The digitisation process has a strong social component. The Internet is not only a medium, it also creates a specific space: the digital space, which can be considered a global common and a ‘public’ space. Being a public space, the Internet brings into focus issues of participation, ethics, rights and political agency.

The notion of a public space is essentially tied to the concept of democracy. Users are not simply passive receivers and consumers of content, but are also active participants and citizens in the online life. The digital space could appear to be the answer to their search for a new hospitable space, where they can exercise their democratic rights.

A. THE BENEFITS

Policy questions: What are the benefits that digitisation could and can bring to political processes, democracy, and to the public trust? How can they be exploited? How can digital tools be most effectively used to strengthen democratic participation and enhance public trust in the online space? Who can make this happen?

1. Digitisation and democratic participation

The digital space, as a cornerstone of the public policy space, can be a great enabler for democratic discourse and participation, as well as inclusive policy-making.

The positive impact of digitisation on democracy can be assessed on different levels. A report by the British non-governmental organisation Nesta identified five main dimensions: observation, issue identification, proposals, decision making, plus monitoring and transparency.
Observation: Digital technology can encourage public engagement in generating useful data. This is the case, for example, with the ‘Air Map – Big Data Challenge’ launched in the U.S., where the exposure to air pollution was measured using mobile phone data.

Issue identification: Institutions can better identify issues that represent a concern for citizens by applying digital technology. For example, in the UK, the ‘FixMyStreet’ mobile application allows citizens to report problems such as graffiti or faulty street lighting to the authorities. In Iceland, the ‘Betri Reykjavik’ initiative allows citizens to submit ideas about budget expenditure across the capital.

Proposals: Digital tools can be used to enhance the involvement of stakeholders in drafting new laws and policies. In New Zealand, for example, the decision-making software ‘LOOMIO’ has been developed to assist different groups during decision-making processes, and to crowdsourc new policy ideas from citizens for developing an alcohol management strategy.

Decision-making: Digitisation has significantly influenced the decision-making process in democracies, through large-scale voting in particular. For example, in Brazil, India, and Venezuela, electronic voting is currently used nationwide, whereas in the US, Japan, Argentina and France, electronic voting is used in some parts of the country. Estonia represents an interesting case: citizens can vote online by using the chip embedded in their ID card as a digital signature which is inserted into a specific card reader to verify their identity.

Monitoring & transparency: One of the more controversial uses of digital technology is a tool to ensure and monitor transparency and accountability. The issue extends beyond the simple consideration that organisations and institutions can – via the Internet – inform the public about their ongoing activities and processes. The debate extends further, e.g. WikiLeaks’ use of digital tools in order to demand transparency from governments and institutions. Some commentators have considered the extent to which WikiLeaks can test the power of ‘total transparency’ in domestic and foreign policy; others have argued that WikiLeaks’ activity only pursues the ‘idea of transparency’ because ‘there is no such thing, even in the age of the Internet, as the instantaneous and complete revelation of the truth. In its undigested form, information has no transformative power at all. Raw data must be distilled; the attention of a distracted audience must be captured; and that audience must accept the message that is put before it. The process by which this is done is complex and easily swayed by commercial and governmental interests’.

2. Digitisation and public trust

Digitisation can help to improve public trust in governments and institutions in a number of ways. When it comes to transparency, online portals and publicly available datasets have facilitated users’ access to information, and interaction with entities. The ability to scrutinise governments’ actions has
increased with the availability of information. The civic participation of the public, such as through engagement in consultations, is extensively facilitated through online tools and processes. In relation to e-governance, online services such as e-payment and e-health have enhanced citizens' access to government services. This applies in particular to government-to-citizen and government-to-business services. Digital tools also support and encourage data sharing. For example, the digitisation of public and land registries have rendered civil processes more efficient. Data sharing among government authorities and entities has also increased efficiency levels, and increased collaboration among them.

3. Digitisation and human rights

The digital space also impacts democracy through the perspective of human rights, as the Internet can be considered to be an enabler of human rights. Access to a free and open Internet means access to information, knowledge, culture, and education, among others. The Internet also facilitates the exercise of rights such as freedom of expression and freedom of assembly, allowing individuals to become active participants in the digital society.

Several instruments and documents adopted by organisations such as the Council of Europe, the United Nations Human Rights Council, and the United Nations Educational, Scientific and Cultural Organization (UNESCO) have underlined the role of digital communication tools in the exercise of human rights. For example, the Council of Europe Parliamentary Assembly Resolution 1877 (2012) on the protection of freedom of expression and information on the Internet and online media noted that the right to freedom of expression and information ‘is typically exercised through the media, and, nowadays, in particular, through media based on new information and communication technologies such as the Internet and online media’. Furthermore, the Resolution welcomes ‘the new possibilities for individuals to share publicly, through the Internet and online media, information which is of public concern’.

In another example, the UN Human Rights Council Resolution A/HRC/32/L.20 (2016) on the promotion, protection and enjoyment of human rights on the Internet outlines, among other things, that ‘access to information on the Internet facilitates vast opportunities for affordable and inclusive education globally, thereby being an important tool to facilitate the promotion of the right to education’. According to UNESCO’s 2016 study on ‘Privacy, free expression and transparency’, ‘the exercising of [the right to freedom of expression] has changed and improved in many ways over the past decades, especially by the connection of so many individuals to an online space. […] Freedom of expression is enlarged in the digital age not only by extending its access dimension, but also by enabling innovative ways to communicate and diffuse information’.
B. THE CHALLENGES

Policy questions: What are the challenges that digitisation could and can bring to politics, democracy, and to the public trust? How can they be addressed, and by whom? What are the roles and responsibilities of the different stakeholders?

1. Digitisation and ‘information disorder’

Digitisation can be a great enabler for democratic discourse and participation. At the same time, the misuse of the digital public policy space can lead to the so-called information disorder and distortion of ‘truth’, mistrust in public information, and misrepresentation of public opinion.

Social media platforms have given voice to the many, but how and who can now distinguish between verified or false ‘facts’, ‘opinions’, and ‘feelings’? The spread of information disorder through manipulated or manipulating online communication, often described as fake news, is one of the issues that has raised growing concern among governments, end users, and intermediaries. It needs to be recalled that manipulation of information and communication is not a new phenomenon, but has existed in various forms in all periods of human history. In recent times however, we witness an increased use of the term ‘fake news’ which is a term used by different actors in different circumstances, such as when criticising factually false information, to a false balancing of factually correct information to just expressing dissatisfaction with a piece of information a particular party does not like. In current academic research, the dominant view is that this vague term is not helpful to understand and analyse the problem, but that a more precise conceptual framework is needed for describing different aspects of information disorder: A recent expert study proposes to distinguish at least three components of information disorder: 1) Dis-information (information that is false and deliberately created to harm a person, social group, organisation, or country); 2) Mis-information (information that is false, but not created with the intention of causing harm) and 3) Mal-information (information that is based on reality, used to inflict harm on a person, organisation, or country).

Also related to the increasing distortion of the truth is the issue of bots, which are reported to be influencing democratic elections. Furthermore, the danger of filter bubbles and echo chambers (‘blistering’) needs to be discussed, as people are increasingly only talking to like-minded people. In a speech in October 2016, the German Chancellor Angela Merkel argued that algorithms operated by search engines could result in insufficient awareness of opposing ideas - leading to so-called filter bubbles and echo chambers - which can harm a healthy democracy. ‘Algorithms, when they are not transparent, can lead to a distortion of our perception, they can shrink our expanse of information.’ Mrs Merkel called on internet companies to make publicly available information regarding the algorithms they utilise in their search engines.
Multiple stakeholders have recently started to engage themselves in what is termed **fact-checking activity**. At the European level, the European Commission launched a public consultation on ‘fake news and online disinformation’ and announced the creation of an expert group to identify best practice and coordination mechanisms in order to address the dissemination of false information. Both the results of the consultation and the work of the expert group should be presented by spring 2018.

As for the role of Internet **intermediaries**, the major social networks have stepped in to combat the flow of information disorder. Facebook developed a strategy which combines crowdsourcing (analogous to how Facebook regulates adult content), reliance on third-party fact checkers, and financial disincentives for misinformation hucksters. Google announced its first policy against ‘blatantly misleading, low quality, offensive or downright false information’ in April 2017, promoting a system based on user feedback which will refine the ‘search engine to surface more authoritative pages and demote low-quality content’. Twitter is considering adding a ‘fake news’ button in order for users to flag tweets that contain misleading, false or harmful information.

### 2. Digitisation and traditional media

Traditionally, independent and trusted media of high quality have been an important pillar for public opinion forming. Furthermore, they have played a crucial role as public watchdogs in a democratic society. However, digitisation is leading to a profound process of transformation in the media landscape.

Traditional quality media formats have come under significant **economic pressure**. Digital channels have multiplied in the television and radio sector, and print media is struggling with declining advertising and subscription revenues. The major structural change that the print and broadcasting industry is currently undergoing is running in parallel with the success of global Internet intermediaries. Furthermore, there has been a **change of media usage behaviour**. The attention of the public is increasingly focused on the Internet and young people in particular are less likely to consume traditional media formats.

The question arises as to how citizens can be given the opportunity to participate in an informed manner in the democratic society, to form an independent political opinion, and to orient themselves in an increasingly complex world. It is desirable for independent and highly trusted quality journalism to continue under the new conditions. In this regard, the role and funding of **public service media**, which should be independent from government as well as business influence, is crucial. However, also a pluralistic press sector and private broadcasters has a pivotal role in relation to public opinion. As these institutions are not traditionally state funded and benefit from guaranteed state
independence, ways of supporting these institutions via indirect measures (such as the funding of journalism schools) could be considered.

Traditional media players have recently started to engage in fact-checking activities. Many of the most authoritative international and European press agencies have set up specific teams or launched initiatives focused on tackling disinformation. For example, in October 2017, France 24 and EURACTIV launched a fact-checking programme ‘Fact or Fake’, dedicated to combating misinformation. Several independent organisations were funded with this precise purpose (e.g. FactCheckEU.org, Full Fact, Les Décodeurs, Pagella Politica, FactCheck.org, FactChecker – a joint project with the Washington Post – and PolitiFact.com).

3. Digitisation and freedom of speech

Freedom of opinion and expression – which includes the freedom to seek, receive and impart information – are among the most fundamental rights in a democratic society. They apply equally offline as well as online. The internet has transformed and reinforced the exercise of these rights, though, in recent years, there has been a tendency towards more restriction and control in the digital space.

In a number of countries in all regions of the world, governments have taken steps to limit the freedom of expression in order to protect morality, public order, and general welfare. Studies on freedom of expression online have been carried out by the Organization for Security and Co-operation in Europe (OSCE) and Council of Europe, among others. Freedom House’s Freedom of the Net Report 2017 concludes that the ‘use of surreptitious methods to distort online discussions and suppress dissent (…) has gone global. Such state-led interventions present a major threat to the notion of the internet as a liberating technology.’

The issue of restrictions on press freedom online is also relevant. In its 2017 World Press Freedom Index, Reporters Without Borders concluded that ‘we have reached the age of post-truth, propaganda, and suppression of freedoms – especially in democracies.’ Attacks on website editors and bloggers are not uncommon. Free media play a crucial role in shaping a healthy democracy by promoting educational programmes, exposing the loopholes in the democratic system, and eventually contributing to some extent to a mechanism of political accountability. Lack of press freedom – both online and offline – is therefore an impediment to democracy.
4. Digitisation and privacy concerns

The access, gathering, use and control of information by governmental bodies as well as intermediaries can give rise to privacy concerns in a democratic society. Governments collect and process vast amounts of personal information – such as birth and marriage records, social security numbers, tax information and housing records – for various purposes related to the exercise of their functions. However, the way in which such information is collected and used, especially in the digital era, raises issues of trust. Governments should only collect and use the personal data needed for the democratic and legitimate performance of their functions. One main challenge is to ensure a proper balance between the democratic performance of government functions and the guarantee of citizens’ privacy rights, including restricting the collection and processing of information to that which is strictly necessary to perform the government’s legitimate functions.

Intermediaries have a role to play in relation to privacy concerns because as technology advances, their surveillance capacity increases. The relevance of intermediaries can be understood on several levels. As depositaries of user data, ‘information intermediaries become a natural target by governments who turn to these private companies to gain access to user information for legitimate and illegitimate reasons’. Even when no disclosure of personal information is involved, big sets of data can be anonymised and personal information can be traced (e.g. through IP addresses and geolocation).

The collection and processing of data by public authorities and Internet companies is an issue left to national legislation, and approaches to it vary significantly. In the U.S., this matter is mainly a consumer protection issue, whereas for the EU this is primarily a human rights issue (right to privacy – which is, however, not considered to be an absolute right). As per the European framework, the General Data Protection Regulation (GDPR) grants EU citizens the possibility to take control of their personal data. The GDPR has implications beyond EU borders, but how this will be reconciled with regulations in other jurisdictions is not yet clear.

The Internet industry also collects and processes vast amounts of data, which in recent years has become a business model. Although their motivation is mainly economic, the concentration of large amounts of data and the data-sharing with other actors could impact citizens and public discussion spaces. The increasingly blurred distinction between security and business surveillance poses a risk for human rights of individuals and democratic processes.
5. Digitisation and crime

Cyber-attacks occur on a daily basis and can seriously impact businesses and governments' systems. This was the case with the ransomware ‘WannaCry’ that targeted the Windows operating system by blocking data and demanding a ransom in Bitcoins. The attack infected the National Health Service (NHS) in the United Kingdom, and companies such as FedEx and the German railway company Deutsche Bahn (Larson 2017 and Hern and Gibbs 2017). Cyber-attacks challenge and undermine governments’ capacity to ‘secure security’, and can have a negative impact on public trust. With every attack on institutions and critical infrastructure, the call for tougher and prompter action is felt, and the discussion on the roles and responsibilities of key players is intensified.

Within the context of crime, the spread of violent extremism should also be mentioned. Terrorists have been using social media and other online channels not only for real-time communication but also to spread their ideologies. This has raised serious concern among governments, who have been applying pressure on Internet companies to tackle such content faster and more effectively. Stakeholders have implemented several initiatives; among these is the Global Internet Forum to Counter Terrorism which is developing technological solutions, performing research to guide policymakers, and building a knowledge-sharing network.

6. Emerging technologies and public trust

Artificial intelligence (AI) and automation are arguably the emerging technologies that have captured the most interest, imagination, and concern in recent years.

Higher levels of encryption in algorithms have resulted in portraying such technologies as ‘cryptical’. The more secure and efficient the technology is claimed to be, the more obscure it appears. Such technology is often regarded as a black box: a problem emerges, inputs are fed into an algorithm and possible solutions are produced with little knowledge from the human side as to how that output was produced. Studies have shown that ‘an [accurate] algorithm that generates accurate recommendations is not enough to constitute a useful system from the users’ perspective. The system needs to convey to the user its inner logic and why a particular recommendation is suitable for them.’ Opaque processing of users’ queries and inputs impairs their ability to understand how the algorithm works, resulting in misconceptions and lack of trust on the part of users. This highlights the issues of accountability and legitimacy of algorithms’ decision-making faculty as well as ‘transparency’ (i.e. if there is actually the possibility for every algorithm to be interpretable).

Trust issues in relation to emerging technologies are understandable not only in terms of transparency, legitimacy and accountability, but also on ethical grounds. When machines are programmed to substitute a human function (e.g. driving a car), are they also able to replace humans
as moral agents? And how should the issue of lethal autonomous weapon systems (LAWS) be tackled?

Transparency and accountability in AI systems is an ongoing area of research, and progress is being made in this direction (for example, researchers at Columbia and Lehigh universities have developed a tool – DeepXplore – that could help bring transparency into AI). A Group of Governmental Experts created by the Contracted Parties to the Convention on Certain Conventional Weapons is tackling the implications of the technology in the field of LAWS, including from the perspective of accountability.

Apart from AI, progress in the development of new technologies towards trust and transparency have been made: blockchain technology is becoming acknowledged as a step in this direction. Blockchain is a system registering transactions that allows each user (i.e. each party of the chain) to hold a copy of every transaction (i.e. modification made) on a given document, thus monitoring changes and consequently assuring integrity (2017 International Finance Corporation Report and ‘Building Trust with Blockchain’). All the parties to the chain are then part of a trust circle in which transactions are monitored and validated by every member. Although the application of this technology in different fields seems promising, there are still challenges in relation to increasing trust.

C. THE WAY FORWARD

Policy questions: Can digital literacy, education, and awareness-raising be the key ingredients for empowering citizens to deal with the challenges related to the misuse of digital public space?

Education and democracy are inextricably linked: education is a crucial element which allows democratic participation. The relationship between the two works in both directions: democracies push for free and universal education, and education tills the fertile ground for a ‘healthy’ democracy.

In relation to the impact of digital technologies on democracy, it is clear that the more digital tools permeate the pursuance of ‘traditional’ democracy, the more urgent the need to tackle the issue of literacy in the digital sphere. Digital literacy is defined as ‘the ability to understand and to use information from a variety of digital sources and regard it simply as literacy in the digital age’. This concept of literacy does not relate simply to the ability of people to access content and produce it on the Internet (this would be closer in meaning to ‘web literacy’), rather it refers broadly to the ability of people to use digital services on all devices (computers, smartphones, tablets, etc).

When it comes to literacy per se, governments play a pivotal role. Governmental initiatives (e.g. in Chile, India, Estonia) have attempted to include digital literacy in their national educational
programmes. However, few countries have actually tackled this issue and embedded digital literacy as a subject covered in daily lessons. A study conducted by the Organisation for Economic Co-operation and Development (OECD) found a mismatch between the fact that digital technologies play a significant role in our personal and professional lives and the fact that these technologies have not yet been fully adopted in formal education. Digital literacy is also inextricably linked to issues such as the digital divide. The issue is not simply the possibility of accessing technology and the Internet, but also the ability to exploit them.

At the international level, efforts have been made in this direction. Within the 2030 Education Agenda, UNESCO’s partnership with Pearson is one such example. This partnership aims to ‘spread awareness of current digital solutions and spark further innovation to help low-skilled and low-literate youth and adults participate more effectively in the digital economy and knowledge society and, in the process, develop their skills and literacy’.

Promoting education and literacy alone will, however, not be sufficient. There is also a responsibility of media actors and platform operators to support citizens and users in finding out who they can trust and how to identify manipulated or manipulating information. Many journalists and other media actors including online platform operators have engaged in activities to develop quality journalism criteria or trust marks as well as ‘fact-checking’ tools that should help users to assess the reliability and also ethical standards of information and its sources.

Also, many governments and intergovernmental institutions have realised that they have a responsibility in creating an enabling environment for a trustworthy public sphere and more secure democratic processes. Concrete steps include, for example, increasing the technical security of voting mechanisms, and providing support for quality and reliable journalism and media. One recent example is the decision of the Council of Europe and its member states to set up an expert group on quality journalism in the digital age.

What is needed in the end is, again, a joint effort of governments, the (media and online) industry, civil society and academia to find practical solutions to maximise opportunities and minimize the risks that digitalization brings to public debates and democratic processes.