aware of our digital rights. Minna Aslama Horowitz presents the framework of information disorders created by Claire Wardle and Hossein Derakhshan. Their theory distinguishes between different types of content according to their purpose (mis-, dis-, and malinformation).

Joonas Pörsti defines political propaganda as a broad form of influence, aimed at persuading the target audience to act in accordance with the propagandist's objectives. As an antidote to propaganda, he recommends fact-checking, digital information literacy and an understanding of propaganda techniques.

Pipsa Havula shares some of the working methods of fact-checkers and suggests what social media users could learn from fact-checkers.

Mikko Salo discusses the ethical issues of fact-checking and briefly reviews the history of the development of ethical codes that complement good journalistic practice.

Kari Kivinen presents the Stanford group's criteria for assessing the expertise of scientists. He also presents a decision chart to facilitate the evaluation of scientific claims.

Harto Pönkä describes different algorithms and how they work and gives practical tips for online users on how to be conscious about algorithms and their operations. To be a fully informed agent in the digital environment and to be able to manage privacy in it, it is necessary to understand how the different devices and services used collect information about users.

Tiina Härkönen presents the results of Sitra's Digitrail survey and the Digipower investigation. The studies revealed in concrete terms the large-scale operation of data collection ecosystems, the countless different entities that process our data and the huge amount of data that is generated about us and stored for unknown companies to use. She shares information about Sitra's Digiprofile test – for children, young people and adults.

Sitra's four-year Digital Power and Democracy project aims to increase understanding of the nature of networked, digital power and to find ways to harness that power - the power of the web - to reform democracy. Jukka Vahti discusses how to harness the power of the web to support and renew democracy.

The Digital Information Literacy Guide answers at least the following questions:

- **What is digital information literacy?**
- **What does it mean to be digitally competent today?**
- **What are the trends in social media in Finland at present?**
- **What is the process of investigative online reading – and how to evaluate it?**
- **What are the user's rights in online environments?**
- **How to define information disorders?**
- **Which are the forms of online propaganda?**
- **What can we learn from fact-checkers?**
- **How to identify a real fact-checker?**
- **How to evaluate a scientific claim?**
- **How to evaluate the expertise of an expert?**
- **What kind of challenges do we face with algorithms and artificial intelligence?**
- **What kind of digital footprint do we leave?**
- **What is Digipower in practice?**
- **How to defend democracy in the online environment?**

Introduction

ELSA KIVINEN & KARI KIVINEN

In the first chapter, Kari Kivinen briefly introduces the different types of media and information literacy skills and their differences and overlaps. Why has the Finnish FaktaBaari decided to promote and support digital information literacy for citizens?

The EU has set ambitious targets that at least 80% of the population should master basic digital skills by 2030. What are these basic digital skills? How are they defined and how could they be promoted?

In the second chapter, DigComp 2.2. author Riina Vuorikari and Kari Kivinen present a digital competence framework for citizens, which for the first time includes examples of media and information literacy knowledge, skills and attitudes. What does it mean to be digitally competent today?

The general assumption is that young people are digital natives, skilled users of modern digital technologies. This may be true for some, but studies have shown that young people are surprisingly inexperienced in some areas, such as assessing the authenticity of online sources, distinguishing advertisements from other content, and so forth. Unfortunately, this is not only true for young people, but for all of us internet users. **In chapter three**, Kari Kivinen explains why everyone should be able to judge whether online claims are reliable. This requires good general knowledge and digital information literacy, which needs to be taught and practised until it becomes as natural as riding a bicycle.

Finns are frequent users of social media services and have a very positive attitude towards them. **In chapter four**, Harto Pönkä analyses Finns' use of social media through a wide range of studies and lists the latest social media trends:

- Covid-19 and the war in Ukraine boosted Finns' social media use
- Short videos on TikTok and Instagram Reels are growing in popularity
- Young people's messaging is moving from What's Up to Snapchat
- Fake content and bought reactions on the rise.

The CRITICAL project, funded by the Finnish Strategic Research Council, is studying critical literacy skills of children and young people, including what supports positive development. The results will be used to develop teaching methods and tools to support critical literacy. **In chapter five**, Carita Kiili presents the latest online reading research projects of the Critical group and sheds light on what investigative, critical online reading can be like. The results of Critical Group's research show that pupils and students need support to gain a deeper understanding of the reliability of evidence.

There are many differences between online and off-line environments. In digital environments, the amount of information available to anyone is breathtaking. In addition, almost anyone can effortlessly disseminate any information to large audiences in an instant. Online environments are evolving rapidly and continuously compared to traditional off-line environments. Online news content can be changed, deleted and added to all the time. In addition, inaccurate or distorted information is increasingly being disseminated online. Therefore, traditional reading skills should be complemented by new online assessment strategies and online literacy skills.

In chapter six, Kari Kivinen presents methods, which have been proven to be effective to tackle disinformation: prebunking (anticipation), debunking (correction), strategic ignorance (the skill of ignoring large numbers of search results that do not meet our information needs and are not worth reading) and lateral reading, where the reader checks the background of the online information (reliability of the author, facts, statistics, sources, etc.) from various sites and sources before delving deeper into the text at hand. Other online literacy skills include 'civic online reasoning' (who is behind the information, what is the evidence and what do other sources say?) and 'click restraint strategy' (when opening search engine results, careful pre-checking is used and focusing on relevant and information-relevant search results from reliable sources).

The digital environment can enlighten, entertain and educate us. It can help us innovate, create, earn a living, connect with others and make a difference. Given the huge potential of the digital environment, we should also take seriously our rights and responsibilities as digital citizens. **In the seventh article**, Minna Aslama Horowitz lists the organisations that support digital citizens' rights:

- The UN lays the groundwork for basic principles and international forums where we can discuss our rights.
- The EU provides support through various legislative initiatives.
- Civil society organisations and groups are often at the forefront of tackling digital harms and problems.
- DigComp 2.2 also gives us a framework to understand what kind of digital citizenship skills we need.

In chapter eight, Minna Aslama Horowitz presents the framework of information disorders created by Claire Wardle and Hossein Derakhshan. Their theory distinguishes between different types of content according to their purpose (mis-, dis-, and malinformation).

In chapter 9, Joonas Pörsti, the editor-in-chief of Faktabaari, explains political propaganda as a broad form of influence, aimed at persuading the target audience to act in accordance with the propagandist's objectives. The hallmark of propaganda is psychological manipulation, typically using disinformation, i.e. deliberately disseminated misleading information

As an antidote to propaganda, Joonas Pörsti recommends fact-checking, digital information literacy and an understanding of propaganda techniques. The impact of propaganda can be weakened by revealing the methods used in advance, so that the manipulation loses its effectiveness as the public leaves the propagandistic messages to their own devices.

In chapter 10, Pipsa Havula, a fact-checker at FaktaBaari, opens up the working methods of fact-checkers and suggests what social media users could learn from fact-checkers.

Fact-checking is the process of checking whether a claim made in public is true or not. Fact-checking helps to distinguish false, distorted, misleading or ill-founded claims from reliable and truthful information. However, it is important to remember that the interpretation of claims is not always unambiguous and that facts can also be interpreted in different ways. For this reason, fact-checking seeks to be as transparent as possible about the source of the information, so that the reader can judge the reliability of the sources and form his or her own opinion. Pipsa Havula also illustrates how anyone can check the accuracy of images and videos.

In chapter eleven, Mikko Salo, the founder of Faktabaari and the contact person with EDMO NORDIS project (Nordic Observatory for Digital Media and Information Disorder), discusses the ethical issues of fact-checking and briefly reviews the history of the development of ethical codes that complement good journalistic practice. He gives an overview of the fact-checkers' approach to information assessment as a public service and explains how ordinary citizens can identify a fact-checker who is committed to an ethical code of transparency.

FaktaBaari has been involved in a project coordinated by Stanford University, where an international team of science and digital literacy experts examined how science education should respond to the challenges posed by the online misuse of scientific information and scientific evidence. The report considers, among other things, how to verify scientific claims made on social media and how to assess the competence of the person making the claim as an expert in the field.

In chapter twelve, Kari Kivinen presents the Stanford group's criteria for assessing the expertise of scientists. He also presents a decision chart to facilitate the evaluation of scientific claims.

Researched knowledge is the best current understanding of the issues. It is not anyone's opinion or personal experience, but the result of a systematic process. It changes and evolves as new research results are discovered and as our understanding grows. There is a wealth of researched information and reliable sources on the internet.

The concept of algorithms is often associated with the functions of web services and applications. But an algorithm is originally a mathematical concept. An algorithm is often a series of steps to solve a problem or solve a task. **In chapter thirteen**, Harto Pönkä describes different algorithms and how they work, for example on Facebook. Algorithms have an impact on the behaviour of their users, and most often this impact is seen in the content that is recommended to users. The business of online and social services is usually based on ad monetisation, i.e. users clicking on ads targeted at them. Naturally, this is encouraged by the need to keep them as happy as possible for as long as possible. It is therefore clear that algorithms are tuned to do just that, even if the services do not express it on their own. The most important thing for users' privacy would be to know in which ways their personal data are used by the algorithms. Indeed, new EU legislative packages are in the process of requiring greater transparency from online services on how algorithms work.

Privacy is one of the most important fundamental rights in the digital age. It is based on national laws and European Union regulations such as the EU General Data Protection Regulation (GDPR) on the one hand, and international treaties and the UN Declaration of Human Rights on the other. Privacy is primarily about the protection of private life, home and communications, but in the digital environment it is more appropriate to talk about information relating to a specific person, i.e. personal data. This is the data that is stored on the digital devices and services we use, such as search engines and social media platforms. **In chapter 14**, Harto Pönkä introduces us to the secrets of active and passive digital footprints.

To be a fully informed actor in the digital environment and to be able to manage privacy in it, it is necessary to understand how the different devices and services used collect information about users. It is also important to be aware of the privacy concerns of other users, so as not to unintentionally infringe their privacy in the digital environment. The article answers important questions such as:

- To whom is it safe to share my data?
- How do cookies work?
- Should you share your location?
- How can data be deleted?

In chapter 15, Tiina Härkönen, Senior Specialist at Sitra, presents the results of Sitra's digitrail survey and the digipower investigation. The studies revealed in concrete terms the large-scale operation of data collection ecosystems, the countless different entities that process our data and the huge amount of data that is generated about us and stored for unknown companies to use. Unfortunately, the findings of both surveys also revealed how poorly data giants comply with European data protection legislation. The digipower investigation also sought to understand whether data and profiling can also be used to influence societal decision-making.

Sitra, in cooperation with experts in the field, has developed a digital behaviour assessment tool - the digiprofile test - for children, young people and adults. The test assesses three different aspects: knowledge, attitudes and online behaviour. The result is a personalised digital profile and personalised tips on how to manage your information.

Jukka Vahtii, Sitra's lead expert on democracy and inclusion, discusses **in chapter sixteen** how to harness the power of the web to support and renew democracy in the article "Digital literacy is a key tool to defend democracy". The rapid changes in the media environment have given rise to numerous new ways of influencing society and new forms of digital power. This has blurred the boundaries between decision-maker and citizen, influencer and influenced, and sender and receiver of messages. A troll spreading confusion with disinformation on social media wields online power in the same way as an active citizen organising online help for people fleeing war, for example. The same is true at the systemic level: digitalisation and various forms of networked power can accelerate the development of society in a democratic or undemocratic direction.

Sitra's four-year Digital Power and Democracy project aims to increase understanding of the nature of networked, digital power and to find ways to harness that power - the power of the web - to reform democracy.

Democracy is based on a sufficiently shared understanding of reality among different people and populations, including a desire for truth, i.e. the desire to know what is true and the ability to form their own opinions based on the information available. Critical digital information literacy and, more broadly, digital civilisation are key to this. The ability to form opinions based on information is a prerequisite for participation in society.

This publication is part of EDMO Nordis project.

Access to information in all its forms is a basic human right and need.

- UNESCO[1]

1. Digital Information Literacy DIL

KARI KIVINEN, FAKTABAARI EDU

The rapid development of the digital online environment has profoundly changed the way we search, analyse, use, and share information.

Powerful search engines can find millions of hits for our search in a nanosecond. The real online challenge is to sort out which information is useful and meets our initial information need. In addition, the search results are very individual and lack transparency. Third parties can influence the order in which the results are shown, for example by technical coding or by buying visibility from the search engine platforms. Unfortunately, the quality and breadth of sources and relevant information in the top search results has diminished as more and more commercial pages find their way on top of the search results. Simultaneously, the sheer volume of mis- and disinformation has increased in recent years.

We need human critical thinking to evaluate the fit of the content that the algorithms are proposing for us. To do this, it is vital to develop our digital information literacy skills.

Literacy definitions

The terminology concerning various online literacies is still in the process of being established. Currently, there are several slightly overlapping digital literacy approaches in the literature. The European Commission expert group tackling disinformation and promoting digital literacy chose to use the term "Digital Literacy". Other relatively common terms are "Critical Literacy" and "Internet Literacy". The online environment has evolved at an extraordinary pace, and new terms related to understanding the online environment appear almost weekly. Here we introduce a few literacy terms relevant to the Nordis project.

Critical literacy refers to an individual's ability to seek information, evaluate, source and interpret texts, and use the overall picture formed by texts in decision making and apply what they have learned when engaging with different communities.[2]

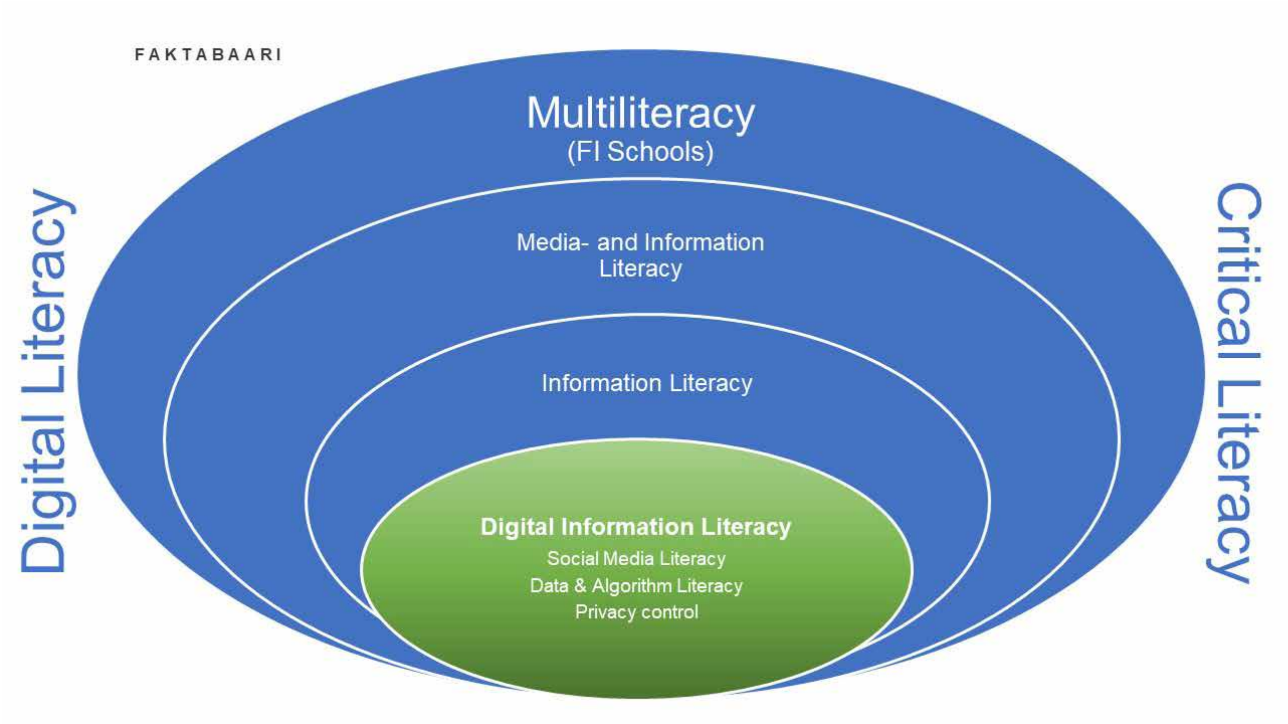


Figure: Digital Literacies

Multiliteracy

The term multiliteracy used in the Finnish national core curriculum is a good way to describe the challenges and requirements the modern communication environment imposes on children and adolescents. In addition to traditional written text, they are expected to interpret and evaluate other types of communication and media texts and to have the competence to handle a great variety of media and communication channels.

The Finnish curriculum describes multiliteracy as follows: "The pupils need multiliteracy in order to interpret the world around them and to perceive its cultural diversity. Multiliteracy means abilities to obtain, combine, modify, produce, present and evaluate information in different modes, in different contexts and situations, and by using various tools. Multiliteracy supports the development of critical thinking and learning skills."[3]

Media and Information Literacy

UNESCO promotes the development of Media and Information Literacy (MIL) for all to enable people's ability to think critically and click wisely[4].

MIL can be defined as an interrelated set of competencies that help people to maximise advantages and minimise harm in the new information, digital and communication landscapes. Media and information literacy covers competencies that enable people to critically and effectively engage with information, other forms of content, the institutions that facilitate information and diverse types of content, and the discerning use of digital technologies. Capacities in these areas are indispensable for all citizens regardless of their ages or backgrounds.

According to Unesco's approach, response to disinformation and misinformation requires a combination of critical information, media, and digital competencies, i.e., media and information literacy (MIL).

Information Literacy

One aspect of multiliteracy is information literacy– the ability to find and constructively critically analyse and understand different texts, messages and news and their contexts[5]. According to Suvi Alaranta[6], the information literacy can be defined as an ability to search for, acquire, evaluate and use information:

"Information literacy consists of identifying information needs, managing sources of information, accessing and using information, assessing information and making use of it - it progresses from information needs to information end-use."

Susie Andretta[7] describes an information literate person as having the ability to:

- Determine the extent of information needed
- Access the required information effectively and efficiently
- Evaluate information and its sources critically and incorporate selected information into his/ her knowledge base and value system
- Use information effectively to accomplish a specific purpose
- Understand many of the economic, legal, and social issues surrounding the use of information, and access and use information ethically and legally

Information literacy covers all the information available to an individual in its various forms - for example, printed products, digital content, data, images and speech. Information literacy is a part of multiple literacies and is closely linked to digital, academic, media and information literacy.

Digital Information Literacy

As a fact-checking organization, Finnish Faktabaari is particularly interested in promoting Digital information literacy, which can be defined as a set of skills and abilities which everyone needs to undertake information-related tasks:

Digital information literacy is the ability to access, manage, understand, integrate, communicate, evaluate, create, and disseminate information safely and appropriately through digital technologies.

It includes competences that are variously referred to as information literacy and media literacy, computer, and ICT literacy but also an ability to understand the functioning of the digital information landscape at large.

Digital Information Literacy involves a dimension of active and civic engagement with the digital world and promotes active citizenship.

"A democratic society depends upon access to true and reliable knowledge, and on the ability to distinguish knowledge that is flawed, incomplete, or that which aims to deceive from that which can be trusted. Hence, the chasm between the public perception of young people's competence and their actual performance represents a growing threat to society, particularly when disinformation proliferates and young adults spend more and more time on digital devices."[8]

Digital information literacy allows us to understand power and the need for the accountability of numerous stakeholders who create technologies, platforms, and content for us in the digital age. Being able to critically evaluate the multiple sources of information empowers us as citizens to reach and express informed views and to engage with society from an informed point of view.

According Manchester University Democracy@Risk report[9] digital information literacy is "a promising pathway for empowering citizens and cultivating mass-level resilience to misinformation and harmful online practices - however, the slow pace of change and the scale of cognitive demands placed on citizens means that it should be treated as only one part of a broader, multi-layered and multi-actor strategy for tackling online harms".

The NORDIS[10] project brings together fact-checking experts, researchers, journalists, and pedagogues to provide digital information literacy support to citizens to resist the perils of mis- and disinformation.

[1] Unesco https://en.unesco.org/sites/default/files/mil_curriculum_second_edition_summary_en.pdf

[2] Critical. (2021). Teknologisia ja sosiaalisia innovaatioita kriittisen lukemisen tukemiseen internetin aikakaudella (CRITICAL): Tilannekuvaraportti 2021. https://www.aka.fi/globalassets/3-stn/1-strateginen-tutkimus/strateginen-tutkimus-pahkinankuoressa/tilannekuvaraportit/stn2020-hankkeet/tilannekuvaraportti-critical.pdf

[3] Finnish National Core Curriculum (2016) https://www.oph.fi/en/statistics-and-publications/publications/new-national-core-curriculum-basic-education-focus-school

[4] Unesco: https://www.unesco.org/en/communication-information/media-information-literacy/about

[5] Kivinen et al (2020) Informaatiolukutaito-opas. Avoin yhteiskunta/Faktabaari. https://faktabaari.fi/assets/Informaatiolukutaito-opas_Faktabaari_EDU.pdf

[6] Alaranta, Suvi, (2018) Informaatiolukutaito: määritelmät ja käyttötarkoitus https://www.theseus.fi/bitstream/handle/10024/159543/ Alaranta_Suvi.pdf?sequence=1&isAllowed=y

[7] Susie Andretta (2005). Information Literacy: A Practitioners Guide

[8] Osborne et al. (2020) https://sciedandmisinfo.sites.stanford.edu/sites/g/files/sbiybj25316/files/media/file/science_education_in_an_age_of_misinformation.pdf

[9] Democracy@Risk Report (2021), Manchester University https://www.manchester.ac.uk/discover/news/democracyrisk---report-and-launch-event/

[10] EDMO Nordis – Sitra https://www.sitra.fi/en/projects/edmo-nordis-and-digital-information-literacy/

2. What does it mean to be digitally competent today?

RIINA VUORIKARI, JOINT RESEARCH CENTRE & KARI KIVINEN, FAKTABAARI EDU

DigComp 2.2 background

The Digital Competence Framework for citizens[2] (DigComp) is based on Key competences for lifelong learning recommendation[3] which was updated in 2018. Competences are composed of concepts and facts (i.e. knowledge), descriptions of skills (e.g. the ability to carry out processes) and attitudes (e.g. a disposition, a mindset to act) that everyone needs for self-fulfillment and development, employment, social inclusion, and active citizenship.

The EU has set ambitious targets for 80% of the population to have at least basic digital skills by 2030[1].

So, what are such digital skills and how are they defined?

DigComp is considered as one of the main digital policy-making tools of the European Digital Strategy including initiatives such as Skills Agenda, the Digital Education Action Plan, the Digital Decade and Compass, and the Pillar of Social rights and its action plan. The target of 80% of the population with at least basic digital skills is also based on DigComp.

Updated in March 2022, the DigComp 2.2[3] framework provides more than 250 new examples of knowledge, skills and attitudes that help citizens to use digital technologies confidently, critically and safely for participation in society. The update was necessary because new technologies such as Artificial Intelligence (AI), virtual and augmented reality, robotisation, the Internet of Things, datafication, or new social media challenges such as increase of mis- and disinformation, have led to a change in digital competence requirements for citizens.

What is new in DigComp 2.2?

DigComp 2.2 includes more than 250 examples highlighting new and emerging themes that have arisen since the last update (2017). The new examples will become useful, for example, for those who are responsible for curriculum planning and updating. They can use these examples to address themes that are relevant in today's society, the following are taken form DigComp 2.2:

- misinformation and disinformation in social media and news sites (e.g. fact-checking information and its sources, fake news, deep fakes)
- media literacy skills as part of understanding the role of media
- the trend of datafication of internet services and apps (e.g. focus on how personal data is exploited)
- citizens interacting with AI systems (including data-related skills, data protection and privacy, but also ethical considerations)
- environmental sustainability concerns

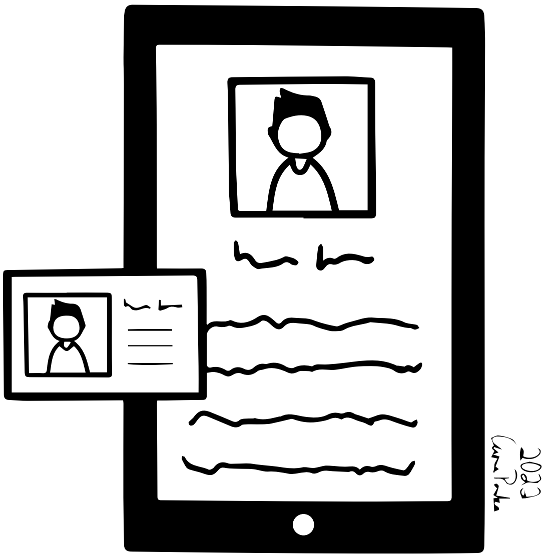
DigComp knowledge, skills and attitudes examples can be used as a basis for developing explicit descriptions of learning objectives, content, learning experiences and their assessment, although this will require more instructional design and implementation.

A deeper look into DigComp 2.2 examples

Information literacy examples

In DigComp 2.2, new examples of applying Information literacy competencies in digital environments have been added as part of the framework. At the heart of this lies general literacy competences. According to the aforementioned recommendation on Key competences for lifelong learning, literacy includes "the ability to distinguish and use different types of sources, to search for, collect and process information". As an increasing amount of information and content is made available online, these skills are needed to critically assess the credibility and reliability of sources, information and digital content that are found online.

In the following, a set of illustrative examples are given related to a competence or a theme. The numbering refers to the examples in the DigComp 2.2 publication.



DigComp 2.2	**1.2 EVALUATING DATA, INFORMATION AND DIGITAL CONTENT** To analyse, compare and critically evaluate the credibility and reliability of sources of data, information and digital content. To analyse, interpret and critically evaluate the data, information and digital content.
Knowledge	**Some examples of DigComp 2.2** 16. Aware that online environments contain all types of information and content including misinformation and disinformation, and even if a topic is widely reported it does not necessarily mean it is accurate. 17. Understands the difference between disinformation (false information with the intent to deceive people) and misinformation (false information regardless of intent to deceive or mislead people). 18. Knows the importance of identifying who is behind information found on the internet (e.g. on social media) and verifying it by checking multiple sources, to help recognise and understand point of view or bias behind particular information and data sources 19. Aware of potential information biases caused by various factors (e.g. data, algorithms, editorial choices, censorship, one's own personal limitations).
Skill	24. Knows how to differentiate sponsored content from other content online (e.g. recognising advertisements and marketing messages on social media or search engines) even if it is not marked as sponsored. 25. Knows how to analyse and critically evaluate search results and social media activity streams, to identify their origins, to distinguish fact-reporting from opinion, and to determine whether outputs are truthful or have other limitations (e.g. economic, political, religious interests). 26. Knows how to find the author or the source of the information, to verify whether it is credible (e.g. an expert or authority in a relevant discipline). 27. Able to recognise that some AI algorithms may reinforce existing views in digital environments by creating "echo chambers" or "filter bubbles" (e.g. if a social media stream favours a particular political ideology, additional recommendations can reinforce that ideology without exposing it to opposing arguments).
Attitude	28. Inclined to ask critical questions in order to evaluate the quality of online information and concerned about purposes behind spreading and amplifying disinformation. 29. Willing to fact-check a piece of information and assess its accuracy, reliability and authority, while preferring primary sources over secondary sources of information where possible. 30. Carefully considers the possible outcome before clicking a link. Some links (e.g. compelling titles) could be "clickbait" that takes the user to sponsored or unwanted content (e.g. pornography)

Participatory citizenship through appropriate digital technologies

One aspect of the DigComp competences defines civic participation through digital technologies. Citizenship competence is defined in the Key competences for lifelong learning as "the ability to act as a responsible citizen and to participate fully in civic and social life". Citizens should be, for example, able to participate in society through the use of public and private digital services. Participatory citizenship is also intrinsically linked to media literacy, as it "requires the ability to use, critically understand and interact with both traditional and new forms of media and to understand the role and functions of the media in democratic societies" (ibid).

One concrete example of attitudes in this area is citizens being proactive about using the internet and digital technologies to seek opportunities for constructive participation in democratic decision-making and civic activities (e.g. by participating in consultations organised by municipality, policy-makers, NGOs; signing a petition using a digital platform).

DigComp 2.2	**2.3. Engaging citizenship through digital technologies** *To participate in society through the use of public and private digital services. To seek opportunities for self-empowerment and for participatory citizenship through appropriate digital technologies.*
Knowledge	**Some examples of DigComp 2.2** 73. Aware of civil society platforms on the internet that offer opportunities for citizens to participate in actions targeting global developments to reach sustainability goals on local, regional, national, European and international level. 74. Aware of the role of traditional (e.g. newspapers, television) and new forms of media (e.g. social media, the internet) in democratic societies.
Skill	77. Knows how to engage with others through digital technologies for the sustainable development of the society (e.g. create opportunities for joint action across communities, sectors and regions with different sustainability challenges) with an awareness of technology's potential for both inclusion/participation and exclusion.
Attitudes	80. Considers responsible and constructive attitudes on the internet as they are the foundation for human rights, together with values such as respect for human dignity, freedom, democracy and equality.

Media literacy competences & AI

Part of the media literacy competence is understanding the role that Artificial Intelligence (AI) plays in online environments and digital tools when they are used for interacting, communication and collaboration. Citizens interacting with AI systems should have knowledge about AI and its role in society as well as ethical considerations about its use and implementations in different parts of society. A specific appendix including more than 70 examples is part of DigComp 2.2 (see p. 77 in DigComp 2.2).

DigComp 2.2	Citizens interacting with AI systems (Appendix 2)
Knowledge	**Some examples of DigComp 2.2** AI 64. Knows that all EU citizens have the right to not be subject to fully automated decision-making (e.g. if an automatic system refuses a credit application, the customer has the right to ask for the decision to be reviewed by a person). AI 63. Recognises that while the application of AI systems in many domains is usually uncontroversial (e.g24. Knows how to differentiate sponsored content from other content online (e.g. recognising advertisements and marketing messages on social media or search engines) even if it is not marked as sponsored. 25. Knows how to analyse and critically evaluate search results and social media activity streams, to identify their origins, to distinguish fact-reporting from opinion, and to determine whether outputs are truthful or have other limitations (e.g. economic, political, religious interests). AI 48. Aware that AI algorithms might not be configured to provide only the information that the user wants; they might also embody a commercial or political message (e.g. to encourage users to stay on the site, to watch or buy something particular, to share specific opinions). This can also have negative consequences (e.g. reproducing stereotypes, sharing misinformation).
Skill	AI 58. Readiness to contemplate ethical questions related to AI systems (e.g. in which contexts, such as sentencing criminals, should AI recommendations not be used without human intervention?)
Attitudes	AI 62: Open to AI systems supporting humans to make informed decisions in accordance with their goals (e.g. users actively deciding whether to act upon a recommendation or not). AI 68. Open to engage in collaborative processes to co-design and co-create new products and services based on AI systems to support and enhance citizens' participation in society.

Focus on digital identity and personal data

Data-related skills and privacy issues related to one's digital identity form a core of new DigComp 2.2 examples. They focus on helping citizens safeguard their personal data while mitigating risks related to safety and privacy in digital environments.

For example, it is important that online users understand how to use and share personally identifiable data and information while being able to protect oneself and others from damages. Importance of understanding the key terms of EU's regulations such as Right to be Forgotten and General Data Protection Regulation (GDPR) are highlighted in examples too.

DigComp 2.2	**2.6 Managing digital identity** *To create and manage one or multiple digital identities, to be able to protect one's own reputation, to deal with the data that one produces through several digital tools, environments and services.*
Knowledge	**Some examples of DigComp 2.2** 104. Aware that AI systems collect and process multiple types of user data (e.g. personal data, behavioural data and contextual data) to create user profiles which are then used, for example, to predict what the user might want to see or do next (e.g. offer advertisements, recommendations, services). 105. Knows that in the EU, one has the right to ask a website's or search engine's administrators to access personal data held about you (right of access), to update or correct them (right of rectification), or remove them (right of erasure, also known as the Right To Be Forgotten).
Skill	108. Knows how to modify user configurations (e.g. in apps, software, digital platforms) to enable, prevent or moderate the AI system tracking, collecting or analysing data (e.g. not allowing the mobile phone to track the user's location).
Attitudes	114. Identifies both the positive and negative implications of the use of all data (collection, encoding and processing), but especially personal data, by AI-driven digital technologies such as apps and online services.

DigComp 2.2	**4.2. Protecting personal data and privacy** To protect personal data and privacy in digital environments. To understand how to use and share personally identifiable information while being able to protect oneself and others from damages. To understand that digital services use a "Privacy policy" to inform how personal data is used.
Knowledge	**Some examples of DigComp 2.2** 180. Knows that the "privacy policy" of an app or service should explain what personal data it collects (e.g. name, brand of device, geolocation of the user), and whether data is shared with third parties. 181. Knows that the processing of personal data is subject to local regulations such as the EU's General Data Protection Regulation (GDPR) (e.g. voice interactions with a virtual assistant are personal data in terms of the GDPR and can expose users to certain data protection, privacy and security risks).
Attitudes	187. Weighs the benefits and risks before allowing third parties to process personal data (e.g. recognises that a voice assistant on a smartphone, that is used to give commands to a robot vacuum cleaner, could give third parties - companies, governments, cybercriminals - access to the data).

Active citizenship and environmental concerns

DigComp 2.2 also contains examples of citizens' agency linked to environmental sustainability concerns. Today, becoming aware of the environmental impact of digital technologies, both their fabrication and their use, and being aware of the impact of one's choices on the environment, become a crucial part of digital competence. Digital tools and services can also be used to improve the environmental and social impact through various citizenship actions.

DigComp 2.2	4.4: PROTECTING THE ENVIRONMENT **To be aware of the environmental impact of digital technologies and their use.**
Knowledge	**Some examples of DigComp 2.2** 203. Aware of the environmental impact of everyday digital practices (e.g. video streaming that rely on data transfer), and that the impact is composed of energy use and carbon emissions from devices, network infrastructure and data centers. 209. Aware that certain activities (e.g. training AI and producing cryptocurrencies like Bitcoin) are resource intensive processes in terms of data and computing power. Therefore, energy consumption can be high which can also have a high environmental impact.
Skill	211. Knows how to reduce the energy consumption of devices and services used, e.g. change the quality settings of video streaming services, using Wi-fi rather than data connectivity when at home, closing apps, optimising email attachments). 212. Knows how to use digital tools to improve the environmental and social impact of one's consumer behaviour (e.g. by looking for local produce, by searching for collective deals and car-pooling options for transportation).
Attitudes	215. Considers product's overall impact on the planet when choosing digital means over physical products, e.g. reading a book online does not need paper and thus transport costs are low, however, one should consider digital devices including toxic components and needed energy to be charged. 216. Considers the ethical consequences of AI systems throughout their life-cycle: they include both the environmental impact (environmental consequences of the production of digital devices and services) and societal impact, e.g. platformisation of work and algorithmic management that may repress workers' privacy or rights; the use of low-cost labour for labelling images to train AI systems.

Supporting adoption of digital competence building

So what does it mean to be digitally competent today? As is seen above, DigComp provides the language to identify and describe the key areas of digital competence, a clear and understandable conceptual framework and a technology-neutral basis for a common understanding of concepts. This commonly agreed vocabulary has now been updated with relevant examples that fit today's digital world. The next steps are up to users, for example education and training organisations, to take advantage of the framework for setting educational objectives, updating training syllabus, and for evaluating and monitoring learning outcomes. An important part of this process is adapting the framework to their own needs, e.g. taking into account the local context and its requirements. Learning from one another in this process will be important in order to support confident and digitally competent citizens in the future.

3. From digital natives to digitally literate critical thinkers

KARI KIVINEN, FAKTABAARI EDU

A common assumption is that students are digital natives immersed in digital technology, and that young people pick up the skills necessary to use today's technology in a fluid and informed manner. Evidence suggests otherwise - young people struggle with evaluating the accuracy of online information[1].

While many youngsters are skilled users of digital devices and applications, research shows[2] that a surprising number struggle with information evaluation and are inexperienced in evaluating content from online sources, for example to distinguish advertisements from other content. In fact, we all struggle with evaluating the accuracy of claims made on social media.

The internet and social media are used by various actors to spread disinformation and they often use the language of science to give credibility to their claims. This undermines trust in science and, more broadly, trust in democracy.

It is therefore important to take a healthy critical approach to the information disseminated online, a skill that should be practised from primary school onwards.

Every member of our society should be able to judge when scientific claims are reliable. This requires both a basic knowledge of science and good digital information literacy skills. Digital media and information literacy must be taught and practised until it becomes as natural as riding a bicycle.[3]

Thinking and learning to learn is one of the Finnish cross-curricula themes[4], which refers to all those skills that can be learned through exploration and experimentation. It includes an investigative and observational way of working, as well as independent and extensive information gathering, and

> **"Our students may be "digital natives" but in some ways they are surprisingly inexperienced at evaluating sources online, distinguishing ads from other content, understanding what a .org domain name means and doesn't mean, navigating search results, etc."**
>
> Carl T. Bergström, University of Washington (Tweet)

the analysis of the information gathered. Emphasis should be placed on critical thinking and reasoning skills and their development.

Students should be encouraged to reflect on issues from different perspectives, to seek new information and to use this information to examine their ways of thinking. Students need encouragement in the presence of ambiguous and contradictory information. The practical implementation of such a learning framework involves all kinds of activities in which students are taught to[5]:

- clarify and specify ambiguous information and re-state arguments (e.g. when evaluating an election or advertising campaign, or when evaluating a blog post).
- identify and evaluate arguments in the communications they encounter.
- compare contradictory claims about reality and evaluate contradictions using their own judgement (e.g. by referring to facts).
- practise metacognition, i.e. awareness of one's own thinking and conscious reflection on one's own opinion formation.
- identify the influences of digital media and challenge distortions through researched information.

Critical thinking means careful reflection and cautious analytical thinking. It does not imply an inherently negative attitude towards the subject of criticism.

The development of critical thinking skills is a long-term process, best learned and taught through practical situations. A student may well understand why critical thinking is important and recognise the lack of it in others, but still be completely uncritical in practical situations.

To avoid critical thinking becoming encapsulated, i.e. limited to one context or type of situation, this practical training needs to be done in a variety of contexts and situations. Generalised, i.e. context-independent, critical thinking is best learned by applying the same simple critical thinking methods to different subjects, themes and events.

In social media, we have to make choices all the time: do I click, like, share, comment? In the digital world, critical thinking is largely a matter of patience, reflection and resistance to mis- and disinformation.

[1] Bennett, S., K. Maton, and L. Kervin, 'The 'digital natives' debate: A critical review of the evidence.' British journal of educational technology, 2008. 39(5): p. 775-786.

[2] Breakstone, J., Smith, M., Wineburg, S., Rapaport, A., Carle, J., Garland, M., & Saavedra, A. (2021). Students' Civic Online Reasoning: A National Portrait. Educational researcher, 50(8), 505-515. doi:10.3102/0013189X211017495

[3] Osborne, J., Pimentel, D., Alberts, B., Allchin, D., Barzilai, S., Bergstrom, C., Coffey, J., Donovan, B., Kivinen, K., Kozyreva. A., & Wineburg, S. (2022). Science Education in an Age of Misinformation. Stanford University, Stanford, CA.

[4] Finnish National Core Curriculum (2016) https://www.oph.fi/en/statistics-and-publications/publications/new-national-core-curriculum-basic-education-focus-school

[5] https://faktabaari.fi/assets/Informaatiolukutaito-opas_Faktabaari_EDU.pdf

4. COVID and Ukraine war increased Finns’ social media use

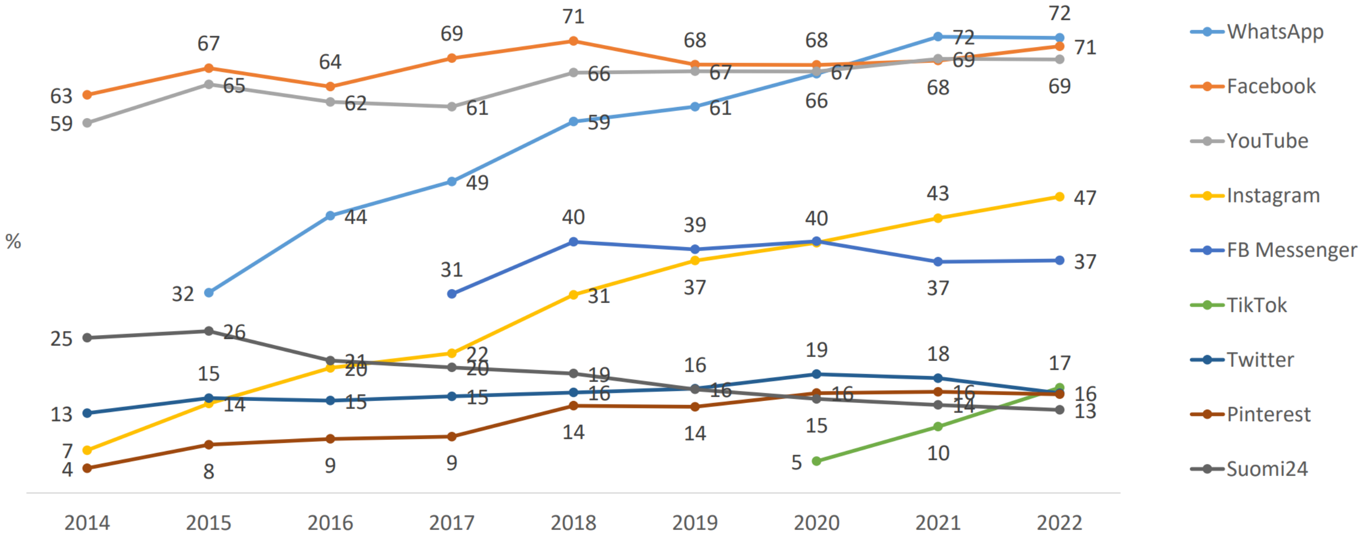
HARTO PÖNKÄ, INNOWISE

Finns are heavy users of social media services and have a very positive attitude towards them.

Many popular social media services such as Facebook, YouTube and Twitter became widely used in Finland shortly after their creation in 2006-2008. The year 2008 can be seen as the real breakthrough for social media in Finland. Since 2009, Facebook and YouTube have consistently ranked among the top three most popular websites in Finland, together with Google’s search engine.

The new services were first popular with young people and young adults but have gradually spread to older age groups. The take-up of social networking services among 16-89-year olds exceeded 50% for the first time in 2014 (SVT, 2014). Initially, it was mainly the use of Facebook.

The social media landscape has diversified over time. Since the early 2000s, a number of new social media services have been created, but most of them have either fallen out of popularity with small - and especially young - user communities or have since been discontinued. Although the social media landscape is constantly changing, for several years now WhatsApp, Facebook, YouTube and Instagram have been the most used social media services by Finns.



Q12a: Mitä seuraavista olet käyttänyt mihin tahansa tarkoitukseen viimeisen viikon aikana? Valitse kaikki sopivat vastaukset. N=kaikki vastaajat, 2022: 2064, 2021: 2009, 2020:2050, 2019: 2009, 2018: 2012, 2017: 2007, 2016: 2041, 2015: 1509, 2014: 1520.

Figure: Most popular social media services in terms of usage, Reuters Institute, 2022

Although Finns are not known for their talkativeness, social media seems to suit us. In a 2020 survey conducted by the research firm AudienceProject, Finns clearly rated social media as more important than respondents in other countries. No less than 56% of Finns considered social media important to them, compared to 50% in Germany, 46% in the UK, 43% in Norway and 36% in Sweden. In the same survey, Finns were also significantly more likely to consider the impact of social media on their lives as positive (41%) than negative (8%).

Overall, the Finns' relationship with social media can be described as enthusiastic and active. Connecting with friends and acquaintances is repeatedly cited as the main reason for using social media (e.g. SVT, 2018). For many, activities related to hobbies and work are also important, as is following companies and brands on social media. Especially in the context of Facebook, it often emerges that for many users, its various hobbies and work-related groups are the main reason for still being on Facebook.

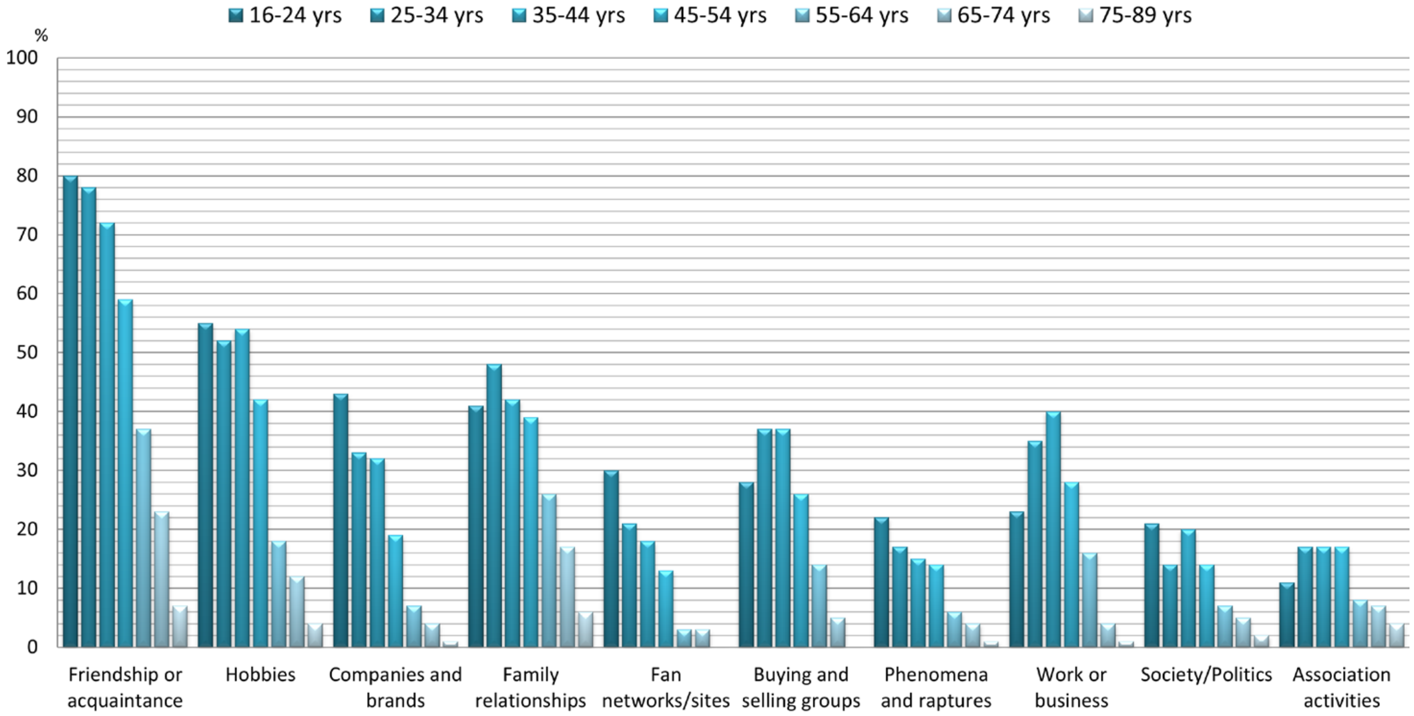
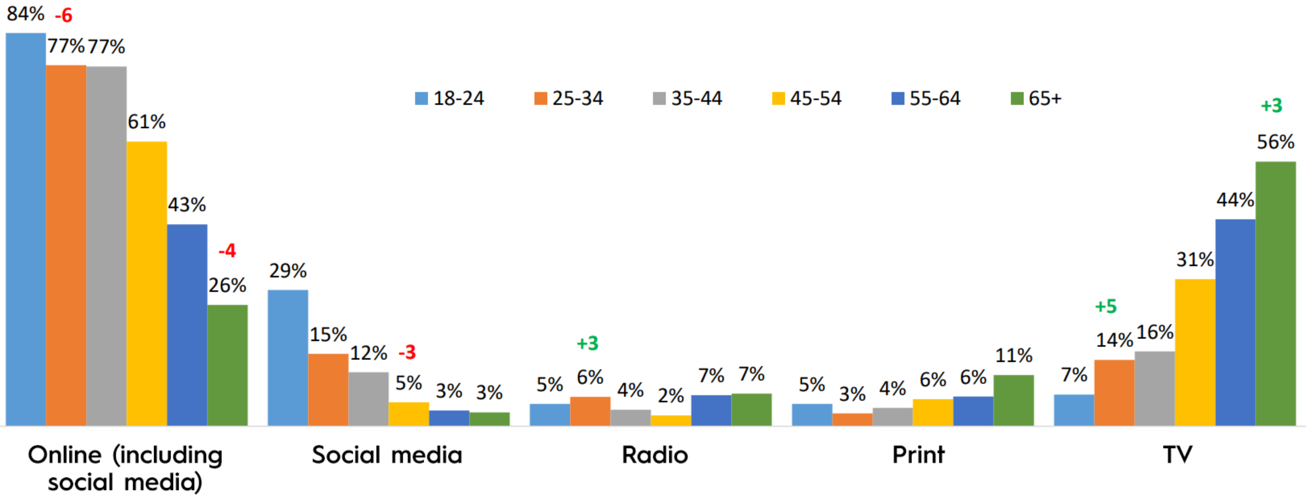


Figure: Following and participating in social media, Statistics Finland 2018, image: HP

Together with online news sites, social media has emerged as the most important channel for Finns to get news (Reuters Institute, 2022). News consumption on social media is particularly high among young users. Almost a third (31%) of Finns use Facebook to follow the news. Other sources of news are WhatsApp groups (14%) and YouTube channels (12%).



Q3/Q4: You have said to have used these news sources during the past week. Which one would you say is your main news source? N = number of people that have said to have used a news source in each age category. Minimum of three percentage point difference from last year has been marked with a coloured number as percentage points.

Figure: News sources by age group, Reuters Institute, 2022, image: HP

The coronavirus pandemic sparked a new social media boom

Social media use in Finland did not grow much between 2017 and 2019. However, the pandemic created a new social media boom, which increased the use of social media services and boosted the use of social networking services from 60% to 70%.

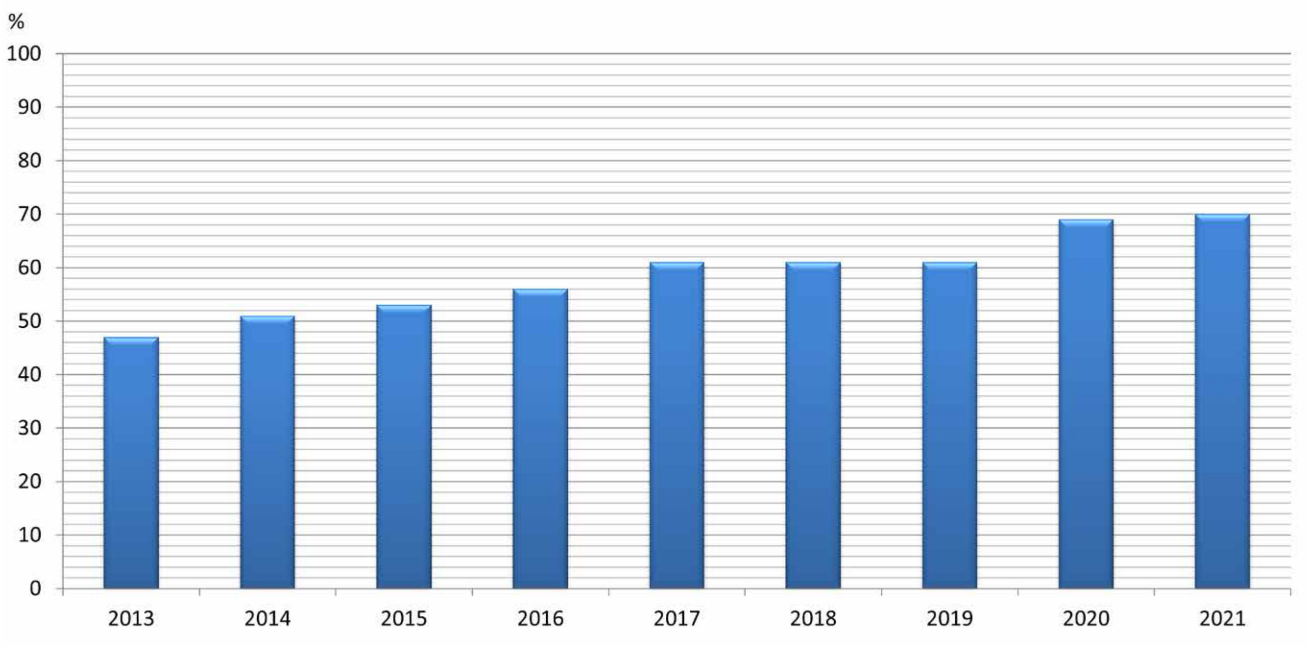
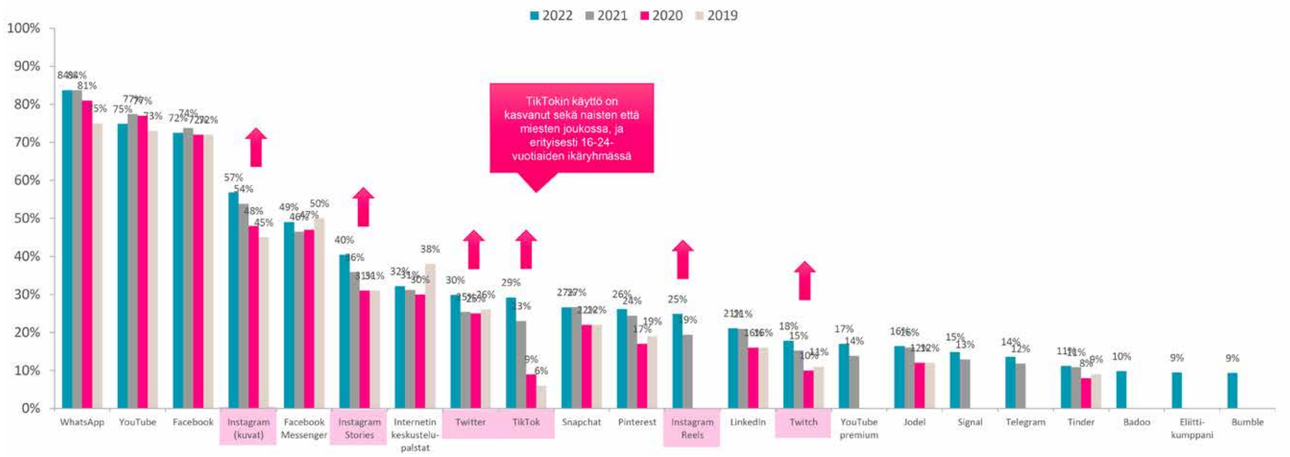


Figure: Social media usage 2013-2021, source: SVT, image: HP

The covid pandemic led to a significant increase in the use of several social media services. Between 2020 and 2022, the biggest increases were in Instagram, TikTok, WhatsApp and Twitter (DNA, 2022). Both social services and messaging apps appear to have been affected by the pandemic. During the period of covid restrictions, people were unable to meet each other normally, putting more emphasis on connecting through social media. Covid itself was also a major topic of news and discussion on social media.



TikTokin käyttö on kasvanut sekä naisten että miesten joukossa, ja erityisesti 16-24-vuotiaiden ikäryhmässä

Figure: Use of social media services in Finland, 2019-2022, DNA 2022a

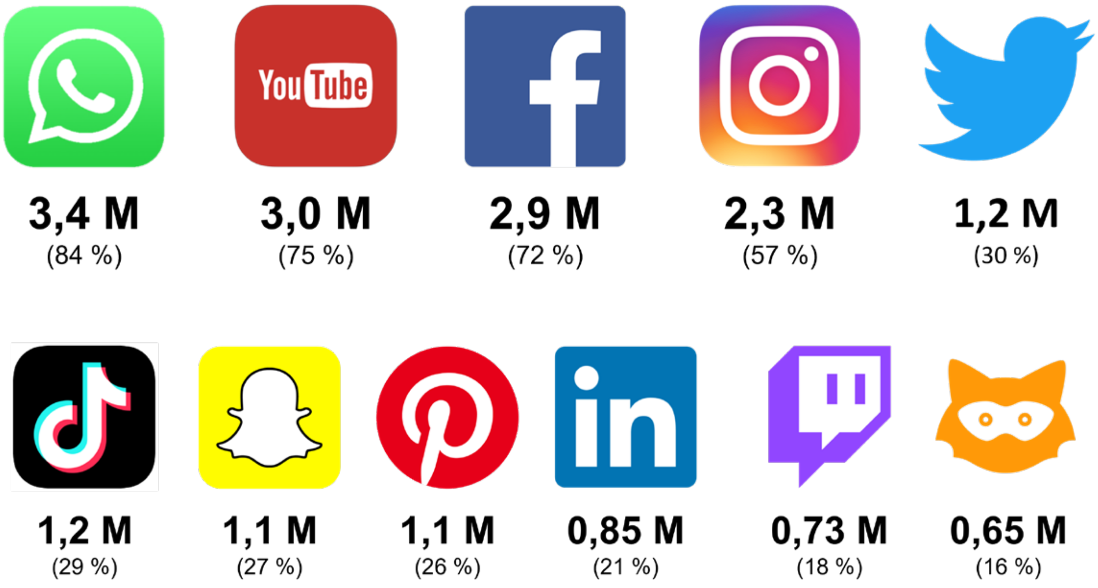


Figure: Finnish users of social media services, DNA 2022a, image: HP

An interesting detail is that Facebook usage in Finland had turned down before the pandemic in 2019-2020. However, Finns' enthusiasm for Facebook was renewed after the outbreak of the pandemic, which boosted usage, especially among people over 30.

While Facebook use continues to decline among young people, overall Facebook use rebounded with the pandemic. As covid restrictions ease, it is expected that Facebook usage will fall again.

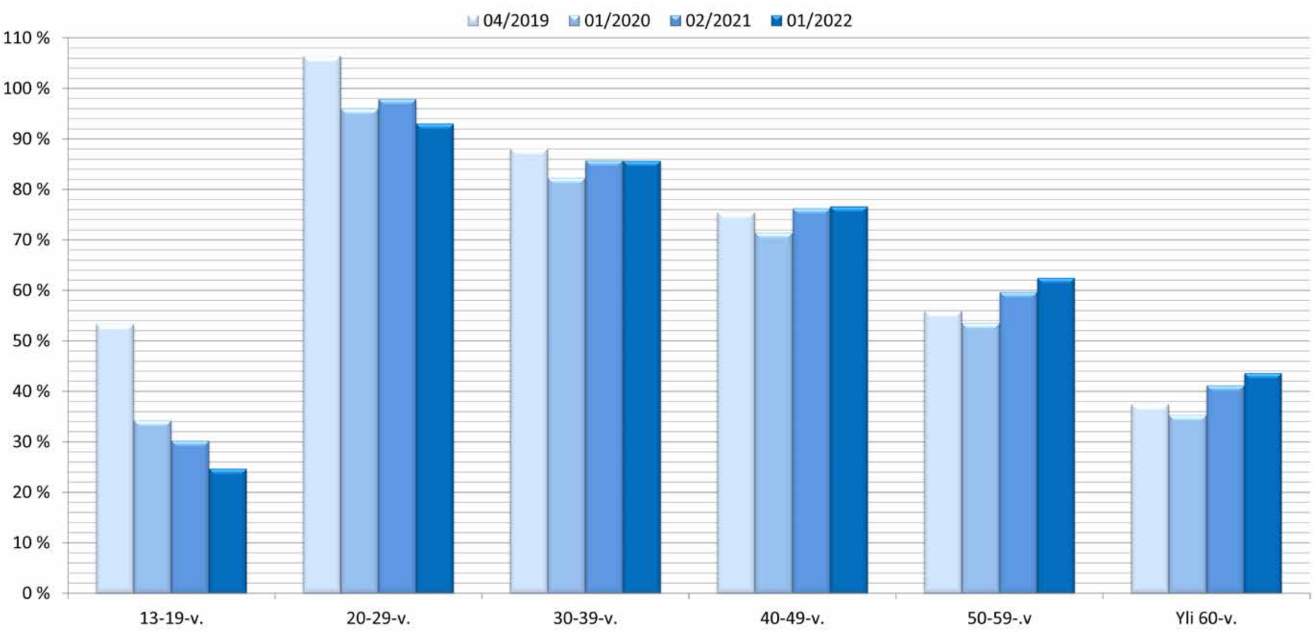


Figure: The number of Facebook users in Finland as reported by Meta's advertising engine on 14 April 2019, 9 January 2020, 25 February 2021 and 15 January 2022 relative to the Finnish population in the same age groups, source: Meta and SVT, image: HP

The war in Ukraine is visible on social media

Alongside covid, social media usage has been boosted by the war in Ukraine. In a DNA survey (2022a), a quarter of respondents said the world situation had increased their use of social media and messaging apps. Half also said they follow the news more than before, which can be expected to be particularly reflected in their use of Facebook.

The debate surrounding the war in Ukraine and Finland's NATO membership has been clearly reflected in the increased use of Twitter. A new record in the number of monthly Twitter users was seen in March 2022. According to the Pinnalla-counter[1], there were 183 000 active Finnish usernames on Twitter, meaning that they had tweeted at least once.

Social media users estimate that covid and the war in Ukraine are also reflected in an increased in the number of scam messages and calls. In a DNA survey, 37% of respondents reported an increase in scam messages and calls. In a survey commissioned by the News Media Association, as many as 75% of respondents believed that deliberately misleading information would increase between 2022 and 2023. Only 38% of respondents believed that other Finns are able to distinguish outside influence. The need for digital information literacy is growing increasingly important with the use of social media.

Young people's use of the social media and new favourites

The popularity of social media services is changing rapidly among young people. The number of young users has declined on many of the social media services that were previously considered favourites. The tendency towards a middle-aged user base, previously seen on Facebook, now seems to be spreading to other social media services. Daily activity among 16-24 year olds has fallen by 10 percentage points per year on YouTube, Instagram and Twitter (DNA, 2022). It seems that as the older user groups grow, young people are moving to other services.

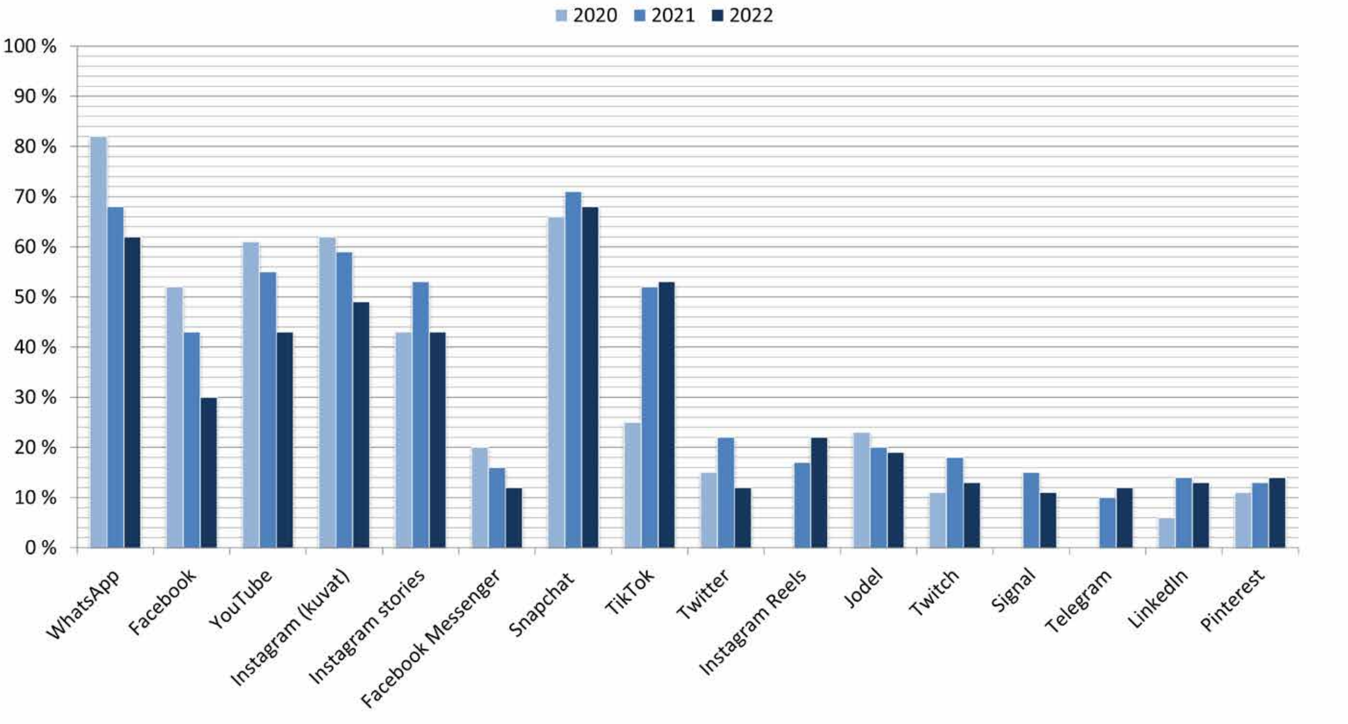


Figure: The daily use of social media services, 16-24-year old, DNA, 2022a, image: HP

Of the social media services favoured by young people, TikTok has grown fastest in recent years. Only three years ago, TikTok was becoming more common, with 9% of respondents aged 13-29 using it, according to the Social media and Young People survey (2019). In a similar survey this year, the figure was 57%. Short videos seem to be the most effective way of communicating with young people at the moment.

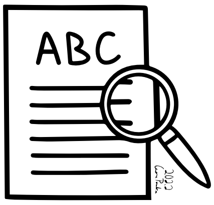
Looking back over the last year, alongside TikTok, Instagram Reels have increased in popularity. It was originally seen as a cheap copy of TikTok by Meta, but as part of Instagram it has found its place as a platform for publishing short videos. Reels now have a daily usage rate of 22% among 16-24-year olds (DNA, 2022a).

Of the messaging services, Snapchat is the most actively used by young people, with 68 % saying they use it daily. WhatsApp is on the decline, but it is still the second most popular messaging service for young people with 62% daily usage. Up to 37% said they had reduced their use of WhatsApp, which predicts a continued decline in its use.

The use of Facebook Messenger and Signal are also declining among young people. Telegram, on the other hand, is on the rise, but its daily usage among 16-24-year olds is still at a moderate 12%. Telegram's growth is driven, among other things, by its numerous open channels focusing on news. Telegram channels, like Facebook groups, are also known to spread disinformation about Covid and the war in Ukraine.

AudienceProject, 2020, App & social media usage, https://www.audienceproject.com/resources/insight-studies/app-social-media-usage-2/
DNA, 2021, Digitaaliset elämäntavat -tutkimus, https://www.sttinfo.fi/data/attachments/00200/838ead53-d63a-4f2a-9d3e-db3845973aec.pdf
DNA, 2022a, Digitaaliset elämäntavat -tutkimus, https://www.dna.fi/documents/753910/11433306/Digitaaliset_elamantavat_tutkimusraportti_2022.pdf
DNA, 2022b, Koululaistutkimus, https://corporate.dna.fi/documents/753910/11433306/DNA+Koululaistutkimus+2022.pdf/45cbcfcd-0308-be26-d7c5-a6f32a6a02d8?t=1649764482372
Ebrand Group Oy & Oulun kaupungin sivistys- ja kulttuuripalvelut, 2022, Suomessa asuvien 13-29 -vuotiaiden nuorten sosiaalisen median palveluiden käyttäminen ja läsnäolo, https://wordpress.ebrand.fi/somejanuoret2022/
Ebrand Group Oy & Oulun kaupungin sivistys- ja kulttuuripalvelut, 2019, Suomessa asuvien 13-29 -vuotiaiden nuorten sosiaalisen median palveluiden käyttäminen ja läsnäolo, https://wordpress.ebrand.fi/somejanuoret2019/2-suosituimmat-sosiaalisen-median-palvelut/
Pinnalla-laskuri, 2022, Twitterin aktiiviset käyttäjätunnukset Suomessa maaliskuussa 2022, https://pinnalla.pyppe.fi/haku?q=&t=2022-03-01T00%2C2022-04-01T00
Pönkä, H., 2014, Sosiaalisen median käsikirja
Pönkä, H., 2022, Sosiaalisen median tilastot ja käyttö Suomessa: somekatsaus 07/2022, https://www.innowise.fi/fi/sosiaalisen-median-kaytto-suomessa-somekatsaus-07-2022/
Reunanen, E., Alanne, N., Helske, H., Lappalainen, E., Niemi, M. K., Pettersson, M., & Seuri, V., 2022, Uutismedia verkossa 2022.
Reuters-instituutin Digital News Report - Suomen maaraportti, https://trepo.tuni.fi/handle/10024/140958
Reuters Institute for the Study of Journalism, 2022, Digital News Report 2022, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2022-06/Digital_News-Report_2022.pdf
Suomen virallinen tilasto (SVT), 2013-2021, Väestön tieto- ja viestintätekniikan käyttö, https://www.stat.fi/til/sutivi/
Uutismedian liitto, 2022, Kolme neljästä suomalaisesta uskoo tietoisesti harhaanjohtavan tiedon määrän lisääntyvän, https://www.uutismediat.fi/wp-content/uploads/2022/05/vaikuttamispyrkimykset-mediatiedote-liitteet_Uutismedian-liitto_toukokuu-2022.pdf

5. Online inquiry requires criticality



CARITA KIILI, CRITICAL-PROJECT, TAMPERE UNIVERSITY

The internet is seen as an up-to-date repository of information, where the information one needs is just a Google search away. The internet is an essential resource for formal and informal learning. It is also used to search for information to support decision-making in various settings, whether it is about buying a new phone or making a health-related decision. When the readers' goal is to understand a complex phenomenon, examine a controversial issue from different perspectives, or make an important decision, the information is no longer a Google search away. Achieving a deep understanding of the issue under examination requires complex processing, as well as the monitoring and regulation of these processes (Kiili et al., 2009).

Online inquiry is a cyclical process

The complex and cyclic process of online inquiry is illustrated in Figure below (cf. Leu et al., 2019; see also Kiili et al., 2021). Notably, the depicted process is ideal and does not necessarily apply to all situations and for all readers. Online inquiry begins with specifying the information needed: the kind of information a reader needs to solve a problem or reach a deep understanding of the phenomenon at hand. In specifying the information needs, readers can also consider sources that would provide credible information. Specifying the information needs is crucial, as it guides online reading processes and the monitoring and regulation of these processes. It is worth mentioning that although specifying the information need initiates online inquiry, it can also become more specific or even change during the inquiry.

Once the information need has been specified, readers can search for information using search engines. To formulate effective search queries, readers consider core concepts and limiting concepts that can relate to content or sources (e.g., organization, profession). Readers analyze search results by using a title, a website address, or an example text. Which search results could meet the information need and lead to credible information? If the search results do not seem promising, readers are required to revise their search queries. Skillful readers can modify their searches by considering alternative expressions, concepts, and sources.

After locating relevant online texts, readers can evaluate them more carefully. If the texts seem credible, readers move on to interpreting single texts and comparing multiple texts. If the information need is not met (texts are not relevant or credible, or some important point of view is missing), the reader returns to the information search phase.

A synthesis—an integrated mental model of online texts (cf. Rouet, 2006) — is gradually constructed during the iterative process of inquiry. In school assignments, students are often asked to produce a written or multimodal product based on multiple online texts that reflect the synthesis. In the synthesis, readers integrate ideas from multiple texts into a coherent whole. The synthesis also includes information about the sources, such as, Who said what? How do different sources support or contradict each other? Readers can use the synthesis, for example, in decision-making or participation in a societal discussion.

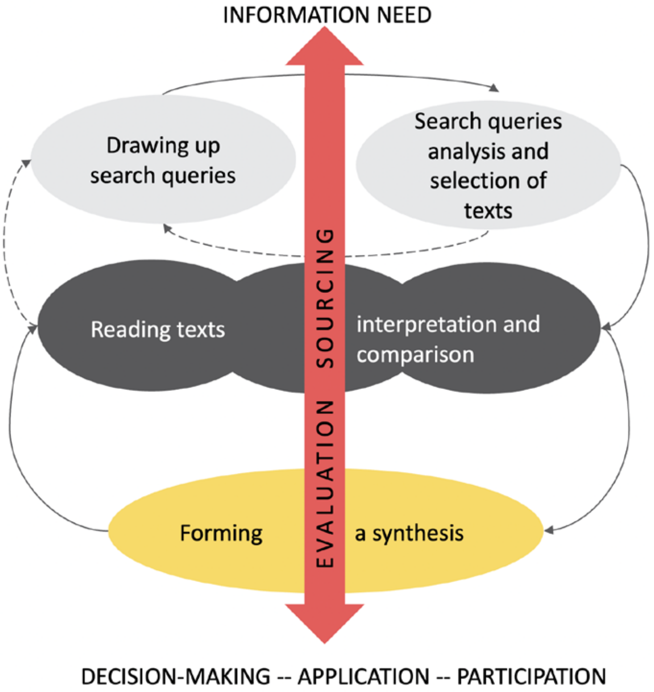

INFORMATION NEED
Drawing up search queries
Search queries analysis and selection of texts
Reading texts
interpretation and comparison
SOURCING
EVALUATION
Forming
a synthesis
DECISION-MAKING -- APPLICATION -- PARTICIPATION

Figure: The iterative processes of online inquiry where information evaluation and sourcing are cross-cutting processes

Online inquiry requires criticality

Online inquiry requires critical reading skills. Critical reading refers to an individual's ability to analyze, evaluate, and interpret information of varying quality and recognize how different texts can be used to persuade or mislead (see Critical, 2021). Credibility evaluation and sourcing are cross-cutting processes in critical online reading (Figure), which I will next explore in more detail.

Credibility evaluation during online inquiry

Credibility evaluation can occur while searching for information, reading online texts, and synthesizing them. In the search phase, credibility evaluation is predictive, as the search results provide only a limited amount of information to support evaluation. Predictive evaluation becomes more precise when readers can examine online texts in more detail and compare the content of multiple online texts. According to Barzilai et al. (2020), credibility evaluation is a bi-directional process in which readers evaluate the content's validity and the source's trustworthiness (e.g., author, publisher). Readers' judgments about content validity are reflected in the evaluation of the source's trustworthiness, and judgments about the source's trustworthiness are reflected in the content validation.

Credibility evaluation aims to determine whether the text content is accurate. Readers can evaluate the content by a) comparing the content with their prior knowledge and beliefs about the topic, b) examining the quality of argumentation, and c) validating the accuracy of the content against the other texts (Barzilai et al., 2020). However, if readers do not have much prior knowledge or if their prior beliefs are incorrect, validating content against prior knowledge and beliefs can be difficult or even harmful. Namely, the stronger readers' misconceptions about the text topic are, the more inclined they are to judge the text that supports their misconceptions as credible (Kiili et al., under review; van Strien et al., 2016).

Readers can also evaluate the author's argumentation from different perspectives: What kinds of rhetorical means does the author use? Is argumentation logical? What does the author argue, and how does he or she support the argument? For example, readers can consider the credibility of the provided evidence. Is the author relying only on personal experiences, or does the author present research evidence to support the claims? Our research shows that students need support to understand what kind of evidence can be regarded as credible when determining cause–effect relationships. For example, only about a quarter of the sixth graders (N = 265) perceived that personal experience could not prove a cause–effect relationship (Kiili et al., 2022b). Many upper secondary school students also struggled to justify why one should be cautious when personal experience is presented as evidence of a causal claim (Kiili et al., 2022a).

Content validity can also be examined by comparing the content of several texts, a strategy called corroboration. Ideally, readers will use several texts to determine the prevailing scientific understanding of the explored issue (Osborne et al., 2022). When we studied credibility evaluation of online texts among more than three hundred upper secondary students, corroboration was the least used evaluation strategy (Hämäläinen et al., 2021). In their evaluations, students paid the most attention to the publication venue. While 89% of students considered the publication venue at least once when evaluating three online texts, the corresponding proportion was 14% for corroboration.

Evaluation of the source (e.g., author, publication venue) is particularly important when readers have little or no prior knowledge of the topic under examination (Bråten et al., 2018a). When evaluating a source, readers can consider several source features, such as the author's expertise, benevolence, and integrity (Hendriks et al., 2015). Readers can draw conclusions about the author's expertise by paying attention to the author's education, profession, position, or affiliation. Notably, it is not sufficient to quickly check credentials. Readers should consider whether the author has expertise, particularly in the topic of the text (Osborne et al., 2022). This should be discussed in classrooms because, in social media, for example, experts from different fields present statements on topics that are not at the core of their expertise. In our study, where we examined pre-service teachers' (N = 169) credibility evaluation skills, we found that only 8–20% (depending on the text) of them considered the relationship between the author's expertise and the topic of the text (Kulju et al., in preparation).

In addition to the author's expertise, readers may also consider the author's or publisher's intentions and integrity. For example, readers can consider whether the author has commercial or political intentions. For younger readers, identifying commercial intentions is not self-evident, even if they are obvious (e.g., company websites). When 63% of the sixth graders identified commercial intentions in a multiple-choice task (Kiili et al., 2022b), only 19% of them questioned the credibility of a commercial web page when they were required to justify their credibility evaluation in an open-ended task (Kiili et al., 2018).

In Table below, I have compiled examples of content- and source-based justifications that upper secondary school students gave for their credibility evaluations. Notably, justifications can include both content- and source-related considerations. For instance, in the last example, a student identifies commercial intentions (source) and considers how these intentions are reflected in the author's argumentation (content). In addition, the student seems to be aware of the legislation that protects consumers, stating that marketing must also be in accordance with good practice.

CONTENT EVALUATION

COMPARISON WITH PREVIOUS PERCEPTION (Hämäläinen ym, 2021)
The text is opinion-based, and everyone has their own opinion on the matter. However, I am of the same opinion as the author of this text.

QUALITY OF EVIDENCE (Kiili ym. 2022)
The author justifies his claim with his observation after the birthday, without knowing about the events of the birthday or other factors that could have influenced the daughter's behaviour (layman's blog, evidence of a single observation).

CONFIRMATION (Hämäläinen ym, 2021)
I have also read the same things on the THL website.

SOURCE EVALUATION

THE EXPERTISE OF THE AUTHOR (Kiili ym. 2022)
The author is a doctor of health sciences who has conducted research on the subject. He also has knowledge of studies and findings by others (research-based text).

THE AUTHOR'S INTENTIONS (Kiili ym. 2022)
The author wants to improve the sales of the company, so he does not talk about sugar in a negative way, even though it has negative effects. Of course, if the information is untrue, the company could get into trouble, so the author tries to avoid that. (commercial text)

([1]Hämäläinen et. al., 2021; [2]Kiili et. al., 2022)

Table: Examples of upper secondary school students' justifications for their credibility evaluations when reading health-related texts.

Sourcing during online inquiry

The evaluation of the trustworthiness of sources is an integral part of sourcing. However, sourcing is a broader construct than source evaluation and is defined as paying attention to, evaluating, presenting, and using sources of information (Bråten et al., 2018b). Importantly, sourcing can occur throughout online inquiry, and it is an essential part of critical online reading (Kiili et al., 2021). When specifying their information needs, readers can consider which sources could provide credible information on the topic under examination. Readers can then use these considerations to formulate their search queries by including trustworthy persons, organizations, or professions in their search queries. For example, if readers want to know what monkeypox is and how it spreads, they can limit their search to the CDC website (Centers for Disease Control and Prevention) by typing in Google "monkeypox site: cdc.gov". If readers do not know any specific publication venue, they can also limit their search by profession, such as "professor," to increase the probability of finding research-based information about monkeypox.

Sourcing is also an essential part of interpreting, comparing, and synthesizing multiple online texts. Sourcing plays a pivotal role, particularly when readers explore controversial issues (Rouet, 2006). Namely, skillful readers pay attention to who says what, which is forming source–content links. When readers consider how the views of different sources support or oppose each other, they form source–source links. When readers compose a source-based essay, sourcing is not just a matter of compiling a list of sources. At its best, a written product provides information on the views of different sources and their relationships.

Our study showed that upper secondary school students engaged in sourcing throughout the online inquiry (Kiili et al., 2021). However, sourcing was relatively scarce in search querying. Interestingly, sourcing in the earlier phases of inquiry contributed to sourcing in the later phases of inquiry. The more frequently upper secondary students (N = 167) engaged in sourcing when specifying their information needs or formulating their search queries, the more frequently they also engaged in sourcing in their credibility judgments. Further, the more frequently students engaged in sourcing in their credibility judgments, the more frequently they used sources in their writing. These findings suggest that instruction should emphasize sourcing as a continuous process that begins early on.

The CRITICAL project aims to support children's and adolescents' critical reading

In this article, I have described how criticality may ideally appear during online inquiry. However, our research among adolescents in Finland shows considerable inter-individual differences in adolescents' online inquiry skills and criticality. While some students need support with basic skills, others need more challenges to further develop as critical online readers. In the CRITICAL project, funded by the Strategic Research Council, we investigate children's and adolescents' critical reading skills, including supporting and hindering factors for development. In addition, we develop research-based methods and materials to support critical reading in classrooms (see educritical.fi/en).

TAVOITTEENA KRIITTINEN LUKIJA •
CR

educritical.fi
Twitter: @EduCritical | Facebook: Critical-hanke

References

Barzilai, S., Thomm, E., & Shlomi-Elooz, T. (2020). Dealing with disagreement: The roles of topic familiarity and disagreement explanation in evaluation of conflicting expert claims and sources. Learning and Instruction, 69, Article 101367. https://doi.org/10.1016/j.learninstruc.2020.101367

Bråten, I., McCrudden, M. T., Stang Lund, E., Brante, E. W., & Strømsø, H. I. (2018a). Task-oriented learning with multiple documents. Effects of topic familiarity, author expertise, and content relevance on document selection, processing, and use. Reading Research Quarterly, 53(3), 345–365. https://doi.org/10.1002/rrq.197

Bråten, I., Stadtler, M., & Salmerón, L. (2018b). The role of sourcing in discourse comprehension. In M. F. Schober, D. N. Rapp, & M. A. Britt (Eds.), Routledge handbooks in linguistics. The Routledge handbook of discourse processes (pp. 141–166). Routledge/Taylor & Francis.

Critical. (2021). Teknologisia ja sosiaalisia innovaatioita kriittisen lukemisen tukemiseen internetin aikakaudella (CRITICAL): Tilannekuvaraportti 2021. https://www.aka.fi/globalassets/3-stn/1-strateginen-tutkimus/strateginen-tutkimus-pahkinankuoressa/tilannekuvaraportit/stn2020-hankkeet/tilannekuvaraportti-critical.pdf

Hendriks, F., Kienhues, D., & Bromme, R. (2015). Measuring laypeople's trust in experts in a digital age: The Muenster Epistemic Trustworthiness Inventory (METI). PLoS ONE, 10(10), e0139309. https://doi.org/10.1371/journal.pone.0139309

Hämäläinen, E., Kiili, C., Räikkönen, E., & Marttunen, M. (2021). Students' abilities to evaluate the credibility of online texts: The role of Internet-specific epistemic justifications. Journal of Computer Assisted Learning, 37(5) 1409–1422. https://doi.org/10.1111/jcal.12580

Kiili, C., Bråten, I., Strømsø, H., Hagerman, M.S. Räikkönen, E. & Jyrkiäinen, A. (2022a). Adolescents' credibility justifications when evaluating online texts. Education and Information Technologies. https://doi.org/10.1007/s10639-022-10907-x

Kiili, C., Bråten, I., Strømsø, H., & Räikkönen, E. (2022b). Why trust or mistrust? Sixth graders' ability to justify the credibility of online texts. Hyväksytty esitelmä EARLI SIG2, 29.8-31.8.2022, Kiel, Saksa

Kiili, C., Forzani, E., Brante, E. W., Räikkönen, E., & Marttunen, M. (2021). Sourcing on the Internet: Examining the relations among different phases of online inquiry. Computers and Education Open, 2. Article 100037. https://doi.org/10.1016/j.caeo.2021.100037

Kiili, C., Laurinen, L., & Marttunen, M. (2009). Skillful Internet reader is metacognitively competent. In L. T. W Hin & R. Subramaniam (Eds.), Handbook of research on new media literacy at the K-12 level: Issues and challenges (pp. 654–668). Hershey, PA: IGI Global.

Kiili, C., Leu, D. J., Marttunen, M., Hautala, J., & Leppänen, P. H. T. (2018). Exploring early adolescents' evaluation of academic and commercial online resources related to health. Reading and Writing, 31, 533–557. https://doi.org/10.1007/s11145-017-9797-2

Kiili, C., Räikkönen, E., Bråten, I., Strømsø, H. I. & Hagerman, M. S. (underm review). Adolescent readers' online evaluation skills are made of abilities to confirm the credibility and question the credibility.

Kulju, P., Hämäläinen, E., Mäkinen, M., Räikkönen,E., & Kiili, C. (in preparation). Pre-service teachers evaluating online texts about learning styles: There is room for improvement in justifying the credibility.

Leu, D. J., Kinzer, C. K., Coiro, J., Castek, J., & Henry, L. A. (2019). New literacies: A dual level theory of the changing nature of literacy, instruction, and assessment. In D. E. Alvermann, N. J. Unrau, M. Sailors, & R. B. Ruddell (Eds.), Theoretical models and processes of literacy (7th ed., pp. 319– 346). Taylor & Francis.

Osborne, J., Pimentel, D., Alberts, B., Allchin, D., Barzilai, S., Bergstrom, C., Coffey, J., Donovan, B., Kivinen, K., Kozyreva. A., & Wineburg, S. (2022). Science education in an age of misinformation. Stanford University, Stanford, CA

van Strien, J. L. H., Kammerer, Y., Brand-Gruwel, S., & Boshuizen, H. P. A. (2016). How attitude strength biases information processing and evaluation on the web. Computers in Human Behavior, 60, 245–252. https://doi.org/10.1016/j.chb.2016.02.057

6. Online reading skills & strategies

KARI KIVINEN, FAKTABAARI EDU

The health of a democracy depends on people's ability to access reliable information.

Hobbs, 2010; Mihailidis & Thevenin, 2013.[1]

Online vs. offline environments

According to Koryzeva et al (2020) in an excellent article "Citizens versus the internet"[2], online environments are replete with smart, highly adaptive choice architectures, designed primarily to maximise commercial interests, capture and sustain the users' attention, monetise user data, and predict & influence future behaviour. In the worst case scenario this can facilitate the spread of disinformation.

Online and offline environments differ from each other in ways that have important consequences for people's online experiences and behaviour. In the online environment, one can broadcast a message to an audience of millions, whereas in face-to-face communication, there are physical limits to how many people can join a conversation[3].

Online environments are often designed to

- **maximise commercial interests,**
- **capture and sustain users' attention,**
- **monetise user data, and**
- **predict and influence future behaviour.**

Kozyreva et al (2020)

The amount of information available to anybody in digital environments is breathtaking and it is possible to diffuse any information effortlessly to vast audiences in no time. Online environments develop rapidly and constantly compared with most offline environments. Contents can be changed, removed and added all the time.

Kozyreva et al. identified four types of challenges typical to online environments: persuasive and manipulative choice architectures, AI-assisted information architectures, false and misleading information, and distracting environments. When people are accessing online information through search engines, their results are regulated by algorithms developed by corporations "in pursuit of profits and with little transparency or public oversight" In addition, "in democratic countries technology companies have accumulated unprecedented resources, market advantages, and control over people's data and access to information"[4]. The collection of data from online users is based on highly developed machine-learning systems and algorithms which outperform us humans and which are not transparent. That's why the results of the search engines and recommender system used for instance by Youtube are individualised and unpredictable.

One solution to this challenge is education. According to researchers, interventions directed to the public as recipients and producers of information, namely in the school curricula for digital-information literacy, would teach students how to search, filter, evaluate, and manage data, information, and digital content[5]. For all these reasons, traditional reading skills should be complemented by new types of online evaluation strategies and online reading skills.

Faktabaari EDU[6] has been promoting information literacy for Finnish teachers and students in line with the Finnish core curricula goals and objectives (informaatiolukutaito-opas)[7]. Because the online scene is developing so fast, we are obliged to update the information literacy guide book published in 2020 with this digital information literacy guidebook. We have added new tools to the digital information literacy toolbox.

Online reading toolbox

It should be noted that good digital literacy skills alone are not enough. Good subject-matter knowledge can make us better at assessing the credibility of information[8]. If you have a good understanding of a certain topic, it is harder for you to be misled. With the understanding of climate change providing a good test case which shows that if one has good knowledge about a certain topic, then it is harder to get misled[9]. However, general higher education may not make you much better at navigating disinformation[10].

The ability to find credible information online is necessary for informed civic engagement – it is a new citizenship skill. This need is particularly acute for young people, who often turn to the internet to learn about social and political issues. Preparing students to evaluate online content, particularly as it concerns social and political issues, aligns with broader efforts to reinvigorate the civic mission of colleges and universities. According to a recent study[11], the majority of students employed ineffective strategies for evaluating digital information. Therefore, it is extremely timely and important to promote online reading skills and online evaluation strategies.

Pre-bunking

Pre-bunking is the name for a process where people are warned in advance that they are about to be the target of false information. Pre-bunking skills can be promoted by providing people with factual and some in-depth information on a particular subject beforehand, and then introducing the existing disinformation about the same subject. They can also be told in advance what kinds of disinformation they can expect.

A good pre-bunk addresses people's concerns, speaks to their lived experience and compels them to share that knowledge. Prebunks are empowering: The whole point is about building trust with your audience instead of simply correcting facts. Research has shown that the logic-based approach has far-reaching benefits. If you teach people to recognize tactics, they can spot them more often than individual claims[12].

There are three main types of prebunks:

1. **fact-based: correcting a specific false claim or narrative**
2. **logic-based: explaining tactics used to manipulate**
3. **source-based: pointing out bad sources of information**

Debunking

Debunking takes place after the false information has appeared. The aim is to correct false information and to prevent others from believing what is verifiably false information. Fact checking strategies can be used to debunk misinformation and disinformation.

Correcting or "disproving" false information is challenging because people are more likely to believe familiar information even if they later learn that the information is incorrect (the familiarity backfire effect).

Research shows that when correcting misinformation, it is best to present key facts before presenting the misinformation to be corrected. It is not enough to correct the misinformation. It is necessary to explain why the information is wrong and to provide a truthful counterpart or explanation. The Debunking Handbook[13] identifies four key areas of myth debunking:

1. Key facts: emphasise what is true rather than what is false. Research shows that when debunking misinformation, it is best to present the core fact first before presenting the misinformation that needs to be debunked.
2. Clear warnings.
3. Alternative explanation: 'When you refute a myth, you create a hole in the human mind. To be effective, your refutation must fill this gap". If you want to replace incorrect information, provide a clear explanation that fills the "information gap". Try to explain things as clearly as possible: people may stop paying attention if they are confronted with overlapping information. This can sometimes mean leaving out some nuances when people are first presented with corrected information.
4. Graphics: visual presentations can help to illustrate key facts more clearly.

Sourcing

Sourcing in text comprehension has been found to have a significant effect on students' abilities to determine credibility and evaluate information, effect sizes ranging from small to large[14]. Knowing where good information is, source trustworthiness, may be as important as source criticism in order to be a well-informed citizen[15]. Therefore, it is important to share where reliable information can be found and who can be trusted.

Civic online reasoning

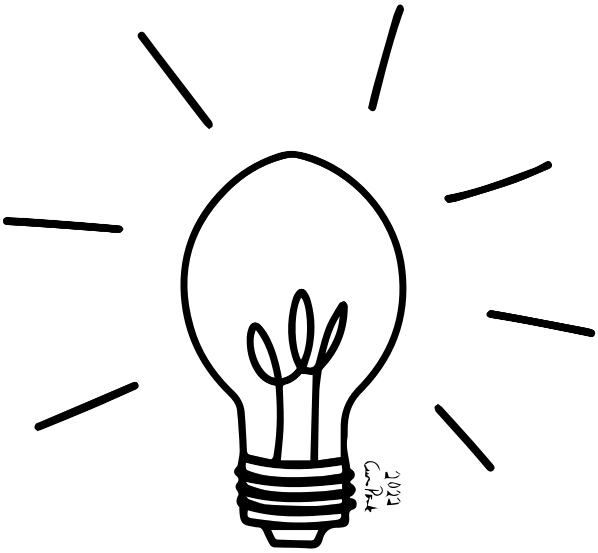
Teaching **civic online reasoning**[16] has proved to be a more challenging task. Researchers at Stanford[17] [18] propose that when one comes across online information, one should ask oneself three key questions:

1. Who's behind the information?
2. What's the evidence? and
3. What do other sources say?

Research on curricular activity to promote civic online reasoning have been effective in advancing individuals in digital source criticism and lateral reading[19].

Teaching young people **how to use cognitive strategies and digital tools** to verify information, has also been shown to have medium size effects on their ability to distinguish between credible and misleading information[20]. Especially those teenagers who, after the self-test or teaching, used digital tools, such as text searches or reverse image search, managed to debunk misleading news.

The attention span of any information seeker is limited and search engines often find a huge number of hits. We do not have the time or the energy to analyse all the results to find the information that is important to us. It is therefore wise to focus our limited attention on the essential information. To do that, we need the skill of strategic ignorance.



Strategic ignorance

When using powerful search engines, we sometimes get millions of hits. How to select information which is useful, truthful and which meets our initial information need? In this process we need human critical thinking to evaluate the value of the content algorithms are proposing for us – and we have put aside and ignore, most of the hits.

Already in 1971 – far before the time of the Internet – Herbert Simon[21] noted that information overload results in a scarcity of attention. Advertisers, corporations, lobbyists, clickbait sites, conspiracy theorists, hate groups, and propaganda-fuelling governments work overtime to hijack our online attention. Often the wisest thing to do is to preserve attention by practising strategic ignoring. Under conditions of limited attention[22], the most crucial decision to make is where to allocate it.

So, we must develop skills to ignore great amounts of non-important information. We should embrace strategic ignoring to avoid disinformation and to preserve our limited amount of attention on content which is really worth reading.

Lateral reading

Lateral reading

The reader checks the background of the online information (author's credibility, facts, statistics, sources, etc.) on various sites and sources before reading the text at hand.

One of the new tools in the digital information literacy toolbox is the lateral reading approach in which the reader verifies the background of the online information (reliability of the source, facts, stats, sources) from different sites and sources before starting to read the text at hand.

Due to the differences between the online and offline information environments, it is necessary to pay more attention to the source of the online information. The traditional reading approach can be ineffective in a digital environment. If we are too busy to analyse unfamiliar online information without checking the origin of the article in the first place – we might not necessarily notice that the whole text is based on biased information.

Wineburg & McGrew (2019)[23] observed how students, academics and fact-checkers deal with previously unknown online information. Fact-checkers opened up several tabs across the horizontal axis of their browser and searched for information about the organisation or individual behind it. Only after verifying what other sites had to say, they returned to the text. Using this approach, fact checkers were able to quickly verify sites that masked their intent and sponsors. In the same experiment students and academics were focused on the original site, resulting in confusion about its real agenda or sponsor.

The strategy used by professional fact-checkers to read online feeds laterally across many connected sites instead of digging deep into the text at hand has proven to be a quick and effective way to avoid spending attention, time and energy on biased information. The use of the **click restraint strategy** is recommended. It means that one should carefully scroll down before clicking links in search results that are relevant and not necessarily ranked as the top result and **take bearing towards reliable sources** of information[24]. Reading of multiple, relevant sources in order to be able to corroborate and contextualise the information enables us to make well-informed judgments about the trustworthiness of the source.

Online traffic rules

In July 2022, the European Parliament adopted the Digital Services Act (DSA)[25] and Digital Markets Act (DMA)[26]. These new EU digital rulebooks set out unprecedented standards on the accountability of online companies, within an open and competitive digital market. Once the new rules are implemented in practice, users in the EU will have more choices and their rights will be better protected online.
It would be beneficial if the big online platforms would start to regulate their content more carefully in the future as foreseen by these Acts. But unfortunately, we cannot count on the good will of the platforms. We need to improve our digital skills and educational input! Citizens should be taught to develop their critical thinking and digital information literacy skills.

Simple online traffic rules would be useful for us all. When I was at school, I was taught simple traffic instructions: First, look to left – and then to right – and to left again before crossing the street. We need similar clear instructions also for online environments.

When confronted with unknown online content, it is always useful to find answers to these three simple key questions before spending time in exploring the content more closely:

- **Who's behind the information? Source?**
- **What's the evidence?**
- **What do other sources say?**

It would be useful to reserve our limited attention to texts worth reading!

[1] *Hobbs, R. (2010). Digital and media literacy: A plan of action. The Aspen Institute.* https://assets.aspeninstitute.org/content/uploads/2010/11/Digital_and_Media_Literacy.pdf
Mihailidis, P., & Thevenin, B. (2013). Media literacy as a core competency for engaged citizenship in participatory democracy. American Behavioral Scientist, 57(11), 1611–1622. https://doi.org/10.1177/0002764213489015

[2] Kozyreva, A., Lewandowsky, S. and Hertwig, R. (2020). Citizens Versus the Internet: Confronting Digital Challenges With Cognitive Tools. Association for Psychological Science. SAGE

[3] Barasch, A., & Berger, J. (2014). Broadcasting and narrowcasting: How audience size affects what people share. Journal of Marketing Research, 51, 286–299. https://doi.org/10.1509/jmr.13.0238

[4] Zuboff, S. (2019). The age of surveillance capitalism: The fight for the future at the new frontier of power. Profile Book

[5] Breakstone, J., McGrew, S., Smith, M., Ortega, T., & Wineburg, S. (2018). Teaching students to navigate the online landscape. Social Education, 82, 219–221.

[6] Faktabaari EDU https://faktabaari.fi/

[7] Kivinen, K. (Ed. 2020) Informaatiolukutaito-opas. Faktabaari. https://faktabaari.fi/assets/Informaatiolukutaito-opas_Faktabaari_EDU.pdf

[8] Lurie, E., & Mustafaraj, E. (2018, May). Investigating the Effects of Google's Search Engine Result Page in Evaluating the Credibility of Online News Sources. *In Proceedings of the 10th ACM Conference on Web Science* (pp. 107-116)

[9] Nygren, T., & Guath, M. (2021a). Students evaluating and corroborating digital news. *Scandinavian Journal of Educational Research, in press.*

[10] Roozenbeek, J., van der Linden, S., & Nygren, T. (2020). Prebunking interventions based on "inoculation" theory can reduce susceptibility to misinformation across cultures. *Harvard Kennedy School Misinformation Review, 1(2).*

[11] Joel Breakstone, Mark Smith, Nadav Ziv & Sam Wineburg (2022) Civic Preparation for the Digital Age: How College Students Evaluate Online Sources about Social and Political Issues, The Journal of Higher Education, DOI: 10.1080/00221546.2022.2082783

[12] First Draft https://firstdraftnews.org/articles/a-guide-to-prebunking-a-promising-way-to-inoculate-against-misinformation/

[13] Debunking Handbook (2020) https://www.climatechangecommunication.org/wp-content/uploads/2020/10/DebunkingHandbook2020.pdf

[14] Brante, E. W., & Strømsø, H. I. (2018). Sourcing in Text Comprehension: a Review of Interventions Targeting Sourcing Skills. *Educational Psychology Review*, 30(3), 773-799. doi:10.1007/s10648-017-9421-7

[15] Haider, J., & Sundin, O. (2020). Information literacy challenges in digital culture: conflicting engagements of trust and doubt. *Information, Communication & Society*, 1-16. doi:10.1080/1369118X.2020.1851389

[16] Civic Online Reasoning site of Stanford University https://cor.stanford.edu/

[17] Breakstone, J., Smith, M., Wineburg, S., Rapaport, A., Carle, J., Garland, M., & Saavedra, A. (2021). Students' Civic Online Reasoning: A National Portrait. *Educational researcher, 50*(8), 505-515. doi:10.3102/0013189X211017495

[18] Wineburg, S, Breakstone, J., McGrew, S., Smith, M., and Ortega, T. (2022) Lateral Reading on the Open Internet: A District-Wide Field Study in High School Government Classes *Journal of Educational Psychology* (Accepted for publication)

[19] McGrew, S., & Byrne, V. L. (2020). Who Is behind this? Preparing high school students to evaluate online content. *Journal of Research on Technology in Education*, 1-19. doi:10.1080/15391523.2020.1795956

[20] Axelsson, C.-A. W., Guath, M., & Nygren, T. (2021). Learning How to Separate Fake From Real News: Scalable Digital Tutorials Promoting Students' Civic Online Reasoning. *Future Internet, 13*(3 60), 1-18.

[21] Simon, H. A. (1971). Designing organizations for an information-rich world. In M. Greenberger (Ed.), Computers, communications, and the public interest (pp. 37–72). John Hopkins University Press

[22] Wineburg, S., & McGrew, S. (2019). Lateral reading and the nature of expertise: Reading less and learning more when evaluating digital information. Teachers College Record, 121(11), Article 22806. https://www.tcrecord.org/content.asp?contentid=22806

[23] Wineburg, S., & McGrew, S. (2019). Lateral reading and the nature of expertise: Reading less and learning more when evaluating digital information. Teachers College Record, 121(11), Article 22806. https://www.tcrecord.org/content.asp?contentid=22806

[24] Breakstone, J., Smith, M., Wineburg, S., Rapaport, A., Carle, J., Garland, M., & Saavedra, A. (2021). Students' Civic Online Reasoning: A National Portrait. Educational researcher, 50(8), 505-515. doi:10.3102/0013189X211017495

[25] DSA https://www.europarl.europa.eu/news/en/press-room/20220412IPR27111/digital-services-act-agreement-for-a-transparent-and-safe-online-environment

[26] DMA https://www.europarl.europa.eu/news/en/press-room/20220315IPR25504/deal-on-digital-markets-act-ensuring-fair-competition-and-more-choice-for-users

7. Claim your rights! From users to citizens in online environments

MINNA ASLAMA HOROWITZ, UNIVERSITY OF HELSINKI

When on social media, we want to be informed and, even more often, entertained. We love the seemingly free access, functions, and borderless connectivity. We may even be aware of the price we pay by giving away our data – and some of us may say that is a bargain for all the content and fun functions that they serve us just as we like it. However, we think less often about the platforms as powerful public arenas that can impact our mental health, promote violence against societal groups, make or break elections, or fuel wars.

The digital era has brought about the centrality of digital platforms in supporting or violating basic global principles on individuals' rights. From that perspective, we are citizens. Our actions come with responsibilities and are also connected to basic human rights. To date, there is not one legal stipulation about our rights as global digital citizens – but many stakeholders are involved in thinking about how to define and protect those rights. This chapter outlines the ways in which digital platforms, the United Nations, the European Union, and civil society understand and protect our digital rights.

Human Rights in the Digital Era

Today, platforms and other technology companies impact such a great part of our lives, and our societies, that they are also key players in realising or restricting our basic rights. Internet access gives us a gateway to unlimited content but platforms also act as gatekeepers for the kind of information Google or TikTok recommend to us. We get free services in exchange for our data – but often we don't know how our data is used and how it affects our privacy. We get to express ourselves easily and freely; yet we also expose ourselves to plenty of false information, manipulation, and hate speech. As the report by the United Nations Secretary-General on digital cooperation notes, digital technologies do not only help to advocate, defend and exercise rights, but they are also used to suppress, limit, and violate human rights[1].

The question is not only about war censorship or internet shutdowns that may happen far away from our daily lives. In fact, we know little about how our rights are respected as users of global digital platforms. The organization Ranking Digital Rights monitors what big platforms and telcos around the world let us know about our rights. Its Big Tech Scorecard ranks corporations in terms of how they let us know about their internal rules and practices (governance), how they address our privacy, and how they protect our freedom of expression. Regrettably, these giants from Amazon and Alibaba to Twitter and Yandex keep us very much in the dark. If one can find the information about their terms of service and users' rights, those terms can be hard to understand. That kind of informal also often lacks crucial facts, such as with whom they share our data, or whether they follow international human rights principles when developing their algorithms. And even if a company such as Meta has a human rights policy, it is practically impossible for individuals or independent organizations to monitor the implementation of the policy.[2].

How the UN and EU approach our rights

Year on year, the UN has become more and more concerned about the impact of digitalization in our world. Many issues that we face in the digital era are already included in the most well known and most global guide to our rights: the United Nations Universal Declaration of Human Rights (UDHR) of 1948.[3] For example, Article 12 stipulates the right to privacy, and Article 19 addresses freedom of expression.

The UN seeks to address human rights and communication in general via its Human Rights Council[4], the Office of the United Nations High Commissioner for Human Rights (OHCHR)[5], and specifically with its annual meeting for nation-states, companies, scholars, and civil society, titled the Internet Governance Forum.[6] Because of the power of private corporations from Google to TikTok, also the UN Guiding Principles on Business and Human Rights[7] are used to stress the rights-based responsibilities of tech companies. While the UN does not create laws, it takes a stand on issues such as digital connectivity as a human right,[8] or ethical guidelines for Artificial Intelligence.[9]

The European Union is another significant, and pioneering, stakeholder in defining our digital rights. With its comprehensive plan for digitalisation of Europe by 2030, known as the Digital Compass[10], the EU is not only creating laws to support its digital economy but also to provide digital security and empower its citizens. The fundamental principles of the Compass are laid out in the European Democracy Action Plan, including the essential role of citizen rights and participation, as well as the work against disinformation[11]. In 2022, the EU proposed a European Declaration on Digital Rights and Principles, the first citizen-centric and rights-based declaration by an international governmental organisation. The Declaration highlights inclusion, participation, users' choices, safety, and sustainability in the digital environment[12].

Civil Society: Freedom Fighters and Watchdogs

While the UN and the EU offer official principles, innumerable organizations are active internationally and locally in safeguarding our digital rights. Some, like Article 19, Freedom House, and Human Rights Watch, are traditional international human rights freedom fighters. Today, these organisations see technology as a tool to hold power accountable but also point to problems brought by digitalization, including the freedom of expression online.[13] Others, like AccessNow and the Electronic Frontier Foundation (EFF) focus on digital rights in particular.[14]

Many other groups and organizations specialise in some aspect of our digital rights. For instance, MyData Global, a non-profit organisation originally founded in Finland, advocates for our individual rights to manage our own data.[15] Privacy International, in contrast, is concerned with state and commercial surveillance.[16] Some organizations, among them the JustNet Coalition, address the so-called digital divides and work globally for a more equitable internet.[17] Many organisations, including our independent EDMO/NORDIS fact-checkers, focus on ensuring trustworthy information and people's capabilities in digital information literacy.

With a Little Help...

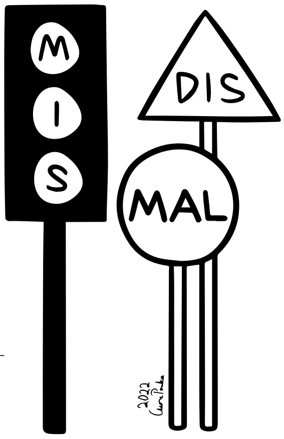
In the end, our rights are up to us. At this time, there is no digital constitution cementing our rights globally. Technology develops at such a fast speed that any detailed rights might become obsolete as soon as they are instituted.

The digital environment can enlighten, entertain and educate us. It can help us innovate, create, earn a living, connect with others, and make a difference. Because of its immense potential for positive change, we should take our rights and related responsibilities as digital citizens seriously. We can do so with support on several fronts:

- The UN sets the stage with basic principles and an international fora to discuss our rights.
- The EU offers support through various legislative initiatives, in particular with its recent Digital Services Act Package that aims to regulate the largest global platforms in particular.[18]
- Civil society organizations and groups, often the pioneers in addressing digital harms and problems, can keep us updated on developments in different aspects of digital rights.
- And, with DigComp 2.2, the EU also gives us a framework for understanding the kinds of digital civic skills we need: knowledge of digital information literacy, capabilities to communicate, collaborate and create content as well as solve problems in the digital environment; and the ability to protect our privacy.

[1] https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf
[2] https://rankingdigitalrights.org/mini-report/key-findings-2022/
[3] https://www.un.org/en/about-us/universal-declaration-of-human-rights
[4] https://www.ohchr.org/en/hr-bodies/hrc/about-council
[4] https://www.ohchr.org/en/ohchr_homepage
[6] https://www.intgovforum.org/en
[7] https://www.ohchr.org/en/publications/reference-publications/guiding-principles-business-and-human-rights
[8] https://www.un.org/en/un-chronicle/case-connectivity-new-human-right
[9] https://en.unesco.org/artificial-intelligence/ethics
[10] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en
[11] European Democracy Action Plan: Making EU democracies stronger. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250
[12] European Declaration on Digital Rights and Principles for the Digital Decade. https://ec.europa.eu/newsroom/dae/redirection/document/82703
[13] https://www.article19.org/issue/digital-rights/; https://www.hrw.org/topic/technology-and-rights ; https://freedomhouse.org/report/freedom-net
[14] https://www.accessnow.org/; https://www.eff.org/
[15] https://www.mydata.org/
[16] https://www.privacyinternational.org/
[17] https://justnetcoalition.org/
[18] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

8. Many shapes and sizes: Dissecting online disorders



MINNA ASLAMA HOROWITZ, UNIVERSITY OF HELSINKI

Fake News! Propaganda! Manipulation! Conspiracy! The digital realm is plagued by content that is accidentally or intentionally false, harmful – or both. This chapter addresses how we can begin to make sense of the different diseases and their symptoms – to support our digital health.

The narrow approach to online disorders focuses on verifiably false information. This form is relatively easy to identify and can be countered by hiring fact-checkers, tagging suspicious postings, removing false news posts, and so on. A more difficult malaise to diagnose is when we begin to address deliberate attempts at the distortion of news to promote ideologies, confuse audiences, create polarisation, and disseminate disinformation to earn money. While many of these activities can be politically motivated, these attempts can take the form of clickbait practices and the intentional filtering of news for commercial purposes, to attract particular audiences. This approach is harder to study and verify empirically. It pertains to the economic models of news markets and variations in the quality of news.

To help us understand different dimensions of false content online, Claire Wardle and Hossein Derakhshan created a framework of **information disorder** (Figure). It makes a distinction between different types **of content based on their intended purposes:**

- Misinformation – false connection or misleading content that can be also unintentional and that is not always harmful. This includes shared content that is believed to be true and should be made public for the common good, even if its veracity has not been checked;
- Disinformation – intentional false context, including intentionally created conspiracy theories, or other content that can in some cases be harmful; and
- Malinformation – false content that is purposely created to cause harm, or use of content for malicious purposes.

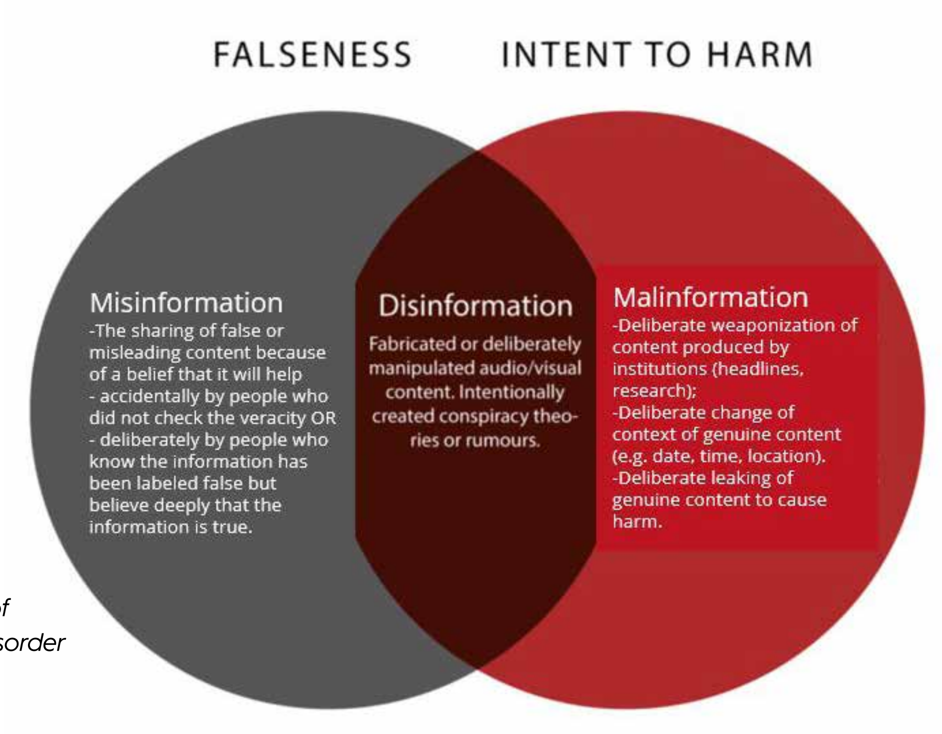

FALSENESS
INTENT TO HARM
Misinformation
-The sharing of false or misleading content because of a belief that it will help
- accidentally by people who did not check the veracity OR
- deliberately by people who know the information has been labeled false but believe deeply that the information is true.
Disinformation
Fabricated or deliberately manipulated audio/visual content. Intentionally created conspiracy theories or rumours.
Malinformation
-Deliberate weaponization of content produced by institutions (headlines, research);
-Deliberate change of context of genuine content (e.g. date, time, location).
-Deliberate leaking of genuine content to cause harm.

Figure: Types of Information Disorder (2022)[2]

For audiences, the distinction between different types might not always be apparent – but for those attempting to remedy these disorders it matters. The framework of information disorder is now widely used by journalists, policy-makers, and researchers as their roadmap to false content online. Naturally, these actors need to focus on the truly harmful content. From a legal perspective, two things matter: what the intentions of the content creator are, the content, and how untrue it is. A journalist may accidentally include inaccurate information in a piece of news. In contrast, a propagandist can deliberately create fully fabricated content, meant to deceive its audiences.[3]

In practice, then, information disorder can take many **forms**. As an example, the European Union (EU) multi-stakeholder High-Level Expert Group (HLEG) on Fake News and Online Disinformation identifies the problem of practices that go well beyond anything resembling "news": automated accounts, networks of fake followers, fabricated or manipulated videos, targeted advertising, organized trolling, visual memes, and so on.

Similarly, information disorder includes many types of **actions**. In addition to the process of creating false content, disinformation is circulated in many ways, including posting, commenting, sharing, tweeting, and retweeting.

Finally, information disorder is not a disease without a cause. It is an action by different **stakeholders** who help to inflame or remedy online harms. Online platforms and underlying networks, protocols, and algorithms make the dissemination of mis-, dis-, and malinformation easy and viral. Because global platforms make money with user data, curbing the spread of false information is not in their interest if it just gets eyeballs, likes and shares. Additionally, various state or non-state political actors, for-profit actors, citizens individually or in groups, and infrastructures of circulation and amplification (including news media) may want to stop false information – or may want to create and spread it widely.[4]

[1] Wardle, C., & Derakhshan, H. (2017). Information Disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

[2] Updated version by Wardle in 2022; see, e.g., https://faktabaari.fi/tapahtumat/claire-wardle-massive-problems-are-tackled-with-a-minimal-budget/

[3] E.g., Möller, J., Hameleers, M., & Ferreau, F. (n.d.). Types of disinformation and misinformation Various types of disinformation and their dissemination from a communication science and legal perspective. https://www.die-medienanstalten.de/fileadmin/user_upload/die_medienanstalten/Publikationen/Weitere_Veroeffentlichungen/GVK_Summary_EN_final_web.pdf

[4] See, https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation.

9. Political propaganda based on psychological manipulation

JOONAS PÖRSTI, FAKTABAARI

Political propaganda is a broad form of influence aimed at persuading the target audience to act in accordance with the propagandist's objectives. The hallmark of propaganda is psychological manipulation, typically through the use of disinformation, i.e. the deliberate dissemination of misleading information. However, the range of means is not restricted to disinformation. It can also be used to disseminate malinformation, i.e. accurate information disseminated with the intention of discrediting or otherwise harming a party. Effective propaganda also relies on partial truths, content taken out of its original context, and the withholding of information.[1]

At the heart of propaganda there is typically an alternative, black-and-white, simplistic narrative that, in the words of philosopher Hannah Arendt[2], "meets the needs of the human mind better than the true reality". A skilled propagandist tailors his or her methods to the expectations of his or her audience, so that they do not find themselves being duped. People are prone to adopt propaganda that reinforces their social status and identity, at least in their mindset.

Propaganda is not limited to the dissemination of information, but goes hand in hand with the manipulation of the target audience through various events. These may include court cases, staged or top-down social movements and mass events, acts of violence, harassment or military threats. Propaganda is counterproductive to democratic ideals in that it seeks to limit public debate on policy options without rational justification[3]. A propagandist can still present himself as an advocate of freedom of expression and democracy. These are often invoked as symbolic slogans when the real aim is to undermine democratic institutions.

Originally, "propaganda" simply meant the spreading of correct doctrine. The term was born in 1622, when Pope Gregory XV founded a 'sacred community for the propagation of the faith' in Rome, the Sacra Congregatio de Propaganda Fide, to serve the Reformation and Catholic missionary work. The concept only acquired a negative connotation in the aftermath of the world wars of the 20th century[4]. In democratic societies in particular, propaganda has since been associated in the mind with authoritarian societies such as Nazi Germany, the Soviet Union, China or Vladimir Putin's Russia.

However, propaganda is also disseminated in democratic societies, and their freedom of expression can make them particularly vulnerable to propagandist influence. In recent years, the systematic use of propaganda in the United States has polarised the political climate and made social reform more difficult. After losing the 2020 presidential election, Donald Trump destabilised the country's political system by spreading the narrative of a "stolen election". The propaganda campaign culminated on 6 January 2021, when Trump supporters stormed the US Congress and more than a hundred police officers were injured on Capitol Hill in Washington[5]. Similarly, Hungarian President Viktor Orbán has used propaganda to silence political opposition and undermine democratic institutions.

State-run propaganda has also been a key form of power in Russia under Vladimir Putin. Putin became president in democratic elections in 2000, but the Russian presidential administration was already prepared to use propaganda to advance its domestic and foreign policy objectives. The country's political opposition was suppressed and critical voices silenced by concentrating ownership of television channels in the hands of those in power. The president's position was also strengthened by building a cult of leadership. At the same time, the Putin regime maximised its room for maneuver in foreign policy by maintaining a semblance of respect for democratic values in Russia[6].

Propaganda is the mobilisation of large numbers of people for political purposes, but it is not limited to state actors - it can be spread by political parties, ideological groups, lobbyists hired by companies or civic activists organised on social media. Propaganda is generally not capable of changing people's minds suddenly, but can gradually shape attitudes in the desired direction. However, the most effective and quickest way is to exploit pre-existing preconceptions, i.e. deeply rooted beliefs and enemy perceptions. Psychological manipulation is based on a good understanding of the recipients' preconceptions. Propaganda can be designed on the basis of cultural knowledge, sociological studies and opinion polls. Historically established cultural myths are particularly useful, they serve as building blocks for worldviews and therefore provide a ready-made framework for propaganda. Myths guide people's social imagination and are linked to notions of the sacred - the nation, its origins and traditional values[7].

Examples of such myths include the anti-Semitic ideology of Nazi Germany, the narrative of Russia as the 'third Rome' protecting Christianity, or the US as the defender of freedom in the world. Propaganda is built on confrontations: in Nazi Germany, the militaristic hero image was built on the lower "races" and the Jews, who were labelled as special syntypes[8].

In the 21st century, the internet and especially social media services have provided new tools for the dissemination of propaganda. Emotional messages spread rapidly on social media networks, the gatekeepers of traditional media are absent and the origin of the message can be hidden behind anonymous accounts. It is easy to spread so-called black propaganda on social media, where manipulative messages are sent under the identities of the opposing party. For example, a single-issue movement or a news site can be set up for this purpose. The content is limited only by the imagination: the aim of propaganda can be to increase social tensions or to distract the public with irrelevant or distorted issues. The content of black propaganda can be completely fake or partly true. The real source of the message tries to remain hidden so that the propaganda does not turn against itself.

In the early days, there was no regulation of digital services and for example ISIS was able to freely spread its propaganda inciting violence on Facebook, Twitter and YouTube[9]. Since then, digital platforms have become more self-regulated, but their commercial profit logic still drives visitors to polarising and emotive content, providing ample tools for propaganda. Propaganda overlaps with all other communications, marketing and news, and online content is mixed[10]. Fact-checking has also increased, but it still provides an incomplete response to information failures on digital platforms.

In the age of the Internet, Russia, for example, has used a model in its propaganda that the US-based Rand Institute has dubbed the firehose of falsehoods[11]. In this model, the propagandist quickly puts out various confusing versions of events without much regard for their credibility. The strategy is to undermine trust in the media and democratically elected decision-makers with "alternative truths" and conspiracy theories[12]. The radical right in the US has relied on similar methods. If nothing is considered true any longer, the propagandist has a freer hand to pursue their own arbitrary policy. The antidote to such propaganda is digital information literacy and an understanding of propaganda techniques. The impact of propaganda can be weakened by revealing the methods used in advance, thus reducing the effectiveness of the manipulation and allowing the public to discount the propagandistic messages[13].

References

Arendt, Hannah. 1958. The Origins of Totalitarianism. Cleveland: George Allen & Unwin.
Berger, Jessica, and J. M. Stern. 2016. Isis: The State of Terror. London: HarperCollins.
Dawisha, Karen. 2014. Putin's Kleptocracy; Who Owns Russia? New York : Simon & Schuster.
Ellul, Jacques. 1973. Propaganda: The Formation of men's attitudes. New York: Vintage Books.
Hasen, Richard. 2022. Cheap Speech. How Disinformation Poisons Our Politics—and How to Cure It. New Haven: Yale University Press.
Jowett, Garth, and Victoria O'Donnell. 1992. Propaganda and Persuasion. Los Angeles: Sage.
Klemperer, Victor. 2002. The Language of the Third Reich. London & New York: Continuum.
Lasswell, Harold. 1951. "The Strategy of Soviet Propaganda." Proceedings of the Academy of Political Science (24).
Lucas, Edward, and Peter Pomerantsev. 2016. Winning the Information War: Techniques and Counter Strategies to Russian Propaganda in Central and Eastern Europe. Washington : Center for Eastern European Policy.
Marlin, Randal. 2002. Propaganda and the ethics of persuasion. Peterborough: Broadview Press.
Nimmo, Ben. 2015. Anatomy of an Info-War: How Russia's Propaganda Machine Works and How to Counter It. Central European Policy Institute. https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/.

[1] Jowett ja O'Donnell 1992, Marlin 2002, Lasswell 1951, Pörsti 2017.
[2] Arendt 1958.
[3] Stanley 2015.
[4] Taylor 2003.
[5] Hasen 2022.
[6] Van Herpen 2015, B. Nimmo 2015, Ostrovsky 2015, Dawisha 2014.
[7] Ellul 1973.
[8] Klemperer 2002.
[9] Berger ja Stern 2016.
[10] Valaskivi 2018.
[11] Paul & Matthews 2016.
[12] Lucas & Pomerantsev 2016.
[13] Nimmo 2015.

10. What can we learn from fact-checkers?

PIPSA HAVULA, FAKTABAARI

The fact-checking process always starts with the same basic question: really? Once curiosity has been aroused, the claim is checked.

Research shows[1] that the way fact-checkers approach new information on digital platforms, called "lateral reading", has proven to be very effective. Traditional reading and textual analysis can be ineffective in the digital environment, because if readers start analysing unknown online information without first checking the source of the article, they may not realise that the whole text is based on biased or completely misleading information. In a lateral reading mode, the reader checks the background of the online information on different sites and sources before engaging with it. When confronted with previously unknown online information, fact-checkers immediately open several tabs in their browser and look for information about the organisation or the person behind it.

While the average reader may spend a considerable amount of time reading and thinking about incorrect information, fact-checkers use what is known as strategic ignoring. With a little scrutiny, online sources that turn out to be dubious and untrustworthy are quickly ignored. The premise is that the information is of poor quality until proven otherwise.

In its simplest form, when a fact-checker comes across a new online newspaper (e.g. the Daily Mail), he or she immediately opens a new tab in the browser, enters the name of the newspaper in the search engine and adds the word "reliability" or "bias" (e.g. Daily Mail reliability) and examines the results. The search engine will look for information that will help to assess the reliability of a website or news article. At the same time, it looks at what kind of articles have been published by the same media in the past, who is responsible for the magazine and who distributes its texts. In Finland, the website of the Council for Mass Media[2] provides a quick way to see whether an online journal has committed to its principles. In more complicated cases, the founder of a website can be traced back to the website's founder, for example, through information in the code or various registry data.

Lateral reading also works when browsing through the stream of images and videos on social media platforms. When curiosity is aroused, the fact-checker looks at different sources to find out who published the claim, possible motives and, for example, where else the same image or video has been published before. There are a number of free online tools available to check the veracity of images and videos, which are described in more detail at the end of this article.

The working methods used by fact-checkers have become an essential part of digital information literacy. Fortunately, these online literacies can be learned, taught and developed, and the fact-checkers at FaktaBaari have collected some of their own and colleagues' approaches to developing source criticism in particular in this article. We will supplement the articles in this guide with educational videos for the FaktaBaari website at: www.faktabaari.fi/dil

Introduction to the fact-checking process and methodology

Fact-checking is the process of checking whether or not a claim made in the public domain is true. Fact-checking helps to distinguish between false, distorted, misleading or ill-founded claims, and reliable, truthful information.

According to the Duke reporters' lab[2] there are currently around 400 teams of investigators and journalists in 105 countries around the world who carry out fact-checking. In Europe, there are more than 110 fact-checking services. Some fact-checking services operate completely independently, some as part of the traditional news media and some, for example, as part of think tanks.

Three tips for source criticism from fact checkers:

1. If a claim, image or video you come across online causes a strong emotional response, stop. Disinformation spreaders often seek to stir up emotions, and when emotions are running high, it's harder to critically evaluate the claim.

2. Ask yourself three important questions. 1) Who is spreading the claim 2) What evidence has been presented to support the claim? 3) What do the various sources have to say about it?

3. Practise a quick read-through. You don't have to read everything from beginning to end. A more effective way to get a handle on the credibility of a source is to read through a site or news story in broad strokes, open a search engine in another tab, and see what other sources have to say about the credibility of that site.

Faktabaari[3] is an independent fact-checking service established in Finland in 2014 with Open Society Association (Avoin yhteiskunta ry) as its administrative association. Faktabaari aims to strengthen knowledge and fact-based public debate in Finland. It works with the University of Helsinki as part of the Nordic NORDIS network[4], whose mission is to identify and combat mis- and disinformation.

Fact-checking is needed because false or misleading information can undermine people's opinions and influence their actions. According to Eurobarometer, 83% of Europeans see fake news and disinformation as a threat to democracy. The world has seen how disinformation can influence elections, erode trust in institutions, undermine freedom of expression or even reduce the willingness to take a vaccine. Verifying claims with reliable information from credible sources is one effective way of countering misinformation.
However, it is important to remember that the interpretation of claims is not always unambiguous and that facts can also be interpreted in different ways. For this reason, fact-checking seeks to be as transparent as possible in indicating the source of the information, so that the reader can judge for themselves the reliability of the sources and form their own opinion on the matter.

The FaktaBaari editorial process:

1. Faktabaari selects the claim to be checked. The editorial team of the FaktaBaari screens socially relevant claims from social media and other public discourse that warrant review in order to promote a fact-based public debate. A claim for review can also be submitted to the editorial office via a hotline form or other means of contact.
2. The claim will be verified by a comprehensive collection of reliable data or by verification, for example by image, audio or video. Some checks can be done with just online fact-checking tools or a few phone calls, but some require several days of research, for example by looking at statistical data or scientific research on the subject. The first step in fact-checking is to get to the original sources. Often, the originator of the claim is first checked to see how the claim is formulated and offered the opportunity to correct it themselves.
3. The fact-checking process involves interviewing experts. There is no such thing as a completely neutral expert and therefore expert opinion should always be checked by at least one other independent source.
4. The collected sources and information from the experts are compiled into a coherent fact-checking story. The fact-checked claim is presented by the fact-checker in the correct context and in accordance with good journalistic practice. If the experts have provided con-

flicting interpretations of the claim, the conflict must be openly documented. In difficult cases, further sources and experts are sought to verify the claim.

5. The decision to publish the fact-checking story is made by the Editor in Charge. Before doing so, its sources are checked once more. The content of the fact-checking story is reviewed by the editorial team and often with the experts interviewed for the story. However, the editorial team makes an independent decision on the content and publication of the story. The story is also published with an overall assessment of the validity of the claim made.

All material generated by the review is documented and archived. If Faktabaari has to justify its decision at a later stage, it must be possible to evaluate each stage of the review afterwards.

If the FaktaBaari publishes incorrect factual information, it will seek to correct it without delay and as comprehensively as possible.

Checking the accuracy of images and videos

When browsing the web, you often come across images and videos that raise questions. Has this been edited? Where and when was this filmed? What is really happening in the video or image? Checking the authenticity of an image or video is not always easy and sometimes it can even seem impossible. However, technology is evolving all the time, and while it's getting easier to edit images and videos, so is the technology to check their accuracy. Anyone can use the free online fact-checking tools that fact-checkers use in their daily work.

It is important to remember that it is not always the case that the video or image has been edited, but that the material is perfectly authentic but presented in the wrong context.

PICTURES

Reverse image search. Reverse image searches provided by various services are often the best places to start checking a photo. A reverse image search uploads or links to the image under review, allowing the search engine to find similar images. This can be used to find, for example, where and when a particular photo was taken, where else the same photo has been published before, or even who the person or building is in the photo. When searching for the original source, it is worth looking at the resolution of the images: usually the highest resolution image will lead you towards the original place of publication.

Reverse image search can be found on Google (google.com/imghp), Tineye (tineye.com), Bing (Bing.com) and Yandex (yandex.com/images). These services work in slightly different ways and may find different things, which is why it is useful to do a reverse image search on several different services. For example, when using reverse image search on Google, you can specify the time period for which you are looking for images. Google will always add a keyword after the image search, and you should try changing it to change the search results. Bing recognises the text in the image and sorts the images by size, while Tineye allows you to put the images in chronological order.

The problem with reverse image searches is that they don't usually find images posted on, for example, Instagram.

Image metadata. Images store a wide range of metadata, which can be viewed on sites such as Fotoforensics (Fotoforensics.com). The metadata may include the date and time the photo was taken. If the image is an original, it will probably also include information such as the model of camera or phone used to take the picture. Sometimes, although rarely, the metadata will also include the GPS coordinates of where the picture was taken.

On the Fotoforensics website, it is also possible to obtain an Error Level Analysis (ELA) of the photograph, which can be used to identify image manipulation. ELA analysis helps to identify areas of the photograph where the compression level differs from other areas of the image. Areas that differ from the rest of the image may indicate image manipulation.

Small clues. It is worth looking for small details and clues in the image. For example, are there signs, flags, license plates, weather conditions, or a recognizable building or landmark? Or can you infer something from the way the people in the picture are dressed?

If the image shows the sign in a foreign language clearly enough, you can upload the image of the sign to Google Translate, which will translate the sign text. The weather conditions on a particular day in a particular place can be viewed on Wolfram Alpha (wolframalpha.com). Various mapping services, such as Google Street view, Mapillary.com and Map.snapchat.com, as well as satellite imagery, can help you find the exact spot where the picture was taken.

VIDEO

Many of the above methods also work for viewing videos: searching for small clues, reverse image search and metadata often help you get on the right track.

Reverse image search. It is also possible to reverse image search a video by taking screenshots of it and uploading them to the reverse image search. The InVid add-on[5] installed in your browser helps you to perform multiple reverse image searches of different parts of the video at once. The InVid tool also allows you to view video metadata, such as the date of shooting.

Watch and listen. There is a lot of talk about real-looking deepfake videos, but so far this technology has not been widely used to disseminate disinformation. Deepfake videos use image manipulation to get a person to say or do things that they have not actually said or done.

More common than deepfake in video hoaxes is that the real video is, for example, cut in a misleading way, creating a distorted picture of what the speaker is saying. The editing may be very subtle and skilfully done, making it difficult to detect.

The original video can be found using a reverse image search or a search engine. There are other ways. By watching the video carefully, listening to the audio and looking for odd jumps, you can track down the editing manipulation. At watchframebyframe.com, you can link to a video posted on YouTube or Vimeo and watch every frame in slow motion, making it easier to spot a surprising jump.

Translating a video in a foreign language. One of the ways in which misinformation is spread is by subtitling videos incorrectly and by placing the foreign language video in a completely false context. If the video is in Russian, for example, and the recipient does not speak that language, it is easy to use fictitious subtitles or a fictitious context to make claims that are not true.

However, the video can be translated into your own language. All you need is two different devices, such as a smartphone and a laptop. The Google Translate app, which can recognise speech and translate it, is downloaded onto the smartphone. On the second device, a video and audio is played, and Google Translate on the phone listens to the speech and translates it into the desired language. Translation services are not perfect, but the context of the video or the rough meaning of the speech can be understood by this method.

The FaktaBaari website shares illustrative video tutorials on these typical basic skills for fact-checkers. www.faktabaari.fi/DIL

Examples of stories that have gone through this process can be found on the fact-checkers' website - for FaktaBaari www.faktabaari.fi.

[1] Wineburg, S, Breakstone, J., McGrew, S., Smith, M., and Ortega, T. (2022) Lateral Reading on the Open Internet: A District-Wide Field Study in High School Government Classes [1] Journal of Educational Psychology https://psycnet.apa.org/fulltext/2022-53872-001.pdf

[2] https://reporterslab.org/fact-checkers-extend-their-global-reach-with-391-outlets-but-growth-has-slowed/

[3] Faktabaari https://faktabaari.fi/

[4] NORDIS https://datalab.au.dk/nordis

[5] https://www.invid-project.eu/tools-and-services/invid-verification-plugin/

11. Fact-checking transparency codes - how do I identify a fact-checker?

MIKKO SALO, FAKTABAARI

In the previous chapter 10 of the Digital Information Literacy Guide, we discussed the methods used by fact-checkers in an easily manipulated digital information environment. The same source-criticism and critical reading skills apply for social media. Social media is often overlooked when it comes to monitoring media, even though, for better or worse, social media is part of citizens' everyday lives. Fact-checkers are kind of "role models" of digital information literacy, with particular expertise in this ethically challenging environment. But what are the professional ethical issues involved in their work?

This chapter briefly reviews the ethical codes of fact-checking that have evolved to complement classic journalistic principles and codes. Fact-checking is a public service that is still in search of sustainable funding models. The chapter opens up premises for fact-checking as a public service to assess information disorders, especially mis- and mal-information, and explains how ordinary citizens can identify a fact-checker committed to an ethical code of transparency and use this work to promote a more fact-based public debate in the midst of the information war. There is a war on facts, but together we can work to ensure that our knowledge is built on the most reliable and transparent approach possible.

Fact-checking based on openness and transparency
The reliability of fact-checking has traditionally been based on exemplary openness and transparency. These principles are also reflected in the international codes of ethics for fact-checking, which form the basis of the Faktabaari Code of Conduct described in Chapter 10 above.

The International Fact Checking Network (IFCN) compiled its transparency principles into the first common code in 2016. At its core, it continues to unite verifiers around 1) requirements for impartiality and fairness, together with 2) transparency of methodology, sources, funding and correction policies. Since then, these principles have been refined both in regards to content since the scope of social media cooperation has increased and territorial cooperation deepened. The table in the annex to this chapter provides links to complementary transparency codes and their memberships.

Following the establishment of the IFCN Global Code of principles, a transparent and regular review process for the evaluation of review services was built into it. The aim was to answer the important question: who checks the fact-checker? This development was spurred by the fact-checking services' initial collaboration with social media companies such as Facebook and Google in the aftermath of the 2016 US presidential election. The fact-checkers took the initiative to also serve the public on social media channels, which evolved into a "third party fact-checking" programme. Over the following years, this programme became a development that strongly professionalised fact-checking but also oriented its content priorities. With funding from social networking sites, and Facebook in particular. Fact-checking became increasingly focused on content from paying sites and outright disinformation, while the traditional and still important work of fact-checking claims made by politicians diminished.

As part of the same professionalisation brought about by the platform partnership, a quantitative requirement for regularity was added to the quality code in 2017, which meant weekly fact-checking. In this context, many smaller fact-checking services or those that focused on background checks with limited resources had to withdraw from the code or change their strategy. In principle, however, all fact-checkers continued to be members of the IFCN community, including meeting collegially to learn from each other at the annual Global Fact events, which have grown to become the main event in the sector.

Social media companies wanted to demonstrate through this "independent fact-checking" programme to politicians, particularly in the US and at EU level, who were eager to regulate them, that they were able to weed out as much disinformation as possible from their platforms so that their business would not be disrupted by new legislation. However, the independent fact-checking programme posed a dilemma for fact-checkers: while few politicians are known for wanting to be fact-checked, social media companies had no interest in embarrassing their regulators.

The platforms incentivised the fact-checking services they funded primarily to focus on potential disinformation cases identified by their algorithms. The details of the contracts with the fact-checkers and social media companies were protected by non-disclosure agreements typical of corporate law. This arrangement placed unreasonable demands on many small fact-checkers. They were able to serve their audiences through new channels, but with less transparency. Statements by elected politicians were excluded from the review activities funded by US companies on the basis of free speech arguments.

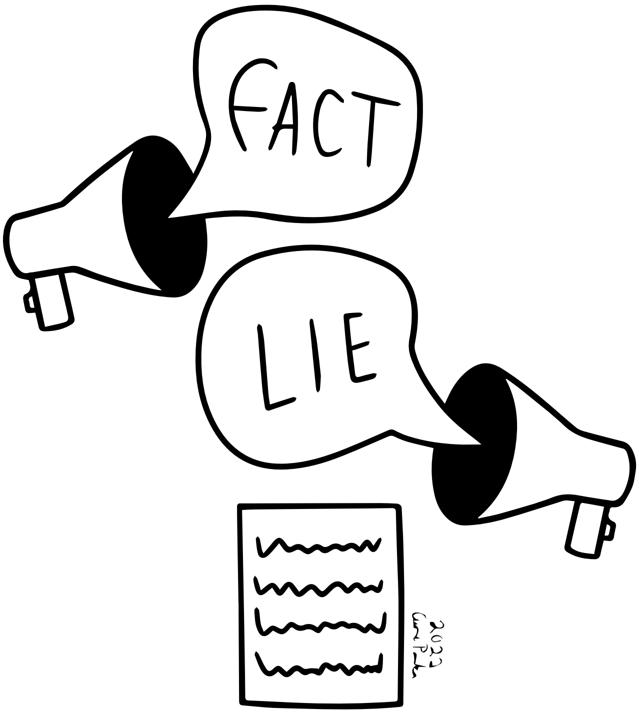
For example, during Donald Trump's four-year presidency, the Washington Post reviewed more than 30 000 inaccurate or distorting statements to hold the president accountable for what he said. The project was, however, a significant and symbolic investment by the traditional media fact-checking service itself against post-truth. In contrast, the "independent fact-checking" programme, which was funded by social media and grew global, checked a wide range of conspiratorial claims - particularly in relation to the important COVID 19 pandemic. This is something that the social media platforms always remember to mention in their PR speeches. However, it is not known how much of an impact the fact-checking exercise has had in limiting the information disorders circulating on the platforms, as it is not reported despite the fact-checkers' claims. In this regard, fact-checkers have called for more transparency from platforms in order to develop their operations in a modern, data-driven way.

The Nordic checkers have also continued to monitor the claims of politicians. In many developing countries, fact-checking has often just become, for the lack of other funding, the content moderation of highly skilled data workers on web platforms.

The choice of platforms not to fund the fact-checking of the politicians' claims has forced fact-checkers to critically evaluate their platform partnerships and also to invest in the search for complementary funding. This development was enforced after the election rigging in the run-up to, for example, the UK's 2016 Brexit vote.

Social media companies are more interested in the bigger fact-checking services within the most influential countries. In smaller countries or language areas, platform cooperation was not yet possible in the first years of the 3rd party fact-checker programme or it was avoided for various reasons. For example, Faktabaari, which focuses on information literacy and elections, saw already in 2017 more problems for the reputation and independence of the checker than concrete benefits. The Nordic fact-checkers have avoided platform dependency through various transparent trust-building arrangements, more details on them provided on their respective websites - in accordance with the code.

However, thanks to their social media experience, fact-checkers have integrated into the new digital media reality in a more agile manner than traditional media, and without abandoning their principles, and are thus suitable for public scrutiny in social media. On the other hand, the majority of people on social media may not even encounter fact-checks in social media, as Facebook (Meta) and Google, for example, use algorithms to lower the visibility of content that fact-checkers classify as



disinformation in their feeds, to the point where it often has to be searched for. As noted, fact-checkers do not have a detailed understanding of the algorithms that regulate the visibility of their output, but have naturally requested more information on their effectiveness in order to improve their performance. The data on this is currently only available to the platforms.

The IFCN's original 2016 openness code has been adopted globally and in all Nordic countries, for example, also in terms of quality alongside national codes (e.g. Finnish JSN and other Nordic media councils). Membership of the IFCN can be seen as a quality mark to be valued by the reader. Unlike Faktabaari, which focuses on digital information literacy, other Nordic fact-checking services are full members of the IFCN and also check claims for news companies.

Awareness of the ethical implications of platform cooperation, including through funding, for editorial choices has also increased via research and information leaks. This is particularly strong in the European Union, which has developed its privacy legislation. As a result, many fact-checkers have expanded their activities towards media and information literacy. The broader field also raises new ethical choices. Awareness of information disorders has also been strengthened in the NORDIS EDMO consortium of all Nordic fact-checkers and four research universities, launched in 2021. NORDIS is currently focusing its EU-funded efforts on checking, understanding and limiting social media information disorders. In practice, this makes NORDIS reviewers particularly good partners for societal actors and citizens interested in various forms of digital information literacy.

European cooperation to deepen transparency coding and broaden the scope of restrictions

Since 2017, fact-checking and related media and information literacy in Europe have been promoted through theoretical work and projects with the support of the EU and the Council of Europe, among others. One contribution of the Council of Europe is the funding of a basic book on digital information disorder (Information Disorder), already mentioned in this guide. The EU woke up to the opportunities of fact-checking after Trump's election and Brexit, before the European elections. Practical resourcing has also been slow to take off, but started to bring important diversity to previous funding from social media and foundations.

Two of the projects, mainly facilitated by the European Commission, are currently preparing the ground for a regional quality code that will complement the IFCN code, while allowing more regional bargaining power towards the social media platforms.

The most important European network of researchers, fact-checkers and media educators dedicated to disinformation is the European Digital Media Observatory (EDMO). Its aim is to create a European network of regional centres of excellence, with a particular focus on tackling disinformation. The Nordic countries are involved in EDMO through the NORDIS network initiative. Alongside EDMO and NORDIS, another ongoing European project is to tighten up the IFCN code in a European context and to seek cooperation with the open source intelligence (OSINT) community. OSINT is most famously represented by Bellingcat, which has excelled in the information wars. While the EDMO network membership is still largely based on the above-mentioned international IFCN codification - with a slightly lighter European quality assessment process, under the European EFCSN will be negotiating a genuinely deeper quality code for the European context would be foreseen in 2022.

Recently, all projects have been strained by the fight against COVID misinformation and, most acutely, by the information war that Russia has fuelled in order to divide Ukraine's supporters.

The main objective of these network projects on codes is to bring added value in intensifying cooperation across broader networks in thr fight against mis- and disinformation.

Year	Code (and development)	Members (07/2022)
2016	International Fact-Checking Network, **IFCN - Code of Principles**	**88 fact-checking organisations** ml. Faktisk.no, TjekDet, Källkritiksbyrån
2017	**Specification** of the IFCN Code with more detailed criteria for the launch of a **"3rd party fact-checker programme"**.	Map of fact-checking services participating in the **"independent fact-checking"** programme. AFP's global network explains the wider coverage than IFCN. Includes Nordic Faktisk.no, TjekDet, Källkritiksbyrån and AFP in Finland.
2021	The EDMO fact-checking **code** is so far largely based on the IFCN code and the **EDMO hubs** membership.	30+ European **members** including all **NORDIS** fact-checkers
2022	**European Fact-Checking Standards Network, EFCSN - project** Towards a wider code than IFCN for European fact-checkers and possibly OSINT operators by 2023?	The working committee has 15 members, including the Danish TjekDet. The wider consultative group consists of members of the European EDMO, IFCN and OSINT communities, including NORDIS fact-checkers. Secretariat with 6 members.

Where are we going with the transparency code(s)?

To summarise for the Nordic audience, the IFCN membership and quality stamp (see below) required for platform collaboration represent the most important code set so far, for which the European EDMO fact-checking community (see link) is a code set of equal quality without any impact on the visibility through the algorithms of the web platforms.

Provided that the European EFCSN community reaches a consensus on a more rigorous code in the course of 2022, European operators will be in a position to negotiate their own European-specific cooperation patterns with the web platforms, supported by the EU legislation that will enter into force between 2023 and 2024.

The global community will certainly continue to play its aggregating role as well as its role in product development. Platform collaboration has recently expanded to include the smaller Twitter and gradually also the fast-growing Chinese-owned TikTok and Google's YouTube.

However, alongside traditional content review, the increasing role of data and algorithms, different legislation, but also cultural differences between countries and practical challenges are now facts in favour of complementary regional quality work. The Nordic countries still represent a unique entity in terms of relatively strong institutions and journalist media. With their own strong and sometimes exceptional institutional information structures, such as strong school systems, broadcasters and libraries, Nordics stand out even within the EU.

The NORDIS network has good potential to develop our response to digital information disruption and to represent the Nordic countries in these wider contexts. It will focus on the Nordic communities of trust, which are also now forced to reassess themselves. For the time being a need for a separate Nordic fact-checking code has not been identified.

How to recognise a fact-checker committed to transparency from a fake fact-checker?

As quality codes become more established, as they grow, the laterally-reading citizen would look for 1) maximum transparency and openness on the part of fact-checkers regarding sources, authors, funding and, more generally, policies (see Chapter 10 of the Guide) and 2) one of the following quality marks from the IFCN and EDMO.

In principle, a commitment to good journalist practice, as defined for example by an independent national media council, such as the Finnish Council of Public Opinion (JSN), also indicates that the journalism is at least responsible. Commitment to codes and principles should always be checked with primary sources: even fake fact-checkers have claimed to be part of codes.

On the other hand, one such fake fact-checker "War on Fake", which spread Russian propaganda about Ukraine, did not go this far, but rather sought to undermine the trust in fact-checking. As we learned in Chapter 9, even raising suspicion can work if reality does not match one's expectations.

In terms of source criticism, digital information literacy assumes that the main line of defence against information manipulation is in between everyone's ears. We recommend fact-checking as an approach, supported by pedagogical fact-checking by professionals. When your own skills may not be sufficient, or you feel that a wider public debate would benefit from evaluating a claim, contact a fact-checking service. Fact-checkers are happy to take story tips and turn them into pedagogical checks, as well as support material to disseminate the checked information with your support. For more information: www.faktabaari.fi/dil

Sources and further information:
https://www.ifcncodeofprinciples.poynter.org/know-more/the-commitments-of-the-code-of-principles
https://www.jsn.fi/en/guidelines_for_journalists/
https://datalab.au.dk/nordis including links to fact-checking services
https://www.facebook.com/formedia/mjp/programs/third-party-fact-checking
https://www.washingtonpost.com/politics/2021/01/24/trumps-false-or-misleading-claims-total-30573-over-four-years/
https://faktabaari.fi/tapahtumat/claire-wardle-massive-problems-are-tackled-with-a-minimal-budget/)
https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c
https://www.jsn.fi/jsn/jsn-media-ja-neuvoston-jasenet/
https://www.ifcncodeofprinciples.poynter.org/signatories
https://edmo.eu/fact-checking-community/
https://eufactcheckingproject.com/

12. How to evaluate a scientific claim and expertise of an expert?

KARI KIVINEN, FAKTABAARI EDU

As a representative of the Finnish FaktaBaari, I had a privilege to be involved in a deeply engaging project coordinated by Stanford University. The final report "Science Education in the Age of Misinformation"[1] was published in spring 2022. An international team of experts examined how science education should respond to the challenges posed by the misuse of scientific information and evidence. The report also considers how to verify scientific claims made on social media and how to assess the competence of the person making the claim as an expert in the field.

It is important to be aware that all types of content circulate online. In addition to correct and useful information, there is also a great deal of incorrect information (misinformation, i.e. incorrect information spread in good faith or by mistake) and falsified information (disinformation, i.e. incorrect or inaccurate information deliberately spread). The dissemination of incorrect or falsified information is often harmful to both the individual and the community. It is therefore useful to identify who is behind the information and to verify the information from multiple sources to understand the perspective and possible bias of the source.

Every now and then we must assess the credibility of scientific news we find on social media. For example, is there scientific evidence of the benefits of using masks? Can we stop climate change? Is nuclear energy safe and is it a sustainable option? Modern science is so highly specialised that no one person can master all fields and all subjects. We are therefore dependent on experts and must evaluate whose expertise we can rely on – especially if the

expert opinions are somewhat contradictory.
In the past two years we have all come across distorted claims about the Covid-19 pandemic, which fact-checkers around the world have had to correct. More than 17,000 Covid-19 claims[2] have been verified by the joint efforts of fact-checkers. Some of these claims are based on what appear to be scientific studies and expert opinion. It is therefore important to reflect on how to take a healthy critical view of scientific claims and how to identify a true expert.

Disinformation is often dressed up as a reliable pseudo-scientific claim. Products may be marketed with misleading or non-existent references to various studies. Articles of questionable scientific quality are circulated on social media.

How to evaluate the expertise of experts?

When we choose a lawyer, plumber, dentist or architect, we look for evidence and references of the person's previous professional skills and qualifications. But how do you assess the expertise and authority of a scientist – whether they are a well-known and respected expert in their field, and what evidence of their expertise is there?

The criteria for a scientist's expertise are similar to those for other experts. It is important to find out[3]:

- **What is their track record and, specifically, their publication record in the field?**
- **Do they have standing within their field? For example, are they a fellow of a recognized scientific body, or have they won an award for their scientific work? Every professional group has watchdogs, boards, and certification authorities who police their own members to ensure that they live up to the standards of the profession and guarantee they are qualified to practice.**
- **What qualifications do they have? Is it a doctorate in the field? Or do they have other relevant experience, beyond formal credentials?**
- **Where do they work? Is it for a recognized scientific body or research institution?**
- **Is there any evidence of potential bias or pecuniary interest?**

Being a scientist requires years of education and often a PhD. Even a doctorate covers only a narrow field of knowledge. Expertise can also be acquired through scientific professional training or practical work experience.

"Just being a practicing scientist, however, is not enough. The individual must be a practicing scientist in the relevant field. Being a Nobel prize winner in one field, does not make you an expert in other fields. Yet, individuals may easily lump all scientists together as undifferentiated 'authorities.' A specialist in radiology is not somebody you would ask for advice on viruses. Being a scientist in one field of science does not make you an expert in all fields of science. A theoretical cosmologist knows no more about ecology than any other competent outsider" (Osborne et al. 2022).

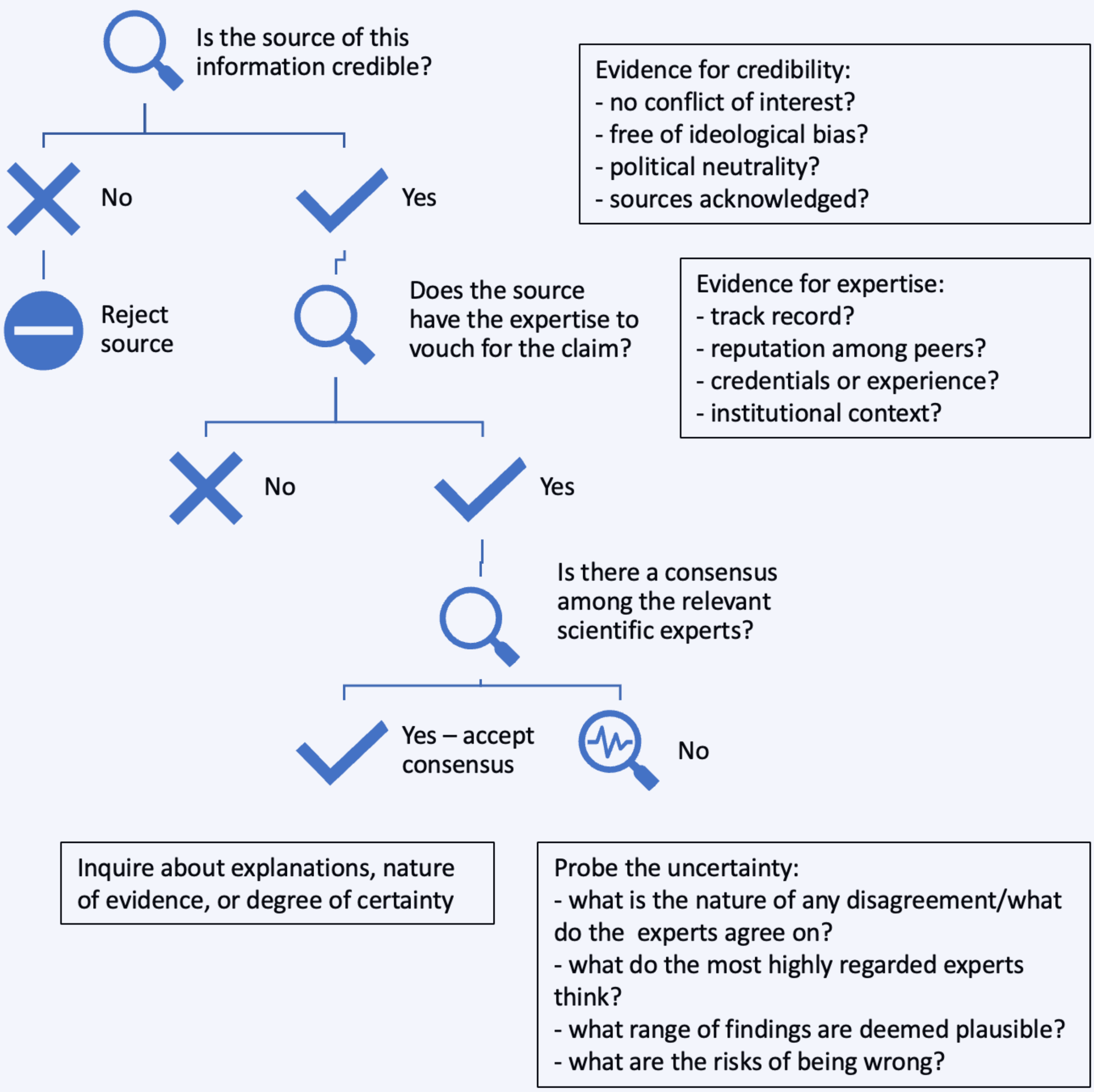
In recent weeks, various experts have appeared on social media commenting on the Russian invasion of Ukraine. It has often been easy to deduce from their statements which side they represent. In times of conflict, it is therefore necessary to take a more cautious and prudent approach than usual to various news reports and expert opinions. It is important to find out who is representing what, what evidence the information is based on and what the real expertise of the person making the statement is on the issue in question.

How to evaluate a scientific claim?

Scientific information must go through a number of processes to ensure that it is reliable. Openness, critical debate and peer review drive research forward. Science is self-correcting. Interpretations of research data are modified and refined as new knowledge emerges. Research builds on knowledge built up over decades, if not centuries.

Scientific knowledge is our best current understanding of things. It is not anyone's opinion or personal experience, but the result of a systematic process. It can change as new research findings and understanding develops. That's why researched science is worth more than opinions!

A decision tree for evaluating scientific information


Is the source of this information credible?
No
Yes
Reject source
Does the source have the expertise to vouch for the claim?
No
Yes
Is there a consensus among the relevant scientific experts?
Yes – accept consensus
No

Evidence for credibility:
- no conflict of interest?
- free of ideological bias?
- political neutrality?
- sources acknowledged?

Evidence for expertise:
- track record?
- reputation among peers?
- credentials or experience?
- institutional context?

Inquire about explanations, nature of evidence, or degree of certainty

Probe the uncertainty:
- what is the nature of any disagreement/what do the experts agree on?
- what do the most highly regarded experts think?
- what range of findings are deemed plausible?
- what are the risks of being wrong?

Source:: Osborne, J., Pimentel, D., Alberts, B., Allchin, D., Barzilai, S., Bergstrom, C., Coffey, J., Donovan, B., Dorph, R., Kivinen, K., Kozyreva. A., Perkins, K., Perlmutter S., Wineburg, S. (2022). *Science Education in an Age of Misinformation*. Stanford University, Stanford, CA.

Figure: A schematic overview of the approach we think needs to be taken to evaluating scientific claims on the internet (Osborne et al, 2022).

When faced with a science-based claim, it is worth finding out whether the person/organisation making the claim has a conflict of interest. Are there economic, religious or political interests at stake? If so, it may be a form of paid advertising and the results should be treated with suspicion. For example, the tobacco industry and fossil fuel companies have used experts on their payrolls to disseminate information that benefits them.

If there is no conflict of interest, the following questions should be asked:

- Does the individual/organization have relevant expertise?
- What is the standing of the author within the scientific community?
- Do they have a record of integrity?
- Does the author have the appropriate credentials or other relevant experience?
- Is there a strong scientific consensus among experts? If not, what do the majority of scientists think?
- How certain of the claims is the scientific community?
- Has the finding been vetted by similar experts and to what degree?

It is also worth pausing to consider the potential benefits and risks involved. For example, during the coronary period, we have had to make personal choices about following expert advice – for example, about taking COVID-19 vaccines, wearing masks, adhering to the length of quarantine periods and the reliability of home tests.

Where to find reliable information?

Reliable background information can be obtained in Finland in accordance with Faktabaari's editorial policy, depending on the subject, for example

- **from public authorities – reports, surveys, studies. In Finland, as in other Western countries, much of this information is available in public databases.**
- **legal sources – legal acts and their preparatory material, court cases.**
- **statistics – statistics exist for almost all information that can be expressed in numbers.**
- **research – research publications in the field, research institutions, researchers.**

To obtain an answer in the English-speaking world Wikipedia is a good place to begin. The websites of major scientific institutions, such as National Academies of Science[4] (www.nap.edu), and long-established news media are also reliable sources of information.

Fact-checkers in different countries have interesting fact-checking websites where you can learn how fact-checkers check the accuracy of various claims and the authenticity and originality of images and videos, for example. EDMO's fact-checking community[5] has an updated list of reliable European fact-checking organisations.

It is also worth checking out the report "Science Education in the Age of Misinformation"[6] for a more in-depth look at the topic.

[1] Osborne, J., Pimentel, D., Alberts, B., Allchin, D., Barzilai, S., Bergstrom, C., Coffey, J., Donovan, B., Kivinen, K., Kozyreva. A., & Wineburg, S. (2022). Science Education in an Age of Misinformation. Stanford University, Stanford, CA https://sciedandmisinfo.stanford.edu/

[2] CoronaVirusFacts Alliance, Poynter, https://www.poynter.org/coronavirusfactsalliance/

[3] Osborne, J., Pimentel, D., Alberts, B., Allchin, D., Barzilai, S., Bergstrom, C., Coffey, J., Donovan, B., Kivinen, K., Kozyreva. A., & Wineburg, S. (2022). Science Education in an Age of Misinformation. Stanford University, Stanford, CA https://sciedandmisinfo.stanford.edu/

[4] National Academies https://nap.nationalacademies.org/

[5] EDMO Fact-checking community https://edmo.eu/fact-checking-community/

[6] Osborne, J., Pimentel, D., Alberts, B., Allchin, D., Barzilai, S., Bergstrom, C., Coffey, J., Donovan, B., Kivinen, K., Kozyreva. A., & Wineburg, S. (2022). Science Education in an Age of Misinformation. Stanford University, Stanford, CA https://sciedandmisinfo.stanford.edu/

13. Algorithmic awareness - the challenges created by artificial intelligence

HARTO PÖNKÄ, INNOWISE

What are algorithms?

Today, the concept of algorithms is mainly associated with programming and the functionalities of web services and applications. An algorithm, however, is originally a mathematical concept. An algorithm, in general, still means essentially the same thing: it is a series of steps to solve a problem or solve a task.

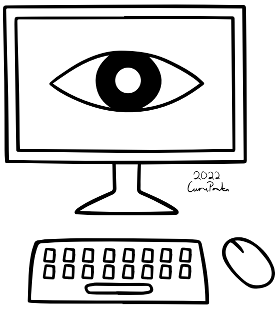
Algorithms are usually thought to work automatically, but originally algorithms were manual, i.e. performed by humans. For example, methods taught in primary schools to solve an equation by multiplication by an integer or by a division angle. Similarly, recipes in a cookbook are algorithms on how to prepare delicious dishes from certain ingredients following certain steps.

An algorithm is characterised by the fact that it uses an input such as starting elements or data to produce the desired result. The desired outcome is determined by the creator of the algorithm. In programming, this is referred to by the concepts of input and output, between which the actual execution of the program takes place.

Computer programme algorithms

The most common algorithms used by computers are, for example, the various file formats used to store and compress images, sounds and videos. For example, a digital photograph can be compressed to a fraction of its physical file size using the JPEG compression algorithm. Algorithms are also used when live video is transmitted over a network to viewers, or when Internet servers deliver a particular web page to a user who has typed its address into his browser.

Sometimes the output data, as well as the measures and results of algorithms are very complex. The complexity is usually related to the fact that the output data used by the algorithm consists of a large amount of previously collected data, or a large number of different variables or data points are used to perform a single task.



For example, the weather in a particular area can be predicted using previously collected data such as temperature, precipitation, wind, barometric pressure and statistical models based on observations. However, today's weather forecasting models are based on virtual modelling of the area to be forecast, which simulates the real atmospheric phenomena. Algorithms using such modelling are based on a mirror image of the real world.

Digital twins and recommendation systems

When algorithms are used to predict and influence human behaviour, this is sometimes referred to as a digital twin. It refers to a set of data collected about a person and their activities, and the combination of data from different sources. For example, online advertising networks and recommendation algorithms used by social media content streaming systems aim to provide each user with the most appropriate option based on the data available.

The recommendation systems aggregate data collected on users and on what is recommended. The best-known recommendation system is Google's search engine. Google's search was originally based on the PageRank algorithm, the idea being that the value of each web page is measured by how many other websites link to it. At the same time, the PageRank value is influenced by the PageRank values of the linking websites themselves, as well as the correspondence of the topics to the target page of the links.

PageRank is currently just one of many algorithms used by Google search. Since 2004, Google's search results have been influenced by data collected from users to personalise the search results, i.e. to recommend different web pages to different users. By 2010, Google reported using more than 250 different variables to personalise search results.

Today, Google search results are influenced by a user's age, gender, family, occupation, hobbies, location, online shopping, travel, interests and online history, among other things. Google's recommendation algorithms are not limited to search results, but are primarily used in Google's advertising system to select ads that are relevant to users. It will come as a surprise to many that recommendation algorithms also select the news that users see, for example in the news view on Android.

AI algorithms

When an algorithm uses machine learning or some other artificial intelligence technique, it is called an AI algorithm. Machine learning means that the algorithm does not give the same result every time, but is trained by constantly collecting new data, so that it "learns" to improve its result time after time.

The most familiar example of a learning recommendation algorithm is probably the YouTube algorithm, which suggests to users which videos to watch next. YouTube's suggestions are influenced by previously viewed videos and other data collected by Google, as well as data related to potential suggested videos, such as their topics and average actual viewing times. But instead of only suggesting new videos related to the topics of previously viewed videos, YouTube's algorithm also suggests videos on topics and channels that the user has not yet viewed.

For YouTube's AI algorithm, each video suggestion is like a trial balloon thrown to the user, from which the algorithm tries to learn new information: in this case, which video topics are of interest to the user and which are not. A similar type of data collection is used by a number of social media services such as Facebook, Instagram, Twitter and Spotify.

Despite efforts to develop algorithms that take into account a wide range of user interests, user activity still tends to lead to algorithms that provide one-sided recommendations on narrow topics. For example, if you repeatedly click on posts on Facebook and Instagram on the same topic, you will continue to see more and more of the same type of content. This is called algorithm bias.

In AI algorithms, bias can also be caused by the training materials originally used in machine learning. For example, the Google Translator algorithm used to translate a personal pronoun in different occupations into "she" or "he", depending on the occupation. Google was even accused of discrimination because of this, even though it was the type of material that had been available for training AI. Today, Google Translator gives two different options for such translations.

Facebook algorithms and emotions

Of all social media services, Facebook has made the greatest effort to harness users' emotions in its news feed algorithm. Liking publications has been a part of Facebook's functionality almost since the service's inception. Emotions were really harnessed in 2016, when Facebook launched the emoji reactions "love", "haha", "wow", "sad" and "angry".

Prior to the introduction of these emoji reactions, Facebook had conducted a practical experiment to see how different posts affected users' actions and emotions. The study found that positive posts caused positive emotions and negative posts caused negative emotions. Using the data collected from the emoji reactions, Facebook's algorithm was able to select posts for users' news feeds based on their emotional state. For example, if a user frequently clicked on wow reactions, they would then see more posts that had received a lot of wow reactions.

From 2017, the value of emoji reactions in the news feed recommendation algorithm was increased to five regular likes. Companies and others studying the algorithm soon found that by making highly emotive posts, they rose to the top of users' news feeds as a result of the algorithm. This kind of activity, which exploits human behaviour and the algorithms of social media services, is called social media optimisation.

A particularly effective emotion on Facebook proved to be the generation of indignation and anger. With more than two billion users, algorithm changes play a major role: they control the type of posts users see, on the one hand, and the type of posts made by influencers, on the other. So when the algorithm seemed to reward incitement to anger, many publishers started to act accordingly.

The high volume of hate content is one of the reasons why Facebook has been widely criticised for many years. Facebook soon ended up lowering the value of hate emoji in its algorithm: first to four likes in 2018, one and a half likes in 2020 and finally to zero likes in 2021 after thousands of documents leaked by ex-Facebook employee Frances Haugen revealed the above information.

Do algorithms have too much power?

Emerging data on Facebook's algorithms has fuelled the debate on whether algorithms have too much power over users of online services. The fact is that algorithms do have an impact on the behaviour of their users. Most often, this influence is seen in the content that is recommended to users.

At the same time, it has been rightly questioned whether even the algorithms' authors always have control over how algorithms work. AI algorithms in particular sometimes produce results that are difficult to predict in advance.

Facebook's algorithms are very complex: it has boasted of using up to more than 10 000 data points to choose what to show each user. With so many different factors influencing what users see, it is not easy to manage the whole.

A 2021 document leak revealed that when Facebook introduced emoji reactions, the company had sought to create a mechanism to prevent hate-face emojis from having a disproportionate impact on the visibility of posts. The algorithm had been programmed to halve the visibility score of a post that caused anger in certain situations. However, due to other variables affecting the algorithm, there was no upper limit to the visibility score, so that at worst, publications that garnered "angry" reactions would receive unlimited visibility scores.

Tellingly, while Facebook's news feed algorithm gave disproportionately high visibility to some posts containing disinformation, hate speech and clickbait, for example, the company's own moderators sought to weed out the same types of content. However, Facebook did not have enough moderators to remove all the damaging posts that the algorithm elevated to the top of the news feed.

Should the algorithms be published?

An often-heard demand is that online giants such as Google, Facebook and Twitter should publish the principles behind their algorithms. These claims relate mainly to the alleged harmfulness of algorithms, such as their attempt to maximise the time users spend on social media, and algorithms' problems in preventing the spread of messages containing incorrect information and creating adversariality.

The business of online and social media services is usually based on advert monetisation, i.e. users clicking on adverts targeted at them. This is of course encouraged by the need to ensure that they stay as long as possible. It is therefore clear that algorithms are tuned to do just that, even if the services do not express it on their own. On the other hand, many studies show that a long time spent online and on social media services is not conducive to users' well-being. The interests of the companies running the services and the users do not coincide in the operation of the algorithms.

Online giants have been reluctant to publish information about algorithms, citing commercial confidentiality and the fact that publishing algorithms would lead to their increasing misuse and manipulation by publishers and other online influencers. This argument is justified, as there has been a constant race to develop and exploit algorithms. On the other hand, it could be argued that it is the responsibility of the web giants to develop algorithms that are good enough to detect and prevent attempts at manipulation.

In the debate on the openness of algorithms, it is often forgotten that some of the algorithms' operating principles have already been published. Google, for example, provides a comprehensive, and at the same time, general description of the factors influencing the results of its search engine. Google has also published a nearly 200-page guide online for anyone to read, for use by its own search result evaluators. In addition, Google has produced a number of tools for website developers to test and improve the performance of their websites and, at the same time, their ranking in Google's search results. Google can be said to be a good example of algorithmic transparency. On the other hand, we have no way of knowing what Google is not telling us.

It is easy to be sceptical about how many users of web services would bother to read hundreds of pages of documents describing the detailed workings of algorithms. In principle, however, this is an important issue. If the principles of how algorithms work were published, awareness would be raised, mechanisms that have been hidden until now would come to light and researchers would be able to study them in much greater depth. For users' privacy, the most important thing would be to know in what ways their personal data are used in the algorithms. New EU legislative packages are therefore in the process of requiring greater transparency from online data providers on how algorithms work.

DigComp 2.2. examples

Knowledge	3. Aware that search results, social media activity streams and content recommendations on the internet are influenced by a range of factors. These factors include the search terms used, the context (e.g. geographical location), the device (e.g. laptop or mobile phone), local regulations (which sometimes dictate what can or cannot be shown), the behaviour of other users (e.g. trending searches or recommendations) and the user's past online behaviour across the internet.
	4. Aware that search engines, social media and content platforms often use AI algorithms to generate responses that are adapted to the individual user (e.g. users continue to see similar results or content). This is often referred to as "personalisation". (**AI**)
	19. Aware of potential information biases caused by various factors (e.g. data, algorithms, editorial choices, censorship, one's own personal limitations).
	21. Aware that AI algorithms might not be configured to provide only the information that the user wants; they might also embody a commercial or political message (e.g. to encourage users to stay on the site, to watch or buy something particular, to share specific opinions). This can also have negative consequences (e.g. reproducing stereotypes, sharing misinformation). (**AI**)
	56. Aware that everything that one shares publicly online (e.g. images, videos, sounds) can be used to train AI systems. For example, commercial software companies who develop AI facial recognition systems can use personal images shared online (e.g. family photographs) to train and improve the software's capability to automatically recognise those persons in other images, which might not be desirable (e.g. might be a breach of privacy). (**AI**)
Skills	27. Able to recognize that some AI algorithms may reinforce existing views in digital environments by creating "echo chambers" or "filter bubbles" (e.g. if a social media stream favours a particular political ideology, additional recommendations can reinforce that ideology without exposing it to opposing arguments). (**AI**)

References

Google, 2022, Miten tulokset luodaan automaattisesti, https://www.google.com/intl/fi/search/howsearchworks/how-search-works/ranking-results/
Google, 28.7.2022, Search Quality Evaluator Guidelines, https://static.googleusercontent.com/media/guidelin's.raterhub.com/fi//searchqualityevaluatorguidelines.pdf
Pönkä, H., 31.10.2021, Infografiikka: Facebookin viha-reaktio ja algoritmin muutokset, https://harto.wor'press.com/2021/10/31/infografiikka-facebookin-viha-reaktio-ja-algoritmin-muutokset/
The Washington Post, 26.10.2021, A whistleblower's power: Key takeaways from the Facebook Papers,
https://www.washingtonpost.com/technology/2021/10/25/what-are-the-facebook-papers/
Wikipedia, 2022a, Luettelo algoritmeista, https://fi.wikipedia.org/wiki/Luettelo_algoritmeista
Wikipedia, 2022b, Tekoäly, https://fi.wikipedia.org/wiki/Teko%C3%A4ly
Wired, 22.2.2010, Exclusive: How Google's Algorithm Rules the Web, https://web.archive.org/web/20110612022158/http://www.wired.com/magazine/2010/02/ff_google_algorithm/2
Yle, 19.12.2016, Näin sinua ohjataan Facebookissa ja internetissä, https://yle.fi/aihe/artikkeli/2016/12/19/nain-sinua-ohjataan-facebookissa-ja-internetissa
Yle, 12.2.2020, Hölkkääjä päätyy ultrajuoksuvideoihin ja kasvisruuan ystävä vegaanisisältöihin – Youtuben algoritmin tehtävänä on katsojan koukuttaminen,
https://yle.fi/aihe/artikkeli/2020/02/12/algoritmin-tehtavana-ei-ole-totuuden-etsiminen-vaan-ihmisten-pitaminen-sivuilla

14. Digital footprint and privacy in online services

HARTO PÖNKÄ, INNOWISE

Privacy is one of the most important fundamental rights in the digital age. It is based on national laws and European Union regulations such as the EU General Data Protection Regulation (GDPR) on the one hand, and international treaties and the UN Declaration of Human Rights on the other.

Privacy is primarily about the protection of private life, home and communications, but in the digital environment it is more appropriate to talk about the information relating to a specific person, i.e. personal data. This is the data that is stored on the digital devices and services we use, such as search engines and social media platforms. Such data is called a digital footprint.

To be a fully informed actor in the digital environment and to be able to manage your privacy in it, you need to know how the different devices and services used collect information about users. It is also important to be aware of the privacy concerns of other users, so as not to unintentionally infringe their privacy in the digital environment.

The digital footprint can be divided into active and passive digital footprints. An active digital footprint is information that a user has consciously added or otherwise generated on the web. Passive digital footprint is data collected by services without the user's knowledge.

The distinction between active and passive digital footprints poses a problem, as awareness of data collection depends on the user's knowledge. Nevertheless, it is a useful distinction to illustrate that often online and social media giants collect data without users' knowledge or in a way that requires specific digital information literacy skills to become aware of it. This chapter therefore aims to provide a basic overview of the most common methods and techniques of data collection.

To whom is it safe to share your information?

Online services and applications usually require you to create a user ID, i.e. register. Before creating a new account and providing your personal information, it is worth checking that the company running the service or application appears to be trustworthy and that the information you provide is secure. This can be assessed by looking for additional information and reviews from other users.

There are several misleadingly named apps and games, which have been created based on popular apps and games. These counterfeited applications have been created with the sole purpose of extracting personal data from users. It is therefore worth checking to make sure that the author of the app is genuine and to read other users' experiences. It is also advisable not to install apps from anywhere other than the official app stores. In the worst case, app downloads can contain malware and viruses that can steal information.

When registering the actual user account, it is wise not to provide any information other than the mandatory information. You may also want to consider whether it is worth telling online services your real date of birth or your name. If this information is not explicitly required by the terms of use, it is not wrong to provide fictitious information. Registration forms can be deliberately designed to try to get the user to provide as much information about himself as possible, even if it is not necessary for the use of the service.

Any unique information such as name, telephone number, email address and home address may be used to search for information from other sources.

It is good advice to use a secondary email address for registration.

For many online services, you can register using an existing user account such as Google, Facebook or Apple. These are also unique pieces of information that usually allow to aggregate information from elsewhere. If the service provider seems untrustworthy, it is better to be safe than sorry.

The use of online services and applications often generates personal and relevant content. Every post, like and comment accumulates data about us. In addition, social media services in particular allow us to communicate with other users. As a result, user accounts are constantly being targeted by fraudsters and other cybercriminals. It is always a good idea to use two-way authentication when logging in, as this provides good protection against hacking attempts.

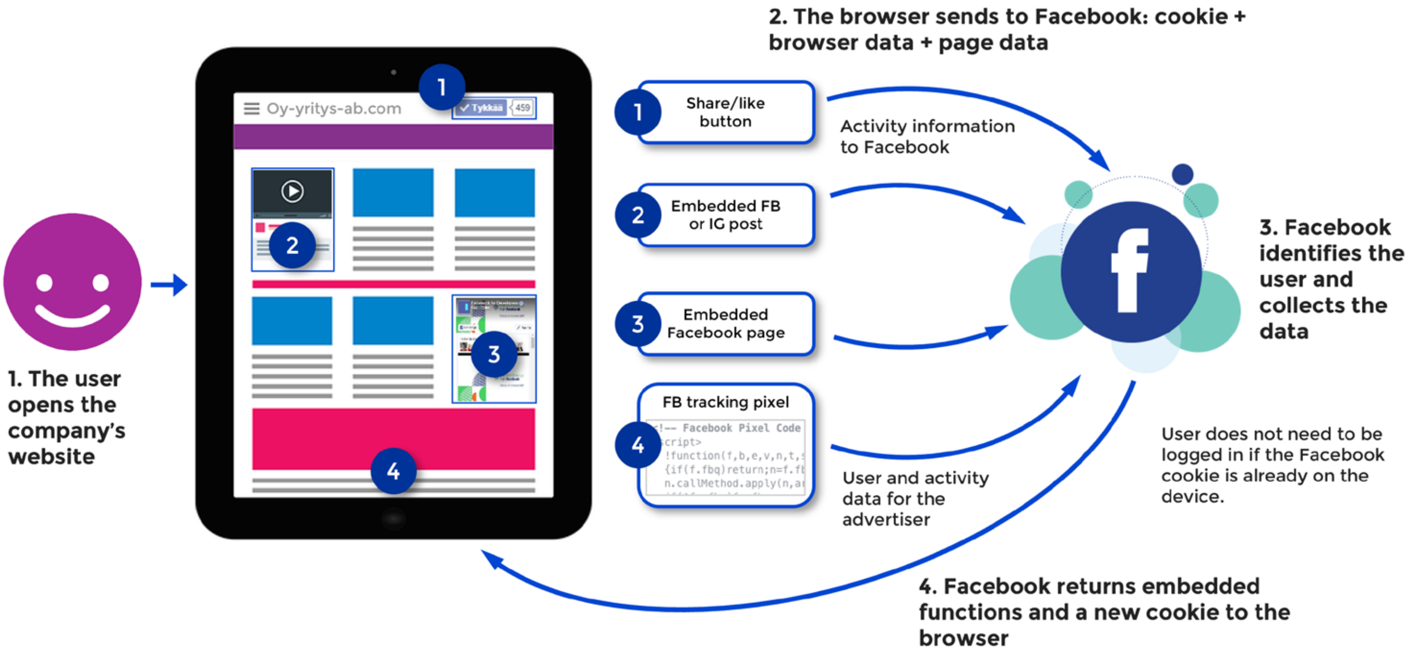
How do cookies work?

Online services and applications may store cookies, i.e. files containing information that they can use to track users, on users' devices. The use and retention periods of cookies should always be explained on the service. In the case of cookies that are not necessary for the functioning of the service, the user's consent must be obtained before cookies are used.

Examples of cookies that are essential are those used for logging in and for storing the choices made by the user. Non-essential cookies include cookies related to advertising, activity tracking and social media platforms. Non-essential cookies are typically related to the collection of data by various online services to gather information on users' activities and interests, i.e. profiling.

For example, when a user logs on to Facebook, a cookie stores information about his or her username. When on Facebook, the cookie is necessary so that the user does not have to keep re-entering their ID and password. However, it is often overlooked that the cookie remains on the device even after logging out of Facebook, unless the user explicitly clears the cookie.

Many social and online services can embed functionality on other websites. For example, a company can embed a Facebook like button, a Facebook page embed or Facebook tracking pixels on its website that can be used to target Facebook ads to users who visit the site. When a user visits such a site, the cookie previously stored on the device is automatically sent to Facebook when the embedded functionality is loaded from the Facebook server. The user does not need to be logged into Facebook at the same time if the cookie has been previously stored on the device. Facebook will be able to read the content of the cookie and identify the user based on that content. At the same time, Facebook will know which website the user is on.



```
<!-- Facebook Pixel Code
<script>
 !function(f,b,e,v,n,t,s
 {if(f.fbq)return;n=f.fb
 n.callMethod.apply(n,ar
```

2. The browser sends to Facebook: cookie + browser data + page data
1. The user opens the company's website
Oy-yritys-ab.com
✓ Tykkää
459
1
2
3
4
1 Share/like button
2 Embedded FB or IG post
3 Embedded Facebook page
4 FB tracking pixel
Activity information to Facebook
User and activity data for the advertiser
3. Facebook identifies the user and collects the data
User does not need to be logged in if the Facebook cookie is already on the device.
4. Facebook returns embedded functions and a new cookie to the browser

Figure: How do cookies work? Facebook as an example

Facebook is able to continuously track user activity through cookies on millions of websites. In practice, this gives Facebook data on what users are interested in, what products they have recently viewed in online shops and so on. This data is used to target ads on the Facebook and Instagram ad platform.

Google and many other online companies also use cookies to profile users. A common use of cookies is so-called 'remarketing', where a user is shown an ad for the same product they have previously viewed in an online shop.

When visiting different websites, we now have to constantly respond to requests for permission to use cookies. It is worth remembering that only non-essential cookies are asked for, which are usually of no benefit to the user, but can be reasonably considered harmful and privacy-reducing. At worst, a single website can send data about a visit to dozens of data collection companies through cookies and other tracking functions. Online services in the EU must offer users the option to opt-out of non-essential cookies at the point of entry.

Cookies are not the only way in which online services can store trackable data on a user's device. Another commonly used technology is local storage in the browser. Again, the service needs the user's consent to use it. In addition, at least Google is developing a technology to replace cookies.

Is it worth sharing the location?

Online services and applications may ask users for permission to track their location. For example, a news site may give a reason to show the user a weather forecast based on their location, when in fact the location is also used to personalise content and ads.

In Google's search engine and ad network ads, location tracking is used to infer user interests. Google explains the use of location as follows: 'if you have enabled location tracking and frequently visit ski resorts, you may later see a ski ad in a YouTube video'. However, this use of location data to target ads can easily be avoided by not allowing Google apps to track your device's location.

The GPS location of a device is not the only way to track users. More coarse, or less precise, localisation can be done, for example, using data from public Wi-Fi networks or the IP address of the user's network connection. Even this type of location can be avoided by using a VPN to connect to the internet.

In addition to online services, many mobile phone applications request location access. It is worth assessing whether there are functions in the application where location is of real use and deciding whether to allow it to track your location. You should also check your phone settings to see which apps you have given location tracking permission to.

Device and browser identifiers

When online services and applications are used on different devices and web browsers, they can be assigned different unique identifiers. For example, Google and Apple have developed advertising identifiers for their advertising systems, which are used to identify users and target ads in mobile applications. The importance of these identifiers is that they can be used to link a specific device such as a mobile phone or tablet to a specific person in the same way as, for example, an email address, phone number or address.

Once an identity has been discovered through one application, it can then be identified in other applications used on the same device. There are numerous data businesses that aggregate and sell identity and user data to identify users.

Web browsers do not have the same unique advertising identifier system as mobile devices. This was not 'necessary' in the past because the use of cookies was very little regulated in the past and in many cases made it easy to identify the user.

As users have become more restrictive in their use of cookies, data collection companies have developed different browser identifiers. These tags are based on differences in browser configurations such as settings, installed fonts and browser plug-ins. They are called browser fingerprints, which describes well their purpose, i.e. to identify the user based on the browser they use. For example, the TikTok application is known to have used browser-specific image and audio tags in its web service, which can be used to identify the user even if he or she is not logged in to the service.

Don't share your contact information with advertisers

When you use Instagram, Snapchat, TikTok or other apps, you may receive a request to allow your address book's contact information to be used. Usually, the reason given for the request is that it would allow you to find and connect with your friends who use the app. However, it is not advisable to give permission, as the request will apply to all your contact information, and it may also be used for other purposes. So it's worth making the effort to find the friends you want to contact through the app yourself.

Contact information is the same information that online and social media services use to target ads and content, as any other information they collect about you. It is network data that tells you who is connected to whom. Even if we do not share our contact information with social media services, they can know about our network of friends based on the contact information shared by others. For example, Facebook and Instagram can use it to suggest new friends and followers.

Sometimes contact information is used in unexpected situations. For example, Google says it uses contact information in its news recommendation algorithm. Most likely, Google assumes that we are interested in the same topics as our friends whose news reading is similar to ours.

Tracking in "dark" social media

Tracking interactions between users is easy for social media services as long as it happens on their own services. It's clear that Instagram, for example, tracks which users' posts we react to and uses the data it accumulates in its news feed algorithm.

In contrast, tracking user activity on applications outside of social media is more difficult for them. Increasingly, links to social media posts and news, for example, are shared on so-called dark social media, which refers primarily to messaging apps such as WhatsApp, Snapchat and Yodel.

Normally, the web service provider has no way of knowing who has shared the link outside the service and to whom. However, many online and social services have developed techniques to attach identifiers to links, which allow them to know who originally shared the link. These tags can, for example, be in the form of a # code following the actual link address or so-called shortened links. A number of link aggregation services allow link sharing to be tracked.

When a shared link is opened, web services know who shared the link from its tag. In addition, web services can often identify the users who have opened the link, for example by using cookies or other means described above. As a result, they will also gain information about link sharing via the 'dark' social media and about the networks between users.

How can data be deleted?

The easiest way to delete data accumulated on online services and applications is to simply delete the publications you have made, clear the location or browsing history stored in the service, delete the contact information you have transferred or delete your entire user account. Usually, the terms of use include a condition that if a user deletes his data, the service provider is not allowed to keep it afterwards.

Many online services and applications allow you to control what information it stores about your activities and how it is used. These options can be found in the settings of the user account. For example, the Google user account settings allow you to opt out of personalisation of ads, so that the data stored in your account is not used to target ads.

The EU's General Data Protection Regulation gives users many rights when using services in the EU. Where the processing of personal data is based on the user's consent or acceptance of the terms of use, i.e. a contract, there are at least the following rights that users can invoke:

- **The right to be informed about the processing of personal data**
- **Right of access to his/her personal data**
- **Right to rectify inaccurate data**
- **Right to delete personal data / right to be forgotten**

DigComp 2.2. examples	
Knowledge	2. Aware that online content that is available to users at no monetary cost is often paid for by advertising or by selling the user's data
	31. Aware that many applications on the internet and mobile phones collect and process data (personal data, behavioural data and contextual data) that the user can access or retrieve, for example, to monitor their activities online (e.g. clicks in social media, searches on Google) and offline (e.g. daily steps, bus rides on public transport).
	34. Aware that sensors used in many digital technologies and applications (e.g. facial tracking cameras, virtual assistants, wearable technologies, mobile phones, smart devices) generate large amounts of data, including personal data, that can be used to train an AI system. (AI)
Attitude	13. Values tools designed to protect search privacy and other rights of users (e.g. browsers such as DuckDuckGo).
	14. Weighs the benefits and disadvantages of using AI-driven search engines (e.g. while they might help users find the desired information, they may compromise privacy and personal data, or subject the user to commercial interests). (AI)

15. Everyday use of digital services generates digital power

TIINA HÄRKÖNEN, SITRA

The massive data collection that is penetrating every area of our private lives originates from a time when there was no related legislation, as well as in contracts we didn't know we had made. The collection of personal data has become so commonplace that the temptation to ignore its consequences is great; since everyone else's data is also collected, can't we just disappear into the crowd?

However, the tools of the biggest technology and platform companies allow them to pick an individual out of any crowd, and a profile built from the data can be used to examine each of us in detail. As long as the company or organisation collecting the data is not malicious, or the country you live in respects individual rights, it can be difficult to identify the problem.

However, privacy is a value in itself. It is important for the development and well-being of every human being and enables free and critical thinking. Creativity and using one's critical mindset require a space where one can feel safe and truly be oneself.

Big tech companies and the players in the digital advertising ecosystem offer us a purpose-driven narrative in which the storing and collection of all digital traces - visible or invisible, active or passive - is absolutely necessary to 'keep the internet freely available'.

The narrative also includes, as an integral part, that we pay for 'free' services with our own data. For the explanation to be at all meaningful, we should all have a clear understanding of the terms on which we have agreed, when this has happened, and the real value of each imaginary 'data transaction'. In order to pay, we need to have a genuine understanding of what currency is involved and what its value is in relation to other currencies, and what its use can mean in terms of losses and gains – and to whom.

To understand the mechanisms of the personal data economy, it is worth considering what kind of data is being collected about us and in what situations. Sitra has carried out a two-fold study on this issue by looking at data collection in the everyday lives of very different people.

In 2019, six ordinary Finns used test mobile phones to track their own data movements in the services they use in Sitra's Digitrail survey project[1]. This revealed in tangible terms the large-scale operation of data collection ecosystems, the countless different entities that process our data and the huge amount of data that is generated about us and stored for unknown companies to use.

In 2021, Sitra continued its research with its partner Hestia.ai, but this time focusing on the data of European policy makers and political influencers and the digipower that arises from its collection. The Digipower investigation[2] aimed to understand whether data and profiling can also be used to influence societal decision-making.

Unfortunately, despite the time difference, both projects also found that datagiants are not complying well with European data protection legislation. It is therefore important that people themselves have sufficient agency to ensure that fundamental individual rights do not have to be compromised online.

Examples of data collection and use

We compiled three examples of actors that collected data on policy makers. Local companies also share data via cookies with major international Big tech companies, which are constantly increasing their huge databases and data on individuals.

Atte Harjanne MP and media company
Harjanne's data revealed that the media company Sanoma has built a very precise profile of Atte Harjanne's interests. The company also has information on his purchasing power, right down to the devices he uses. Gambling was identified as an area of interest for him, as Harjanne has had to follow the industry for his job.

Jyrki Katainen, President of Sitra, and the retail sector
The data collected by a major retail chain, the K Group, formed a 172-page document on Katainen. Most of it was shopping and other data accumulated during the relationship between the retailer and him. Some of this data goes to Google through, among other things, Google Analytics. When Katainen searched the store's app for a recipe for spaghetti carbonara, the data was sent to Google.

Miapetra Kumpula-Natri, MEP, and the home electronics chain
Information about Kumpula-Natri's purchase at Gigantti, the flagship store of the home electronics chain, was sent from the company to both Google and Facebook.

Clicking on a link in the chain's electronic marketing mail on the phone revealed the location of the holiday home where she stayed, even though the location service was not used. Gigantti later confirmed that it recognised the device's IP address and used it to determine the location. In this case, the test person did not identify a situation where they had given permission to track their location. By accepting Gigantti's website cookie, the customer was also accepting 231 cookie partners, including the 10-year cookie from the Russian company Yandex.

Steps towards data sovereignty

Of course, individual rights also apply to digital services. We all have a right under European law not only to privacy but also to our own data. We must also remember that it is the responsibility of adults to safeguard the privacy of children.

It is possible that if rights were more widely and actively demanded, the international data giants would also have to genuinely reform their practices and the regulatory authorities would get away with less. Now, the exercise of rights is for the chosen few and the processing times for complaints to data protection ombudsmen, for example, are disproportionately long.

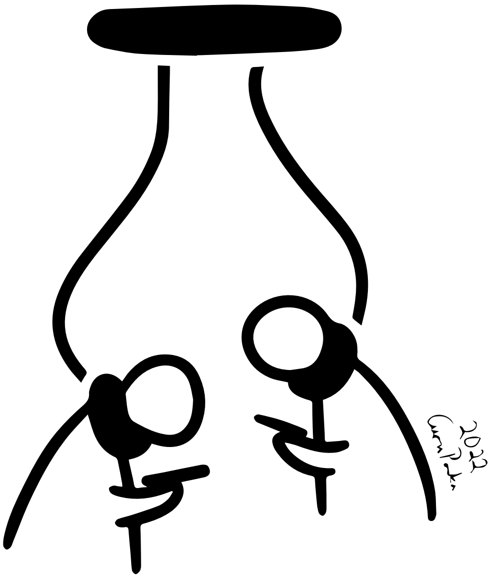
Digiprofile test[3]

Sitra has worked with experts in the field to develop an easy and fun digital behaviour assessment tool for children, young people and adults alike. A first step towards digital - or personal data - empowerment and self-determination could be to take the Digiprofile Test. The test assesses three different things: knowledge, attitudes and online actions. The result is a personalised digital profile and personalised tips on how to manage your data.

Sitra has worked with experts in the field to develop an easy and fun digital behaviour assessment tool for children, young people and adults alike. A first step towards digital - or personal data - empowerment and self-determination could be to take the Digiprofile Test. The test assesses three different things: knowledge, attitudes and online actions. The result is a personalised digital profile and personalised tips on how to manage your data.

At the time of writing, there are more than 28,000 test takers, the majority of whom are Finnish. The results are reasonably clear: of all age groups, people under 19 are the least critical of digital service providers. Not only do children and young people trust digital services far more than other age groups, they are also the least likely to act to secure their own rights to privacy and the least aware of the risks of online services.

Both exercising rights and protecting privacy require digital skills, which were already identified as new civic competences in the introduction of this guide. The key to digital agency is the broad digital literacy and competences of children and young people. But these are also needed for all other age groups and citizens.



[1] Digiprofile test, Sitra, https://digiprofiilitesti.sitra.fi/
[2] Tracking Digipower, Sitra, https://www.sitra.fi/en/publications/tracking-digipower/
[3] https://digiprofiletest.sitra.fi/

16. Digital civic skills are a key tool for defending democracy

How to harness the power of the web to support and renew democracy?

JUKKA VAHTI, SITRA

Digitalisation and the platforms and networks it enables have rapidly revolutionised the way we produce, acquire, disseminate and use information. With the development of technology, the arena of the public sphere has become much more complex and difficult to navigate than before. Whereas the traditional mass media used to be the gatekeepers of the public sphere, with at least in principle a great deal of influence over what and how social debate took place, they have now been joined and sometimes overtaken by a myriad of interlocking networks, some visible and some not.

Since the invention of the printing press, the technological revolution in communication has led to major changes in power relations. This shift in power is happening now with the internet and social media. Recent years have shown that what happens in the digital world has very concrete practical consequences. Indeed, in ten years we have come a long way from the 'techno-utopia' of the Twitter revolutions which took place during the Arab Spring in the early 2010s, through the Brexit vote in the UK, the takeover of the US Capitol and the proliferation of disinformation campaigns, to 'techno-pessimism' and the so-called information wars.

The rapid changes in the media landscape seen in recent decades have given rise to a plethora of new ways of influencing society and new forms of digital power. This has blurred the boundaries between decision-maker and citizen, influencer and influenced, and sender and receiver of messages. In recent years, Sitra's megatrend list[1], among others, has referred to this phenomenon as the rise of relational power – networks and interaction will be increasingly significant in the future. The phenomenon is complex, and one can rightly see both threats and opportunities in it. For instance, a troll spreading confusion through disinformation on social media uses network power in the same way as an active citizen organising online help for people fleeing war.

The same is true at the systemic level: digitalisation and various forms of network-enabled power can accelerate the development of society in a democratic or undemocratic direction. For example, in its report The Global State of Democracy: Building Resilience in a Pandemic Era[2], published at the end of 2021, the Stockholm-based International Institute for Democracy and Electoral Assistance (IDEA)[3] estimates that the covid pandemic widened the gap between democratic and non-democratic systems. For autocratic regimes, the pandemic provided a reason and a means to strengthen control over citizens. On the other hand, democratic regimes took a digital risk, for example to enable parliaments to function or elections to be held in emergency situations.

From a global perspective, IDEA's message is in line with that of numerous other democracy reports published in recent years: the lifeblood of democracy in the world has continued to shrink in recent years. Finland and other Nordic countries are not immune to this development. Here too, for example, online harassment and intimidation have been shown to reduce people's willingness to participate in social debate or to take a public stand as an expert on sensitive issues. Or to stand for election.

In a survey Well Said campaign[4] commissioned by the Finnish Broadcasting Company YLE in 2021, 63% of Finns felt that the culture of public debate had taken a turn for the worse, and that public debate was not seen as inviting everyone to participate. Trust in democracy and in other people is also being eroded by new and non-transparent ways of influencing based on data and algorithms. Already in 2018, a Eurobarometer survey[5] found that 83% of Europeans considered disinformation a threat to democracy, 63% of young Europeans encountered fake news more than once a week and 51% of Europeans believed they had been exposed to disinformation online. There is no reason to believe that these phenomena have diminished in importance since then.

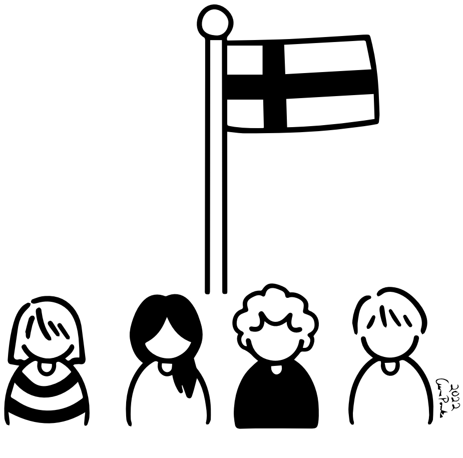
Broad participation as a resource for democracy

In spring 2022, Sitra launched a four-year project called Digital power and democracy[6], which aims to increase understanding of the nature of networked, digital power and find ways to harness that power - the power of the web - to reform democracy. The core tension that the DigiPower and Democracy project addresses is that our everyday lives have moved to digital environments faster than the structures and practices that traditionally sustain our democratic social order. This, in turn, leads to a discrepancy between policy rhetoric and approaches and our everyday experience.

Lowering existing barriers to social participation is therefore a key means of defending democracy. As noted, in digital environments, such barriers have been identified in various surveys and studies, both in Finland and worldwide. Disinformation, confusing content, cyberbullying and the polarising nature of social media platforms' algorithms impede meaningful public debate. Also linked to the same cluster of problems is the lack of transparency in the collection and use of data described in the previous article.

These obstacles pose a different threat to democracy than, say, military force or traditional cyber-attacks, against which various defences and 'walls' can be built. In the case of information warfare, on the other hand, the battle is over issues such as what is true and what we can trust. This question is at the heart of democracy, which is based on a sufficiently shared understanding of reality among different people and population groups, as well as on a desire for truth, i.e. the desire to know what is true and the ability to form an opinion on the basis of the information available.

Critical digital information literacy and, more broadly, digital civilisation are key to this. The ability to form opinions based on information is a prerequisite for participation in society. Social participation is important for both the individual and the democratic system, otherwise the human being, the main driving force of democracy and the ultimate purpose of the whole system, will remain a bystander. It is therefore important that the defense of democracy is not based solely on the construction of various physical or digital walls or the filtering of media content. That is when we run the risk of losing the very values we are trying to defend.



[1] Sitra's megatrends https://www.sitra.fi/en/articles/megatrend-3-relational-power-is-strengthening/
[2] The Global State of Democracy Report 2021 https://www.idea.int/gsod/
[3] IDEA https://www.idea.int/news-media/news/democracy-and-challenges-climate-change
[4] Hyvin sanottu: tutkimustulokset 2021, Yle, https://drive.google.com/file/d/1Fu86EW3_Nh9Rbocl2m_2wwVvtVCTVc2-/view
[5] Eurobarometer https://europa.eu/eurobarometer/surveys/detail/2183
[6] Digital power and democracy, Sitra https://www.sitra.fi/en/topics/digital-power-and-democracy/

Writers

Minna Aslama Horowitz is a Docent at the University of Helsinki, a researcher at the Nordic Observatory for Digital Media and Information Disorder (NORDIS), a Fellow at St. John's University, New York, and an Expert on Advocacy and Digital Rights at the Central European University, Vienna. She is also a member of the Think Tank of the Nordic Council of Ministers to address platformisation in the Nordics. Horowitz researches (public media) policies, digital rights, and media activism.

Pipsa Havula is a fact-checker and freelance journalist at Faktabaari. She has worked as a domestic and foreign news reporter for various newspapers since 2012. At Faktabaari, she has particularly focused on instructing readers on how to use fact-checking tools.

Tiina Härkönen is a Leading Specialist in Sitra's Democracy and Participation theme, Digital power and democracy project. She has had a long career in the corporate world working with data and information networks, in marketing, communications, and business development management positions. Tiina has worked mainly in the IT industry but joined Sitra in 2018 from a management and development role in customer and marketing analytics at Posti.

Carita Kiili is an Academy Research Fellow at the Faculty of Education and Culture, Tampere University where she leads the Educating for future literacies research group. She holds a title of docent in digital literacies at the University of Lapland. Kiili's research focuses on developing and testing methods to assess and support students' critical online reading skills.
Elsa Kivinen (MSc), Working as assistant on Faktabaari EDU's operations and projects, school visits, in-house text editing and translating, internal communications and some stakeholder relations in relation to projects.

Kari Kivinen, PhD, is an Education outreach expert at EUIPO. He has over 30 years of experience in international education. Since 2017 he has led the pedagogical development work at Faktabaari EDU digital information literacy service building on fact-checking methodology and co-authored and piloted the learning materials with fellow teachers around Finland and abroad. He is a member of the Commission expert group on tackling disinformation and promoting digital education. The author works for EUIPO and agency of the EU but the views expressed are purely personal and cannot be taken as being official statements of either the EU or the EUIPO.

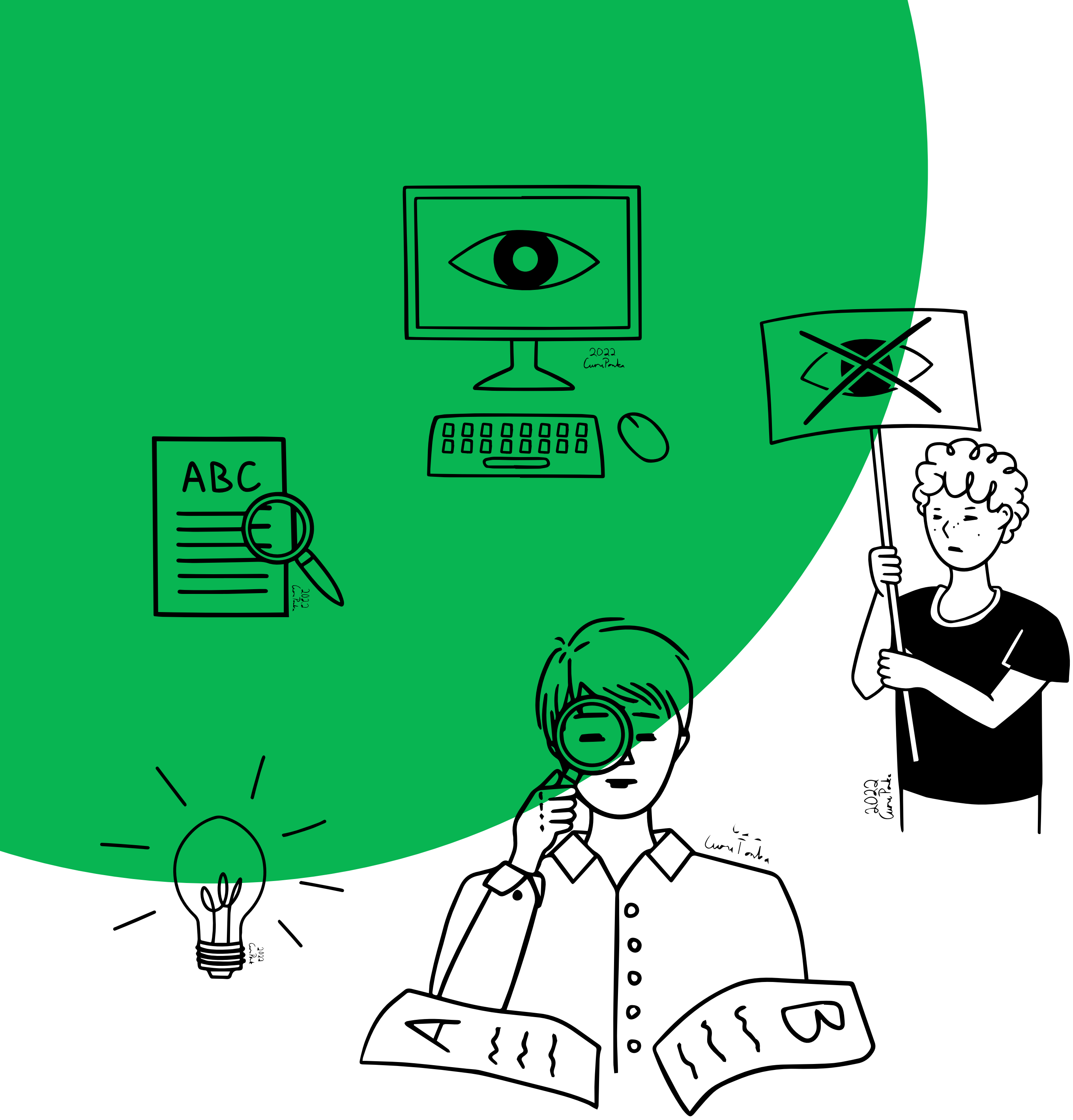
Joonas Pörsti is a foreign affairs journalist and doctoral researcher at the University of Helsinki. In 2018, he won the State Award for Public Information for the book Propagandan lumo (The Enchantment of Propaganda). He is Editor-in-Chef of Faktabaari.

Harto Pönkä (M.Ed.) has a broad background in e-learning pedagogy, media education, social media and data protection. He has been a trainer since 2008 and has published books and articles on social media. Pönkä provides training and analysis for companies, associations and public administrations. Pönkä works for his companies Innowise and Tweeps.

Mikko Salo is chair to Finnish transparency NGO Avoin yhteiskunta ry in charge of Faktabaari he founded in 2014 for fact-based public debate. He joined the 2018 European Commission's High-Level Group on Fake News and Online disinformation as an expert on fact-checking and media and information literacy. He continues as an independent member to the EC expert group on media literacy, with several advisory roles in national and international networks tackling digital information disorders. He is NewsBeez media start-up Co-Founder and EU Senior Advisor to LUT University management on EU research and innovation policy and digital affairs.

Jukka Vahti works as a project director in Sitra's project Digipower and Democracy, which is part of Sitra's Democracy and Participation theme. In his work, he focuses in particular on the challenges to democracy posed by the rapidly changing media environment, social media and dis- and misinformation, and on increasing understanding of the societal significance of data and digital power. Jukka was co-author of the report "On the trail of digital power - How data can be used to influence decision-makers and govern the world". Jukka was also co-author of Sitra's report Media-mediated social influence - The transformation and the future, published in January 2021.

Riina Vuorikari worked as a senior research fellow at the Joint Research Centre of the European Commission (2013-2022). Her work focuses on citizens' digital competence, recently she led the DigComp 2.2 update and contributed to EU's Digital Skills Indicator 2.0. Vuorikari has degrees in education (M.Ed in 1998 in Finland), hypermedia (DEA in 1999 in France) and her PhD is from the Dutch research school for Information and Knowledge Systems (2009). Since 1999, she has worked in the field of digital education.



FaktaBaari EDU

faktabaari.fi

NORdic observatory
for digital media and
information DISorders

Co-financed by the Connecting Europe
Facility of the European Union

SITRA