SHAPEDEM-EU

Digital Transformation as a Double-Edge Sword for Democracy

Working paper on digital transformation

PUBLICATION #5

Funded by the European Union

SHAPEDEM-EU Publications

Published by National University of Kyiv-Mohyla Academy (NaUKMA). July 2024.

This publication is part of WP1, led by Roskilde University (RUC).

Authors: Anna Osypchuk, Anton Suslov, and Yaroslava Shaporda (all NaUKMA)

Contributing authors : Carme Colomina (CIDOB), Kateryna Korpalo, Mariia Kriuchok, Bohdan Hultai (all NaUKMA)

To cite:

Osypchuk, Anna, Anton Suslov, and Yaroslava Shaporda, 2024. Working Paper on Digital Transformation. SHAPEDEM-EU Publications.

Design: EURICE GmbH

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency (REA). Neither the European Union nor the granting authority can be held responsible for them.

Table of Contents

List of Tables

Abstract

The paper discusses the juxtaposition of digital transformation (DT) and democracy support and democracy contestation. While the DT is defined as an adaptation and implementation of digital technologies into political and social processes, digital tools are seen as such that could be used both by democratic and non-democratic systems and are perceived as 'neutral'. The paper aims to reveal how digital transformation in governance, public services, civic engagement, and more broadly in everyday social practices impacts democracies and democracy support. The digital transformation instruments are reviewed in the context of democracy support and democracy contestation and the conceptual framework for understanding of the role of DT as a cross-cutting issue in the SHAPEDEM-EU work packages is provided. The paper sets the ontological framework for the nexus of DT and democracy support or contestation. It discusses digital democracy and digital authoritarianism first on a conceptual level and then through the analysis of digital instruments and solutions. While they are sorted into two toolboxes – democratic and autocratic – almost all of them could be applied equally to enhance democratic support or to contest democracy and both to facilitate and to circumvent democratic practices and rights. Also, the interconnection of two cross-cutting issues of the SHAPEDEM-EU project: gender equality and DT, is outlined. Finally, the paper reviews EU policies concerning DT and the question of media literacy and its relation to democracy support and democracy learning.

Introduction

Digital transformation (DT) has become a buzzword in recent years, and its impact on the democratic process has been a popular topic for debate in many fields. The advent of new technologies and their integration into various aspects of society has led to significant changes in the way people interact with one another, businesses, and their governments. In this paper, the digital transformation is perceived through a sociopolitical lens and thus defined as *an adaptation and implementation of digital technologies into political and social processes.* It includes leveraging information, computing, communication, and connectivity technologies through regulations that transform organisational, business, political, societal, etc. processes and might lead to social changes in a target entity (organisations, societies, industries, etc).

Vial's (2019) review of digital transformation shows its complexity and different aspects of DT. Because digital transformation covers "broader individual, organisational, and societal contexts" (Legner et al., 2017, p. 301), it is multidimensional. Thus, DT is primarily about improving the process but not the outcome of the transformation itself. DT is primarily about instruments and procedures and could provide opportunities and challenges both in the context of democracy support and democracy contestation.

In this paper we aim to reveal how digital transformation in governance, public services, civic engagement, and more broadly in everyday social practices impacts democracies and democracy support. We review digital transformation instruments in the context of democracy support and democracy contestation and provide conceptual framework for understanding of the role of DT as a cross-cutting issue in the SHAPEDEM-EU work packages.

We start with setting the ontological framework for the nexus of DT and democracy support or contestation. Then, we discuss digital democracy and digital authoritarianism first on a conceptual level and then through the analysis of digital instruments and solutions. While we sort them into two toolboxes - democratic and autocratic - it should be emphasised that almost all of them could be employed by any country - democratic or not - or even some tech corporations. Thus, all these instruments could be applied equally to enhance democratic support or to contest democracy. Then, we discuss the interconnection of two cross-cutting issues of the SHAPEDEM-EU project: gender equality and DT. In the last two sections, we review EU policies concerning DT and the question of media literacy and its relation to democracy support and democracy learning. All sections end with the guiding questions that could be used by SHAPEDEM-EU researchers in their empirical work.

1 Digital Transformation: Between Structure and Culture. And What about Agency?

Conceptualisation of DT and its role brings us back to the ontological debates about the interplay of structure, culture, and agency. While digital technologies have the potential to transcend social and cultural constraints and enable agents to act undetermined by them and creatively, they also could be utilised by states and institutions to limit the space for such actions. Thus, consideration of structure-culture-agency intersection is important for us as it directly influences the ways digital instruments and solutions are utilised for democracy support or democracy contestation. In turn, DT also reciprocity impacts structure, culture, and agency.

On the structural level, digital technologies become embedded into social structure and hierarchies. The critical political economy appears to be a helpful concept focusing on power relations and social inequalities and covering issues regarding ideologies and structures affecting those power relations.

For example, digital platforms are driven by a set of mechanisms that includes datafication and commodification (Van Dijck & Poell, 2016) which affects how users and companies interact through services and products and how businesses can earn more money using big data for their commercial needs. Another aspect of the critical political economy relates to the so-called political economy of communications and emphasises the power relations that shape media and communication systems (Havens & Lotz, 2012). This approach assesses the public sphere as an element of democratic regimes and how digital technologies modify traditional media, change online media space and bring new challenges for communications in general.

Overall, the critical political economy argues that technologies cannot be neutral as there is an interest of the owners of the technologies that shape certain power relations. However, not all technologies are private, so they can be owned by the government, created by activists or even by a broader group of people with an open code that provides more transparency on how it works. Therefore, critical political economy provides a lens for analysing the economic and political implications of digital transformation (e. g., Srnicek, 2017; Schiller, 2011).

The focus on the structural relations and hierarchies should not prevent us from considering culture. Many scholars stress culture as an important factor for success in digital transformation (e.g., Karimi and Walter, 2015), mainly considering the organisational culture within industries and companies. In the systematic literature review on digital maturity, Tiechert (2019) showed that digital culture attributes are not systematically integrated and can be a barrier to digital transformation in the company impacting its effectiveness, ability to experiment and to get investments. While the majority of the literature on DT discusses organisational culture as it focuses on business administration and industries, it is safe to extrapolate the same arguments to the societal level. Thus, the political culture and sociocultural practices in societies are pivotal in the ways DT instruments are shaped and utilised. We can see this within the SHAPEDEM-EU project in comparing how different countries in EU Eastern and Southern Neighbourhoods regulate and use DT or how their discursive understanding of democracy and democratic values and practices connects to the EU DS.

Finally, we come to the question of agency. Through meaningful participation and collective action, agency might be performed as an action or practice that is conditioned but not determined by structural or cultural constraints. In its turn, DT both enables and constrains agency. For example, digital instruments can give a voice to marginalised people by providing them with access to different audiences and transcending geographical or social boundaries, while algorithms employed by social media or digital censorship might limit the outreach of these people's messages. The networkability of digital instruments and solutions is also an important indicator as it focuses on engaging more people, facilitating exchanges (Moro Visconti, 2020) and increasing the ability to explore and expand different markets, auditories, and areas. On the microlevel, several theoretical perspectives could be employed: network theories, ANT, and approaches that focus on the analysis of collective actions or communities of practices.

How to apply within SHAPEDEM-EU – Some Guiding Questions:

1. What are the structural and cultural factors that impact DT in the case countries?

2. How do they impact the employment of digital instruments and solutions in democracy support and democracy contestation?

3. How does the DT change the social and cultural landscape in the EU and Neighbourhoods?

4. Does DT enhance or constrain agency in the case countries? Is it possible to create an index?

5. In the DT regulations, are people seen as “agents or subjects” by states or/and the EU?

2 Digital Democracy vs Digital Authoritarianism?

In the context of digital transformation, democracy support mainly lies either in the development and enhancement of digital democracy instruments or in combating digital authoritarianism and obstructing authoritarian learning.

Some scholars even introduce the term "digital democracy" as an effort to explore digital technologies from the perspective of democratic theory. Berg and Hofmann (2021) define digital democracy as "a concept that links practices and institutions of collective political self-determination with its mediating digital infrastructures". One of the challenges is that there is no legally agreed definition of "democracy" (European Committee on Democracy and Governance & Mergel, 2021). While there might not be any unified definition in legal terms, the existent theoretical perspectives provide a certain flexibility to explore those concepts and see how digital technologies can facilitate greater transparency, accountability, and participation in political decision-making processes. For example, Froomkin (2004) stated that with web 2.0 a representative democracy will be characterised by mass participation; Hacker (2002) suggested "network democracy" to explain a new networked society (Castells, 2009) in the democratic frame, while Noveck (2009) argued about "wiki democracy" to emphasise the volunteering nature of networked communities for collaboration.

Proponents of digital democracy also believe that digital tools can provide a more inclusive form of citizen participation and create a "relationship between collective self-government and mediating digital infrastructures" (Berg & Hofmann, 2021). Albeit there are many positive aspects of using this approach, there are some risks that should be considered within this theoretical frame. That includes issues of privacy, cybersecurity, and the potential for digital exclusion, as well as the potential for polarisation and disinformation. Critically approaching digital democracy scholars (Bernholz et al., 2021) raise questions regarding new institutional principles for democracies to facilitate new technological tools, how private resources of the digital platforms can be used for public benefit, how existing digital infrastructure excludes entire communities, and how to build trust online with citizens considering the vast amount of information and disinformation around them online. Those questions are usually underestimated within the democratic theory and need more attention for future research.

Whilst discussing digital democracy with its threats and opportunities, we can't omit mentioning **digital authoritarianism** and the ways in which non-democratic states and/or authoritarian regimes utilise DT to promote themselves and retain their power.[1] It should be noted that in talking either of digital democracy or of digital authoritarianism, we rather discuss the usage in different contexts of particular tools that constitute their arsenals of digital instruments and solutions than discuss the political regime as a whole.

The political context and values that dominate within authoritarian regimes impact how technology is used and adopted there in contrast to democratic countries. The same tools that in free societies allow citizens to exchange information and opinions, defend their rights, engage in the political processes and effectively enjoy public services, may be used for opposite goals and strengthen dictatorship and

[1] For the purpose of the argument, we divide countries into democratic / non-democratic or authoritarian. At the same time, we are aware of discussions regarding democratic countries employing (arguably) non-democratic tactics and vice versa. Still, the debates about what could or should be described as democratic or authoritarian and whether the usage of democratic or non-democratic instruments defines the nature of the political regime is not in the focus of this paper.

contest democracy. In the hands of authoritarian regimes, through authoritarian learning digital instruments become means for deepening control over societies, repressions, political persecution, and manipulation.

For the last thirteen years, according to the latest Freedom House report, the level of global Internet freedom has been decreasing (Shahbaz et al., 2023), and democracy around the world has been declining (Freedom House, 2023). This negative trend is coinciding with the growing usage and popularity of the online sphere and social media. Web platforms become central in the formation of public opinion and rhetoric both in people's everyday lives and on a global level (Jovanović, 2023). Also emphasised is the ability of regimes to utilise Internet platforms to extend their domestic and international hegemony through direct or indirect infrastructure ownership which is defined as **social media power** (Jones, 2022). Also, it should be taken into account that social media are privately owned, and the majority, if not all, digital public services are provided by tech corporations. This gives opportunity to these providers and owners to establish their own rules or regulations which limits spaces of democratic control (Opinion on democracy in the digital age, 2023).

Two aspects of ''digital authoritarianism'' could be defined as its key elements:

1) through digital algorithms and censorship (on social media platforms, creating 'Great Firewall' or 'sovereign Internet', etc.), a picture of unanimous informational space is formed in a more subtle and subversive way than by traditional propaganda;

2) digital surveillance or dataveillance that includes the usage of AI algorithms without obtaining informed consent from citizens.

While digital authoritarianism is still a developing concept, there is another term that is used to explain and explore digital transformation in non-democratic countries. The concept of "networked authoritarianism" links authoritarian regimes with digital communications (MacKinnon, 2011). According to MacKinnon (2011), the main characteristic of the networked authoritarian state is that "the single ruling party remains in control while a wide range of conversations about the country's problems nonetheless occurs on websites and social-networking services" (p.33). While the government has means to control online communication and messaging, people are still able to post about social problems or injustices to draw attention and even to have an impact on government policies. Thus, people with Internet or mobile access feel that they are able to speak freely and be heard, unlike under classic authoritarianism (MacKinnon, 2011, p. 33).

Nevertheless, social media serve as platforms for promoting narratives of authoritarian regimes that would otherwise be in strict informational isolation. Some social media legitimise these regimes by presenting their position as an alternative one with the right to exist (The UN Refugee Agency, 2021, p. 230; Jovanović 2023, Ch.3). Authoritarian regimes use social media to carry out repression and prevent common action, employing them as tools of control, surveillance, and censorship. This may include blocking or restricting access to specific platforms, extensive monitoring of citizens' online activities, and disseminating propagandistic information to manipulate public opinion and support the regime (Jovanović, 2023, Ch.1.2).

It is important to note here the difference between governmental intrusion into public or civic discourses and even opinion formation in non-democratic and democratic states, particularly through digital means. In democracies, the prevailing motivation for regulating or intruding into civic discourses

on digital platforms is to mitigate the risks of manipulations, spreading of mis/disinformation, creation of echo chambers, exacerbation of conflict situation, spreading of radicalised and polarised views, or preventing digital bullying and organised online campaigns of defamation. There is an assumption that such intrusions are induced by the need to protect the people during periods of turbulence – political, economic, or healthcare, – and are not posing threat to democracy, as they are usually provisional and designed to avert chaos and further exacerbation of the problem (e. g. the disinformation campaigns during the Covid-19 pandemic that required states' interventions). Still, this instrument could be abused even in a democratic state. At the same time, authoritarian regimes and countries are primarily intruding into public or civic discourse and opinion formation to uphold and reproduce the existing power structures and to tame or eliminate dissident thinking and opposition.

As authoritarian regimes not only pay a lot of attention and a heavy price for controlling people and communication within their state but also spend colossal resources on spreading their influence and tactics, in particular through authoritarian learning techniques. Even more, they exploit and employ all possible weaknesses and democratic practices and processes to their own means whenever possible, corroding and undermining them - particularly manipulating such basic democratic values as freedom of speech, right to privacy, and other basic freedoms. Thus, protecting these freedoms from coercion and manipulation, together with democracy support and democratic learning, becomes of utmost importance. This issue must be tackled with combined efforts of governmental and civil actors as well as technology industry leadership (Shahbaz, 2018), as global promotion of digital authoritarianism can only be conquered with coordinated multilateral efforts in building resilience of societies, disclosing hostile actors and suppressing their influence.

How to apply within SHAPEDEM-EU – Some Guiding Questions:

1. How the political regime in the case country could be described: democratic or authoritarian?
2. Does the government use the "democratic" digital tools? What are the aims and justifications?
3. Does the government use the "authoritarian" digital tools? What are the aims and justifications?
4. What is the role of non-state actors (e. g., tech corporations) in providing "democratic" or "authoritarian" digital tools?

3 Digital Toolbox for Democrats and Autocrats

In this section, we discuss the digital tools and technologies that form repertoires of digital democracy and digital authoritarianism as well as facilitate democratic or authoritarian learning. As such, these toolboxes could also be applicable in democracy support as well as in democracy contestation. We insist that democracy support might be facilitated through development of ''democratic toolbox'' while mitigating both ''autocratic toolbox'' and negative side effects of digital tools within ''democratic toolbox".

Before proceeding to the discussion of particular toolboxes, it is necessary to highlight the positive effects digitalisation has on democratic processes and practices.

1. **Inclusive participation.** Digital technologies facilitate access to communication, information, and civic and electoral practices and processes for everyone, and particularly for people with disabilities, from marginalised groups, and different geographical locations. Electronic voting machines can have Braille lettering, voice output to follow instructions and candidate names and touch screens (Raja, 2016, 16). Government websites can provide information in various formats tailored to different needs. When government services and registries are available in digital formats, there is a higher possibility that people with disabilities will be able to access services autonomously and independently through customised interfaces. (Raja, 2016, 16). Digital platforms can also enable remote participation in democratic processes, such as virtual town hall meetings, public forums etc.

2. **Accountability** and **transparency** (Poiran, 2023; Shenkoya, 2022) as citizens can closely monitor the government's activities via electronic and online registries, budget, reporting mechanisms, public procurement, etc. Also, when services are provided online or with the help of AI solutions, there is less space for corruption. Blockchain technology is one of the instruments in ensuring transparency and integrity in political processes (Poiran, 2023) - for example, in e-elections during the processes of voting and counting (Berenjestanaki et al., 2024).

3. **Effectiveness of governance.** They streamline authorities' responses to problems raised by the public (Poiran, 2023) and facilitate interaction between government and citizens. The European Committee on Democracy and Governance has highlighted that digitalisation enhances participatory democracy through bottom-up and top-down tools. Thus, one of the primary goals of DT initiatives is to bridge the gap between representative institutions and citizens and to address such weaknesses as a lack of civic engagement and public support for policies etc. (European Committee on Democracy and Governance & Mergel, 2021, p. 16)

While we will discuss particular threats and challenges of digitalisation further, the general remark regarding DT should be made. Despite the opportunities offered by digital democracy practices, coercive digitalisation might cause harm to both citizens and public institutions, as highlighted in Berger's (2015) study. Transformation of public services into a 'digital only' format might lead to the diminishing of these services' effectiveness or to some people losing access to them due to the digital divide, infrastructural issues, complexity, etc.

We start our analysis of toolboxes with a 'democratic toolbox', which includes digital instruments to promote civic participation, accountability and good governance, and other instruments. The proposed categories could be further operationalised within the SHAPEDEM-EU project according to the empirical cases and research tasks of particular work packages. In *Table 1. Democratic Toolbox,* we describe digital tools as such, discuss opportunities they provide for democracies and challenges or threats they might present thus opening the way for non-democratic practices.

Now, let's focus on the ''autocratic toolbox" of digital instruments and solutions. The tactics of digital authoritarianism are various and evolve with the emergence of new technologies as authoritarian regimes also learn from their own and other regimes' experience. Feldstein (2019) distinguishes six main techniques of digital suppression: surveillance, censorship, disinformation, cyber-attacks and hacking, Internet shutdown, and targeted arrests and violence. They are discussed in *Table 2. Autocratic Toolbox.*

Almost all digital instruments and solutions that we included into these toolboxes provide both opportunities and challenges or even threats to democratic practices. They could be used for democracy contestation by insiders or outsiders. They also are employed for democracy support. Every country or corporation might use almost any of these digital tools and the task for DS policies is to limit the usage or manifestations of negative tactics and enhance positive.

Table 1 Democratic Toolbox

	Description	Opportunities	Challenges and Threats
Social Media	Social media refers to online platforms and services that allow users to share content among individuals, groups, or communities. From individual messages to texts, images, files, and videos, social media has become an essential part of the information space for the vast majority of people with internet access.	The freedom of speech facilitated by social media plays an important role in advancing democracy. Social media by being (almost) state censorship free allow for free and open discussions enabling individuals to express their opinions without fear of repercussion. This fosters an environment where a multitude of voices can contribute to the collective dialogue without constraints. Social media are a powerful tool for building social capital (Ellison & Vitak, 2015). They enable virtual groups and communities with similar interests to form, allowing them to advocate for their interests, thus directly engaging in participatory practices and civic activism or other socio-political processes. Social capital increased through digital technologies strengthens an active civil society and engagement (Fukuyama, 2000). Social media strengthen the "global village" effect, simplifying direct interaction between users from different social groups without spatial constraints (Jovanović, 2023). Individual communication in the “global village” is useful	While in democratic societies the state censorship on social media platforms is limited, social media corporate or platform rules introduce policies that limit freedom of speech and censor voices. Social media are conducive environments for democracy contestation, including normative and cultural contestation. Mis/disinformation, fake facts and manipulative narratives, populist attitudes and conspiracy theories easily find their niches and become viral on social media, thus highlighting the necessity for media literacy programmes and requiring countries to develop policies to combat mis/disinformation, propaganda, and fakes. In a way social media platforms sometimes act - intentionally or not - as useful idiots in promoting authoritarian regimes and spreading disinformation (Jovanović, 2023, p.25). Social media are prone to formation of "echo chambers" – informational spaces that reinforce our views, limiting access to

	Description	Opportunities	Challenges and Threats
		in defending one's freedoms and human rights. For example, in investigating and posting on the war crimes committed by the Russian army in Ukraine (Smith, 2022). Thus, users of social media help to fight war crimes and IHL violations and facilitate restoration of justice (Goldenziel, 2022).	alternative ones (Jovanović, 2023, p.17). This is achieved by social media algorithms that inevitably influence the content each user consumes and in turn suggest and show users content that is similar and in line with the one they liked, produced and consumed previously. Such informational limitation can lead to information isolation, the polarisation of user positions, and the deprivation of perspectives for mutual understanding and consensus in addressing socio-political issues (Shahbaz, 2018), particularly during elections. AI algorithms on social media have the potential to manipulate public opinion by distorting information accessibility and violating the rights to freedom of thought and opinion. This distortion may foster hatred and violence between social groups (Jones, 2019). As social media are privately owned, their accountability and compliance with (democratic) norms and laws governing state institutions is limited. There are also known cases of users' personal data leaks or

	Description	Opportunities	Challenges and Threats
			transfers to third parties without users' consent (Phillips, 2023).
DT and Civic Participation			
Political mobilisation in the digital era	Social media and other digital platforms and solutions effectively mobilise people: increase political awareness and citizens' propensity to partake in online and offline activism or engage in decision-making processes (Earl, 2010). There is a strong positive correlation between Internet usage and protest activism (Norris, 2012). Online open platforms allow users not only to consume information but also to actively engage in community interaction, collaborative content creation, and social networks building (Reddick & Aikins, 2012).	Digitalisation blurs the distinction between those who produce, distribute, and consume politics, increasing the role of a citizen and giving more agency to the electorate (Abbott 2012). Citizens become more engaged in the processes of policy formulation and adoption, participate in polls and petitions, join parties, and engage with politics in other ways (Kersting, 2012). Online interactions promote horizontal networks within society which have no defined leadership or hierarchy. Due to the fast spread of information, successful tactics of the politics of dissent spread worldwide.	"Slacktivism" and "clicktivism": activism, when limited to online dimension only, is ineffective and/or insincere as it does not require intentional effort, does not promote significant change, and does not foster accountability (see Morozov, 2012). Such performative expressions do not substitute the real democratic engagement though can be its constitutive element: low-effort online activity creates the ground for deeper involvement in social activism (Bennett & Segerberg, 2012). Online political mobilisation can divert public attention from meaningful discussion of the political realm "at home". Particular issues can be hyped. Thus, citizens may fail to form coherent positions regarding

	Description	Opportunities	Challenges and Threats
			candidates or decisions. (Koc-Michalska & Lilleker, 2016).
Electronic petitions and protest campaigns	Carried out mostly through official websites, e-petitions as a bottom-up communication tool can be initiated and signed by any verified user and addressed to governing structures on different levels. After reaching a prescribed quorum, a petition must receive a meaningful reply from the addressee. Can be used as an agenda setting instrument.	The main advantage is the possibility for any citizen to launch a protest/propositional petition and receive support without investing significant resources. An e-petition can be an easy first step to establish a dialogue on a certain topic with the authorities. It also may serve as a protest form for opposition with no political power.	Most electronic petition services require personal data, contain information about the initiators, and full lists of signatories. On the other hand, cases where pseudonyms are used for privacy reasons may raise the question of legitimacy of these signatures. If verification is not required, the same user might use several emails to sign the petition and thus amplify their voice which undermines the core democratic principle of equal representation. The meaningful reply to the petition does not necessarily constitute the support or implementation of it by authorities. The bottom-up nature of this instrument which allows anyone to start a petition leads to the huge number of petitions being filled and supported which might overload corresponding public bodies.
Online electoral campaigns	Political parties, activists or interest groups, and social movements use online platforms to interact with the people,	Communication with the electorate directly through media and the Internet facilitates information flows, making it more accessible to	Campaign platforms could be used by their owners for dis/misinformation.

	Description	Opportunities	Challenges and Threats
and support gathering	present their agenda, and run campaigns. The tools and platforms for such purposes are official websites and social media accounts administered by parties (on platforms such as Facebook, Twitter, YouTube, and others), paid advertisements on the web, broadcast and online media.	keep abreast of the times in the political sphere. This format of advertising, due to its low cost and ease of implementation, is beneficial for small political parties and independent candidates with little resources to spend on promotion (Council of Europe, 2017). These platforms are interactive and could be used for mobilisation of supporters.	Targeted ads on social media shape users' information bubble by algorithms picking tailored messages for target audiences rather than by subjective choice (Römmele, 2012). This creates 'echo chambers' and instead of widening our social networks enclose us in communicative bubbles which might in turn lead to radicalisation of thoughts and opinions. Also, there is a risk of nonconsensual personal data usage for targeting.
Electronic elections (through voting machines) (e-voting)	The two main types of e-elections are Internet voting and voting by electronic machines. The latter is organised at polling stations through machines that record and/or count the votes; they also differ in their functionality, and, therefore, affordability. While partly automated, this process requires human resources for verification and assistance, though some machines also provide electronic verification. Elections organised electronically ought to be supported by awareness campaigns and tutorials to establish public confidence.	Facilitation of election conduct for large populations. Some researchers argue that an electronic system as unbiased and invulnerable to human factors would also likely strengthen citizens' trust in elections (McCormack, 2016) as manual count is not always completely accurate. This type of election still allows such traditional instruments of control as parallel vote counting and election observation. Potentially, the trust in e-voting might positively affect voter turnout. More advanced machines are also equipped to correspond to the needs of people with seeing disabilities or illiterate population,	The major issue with electronic elections is the possibility of equipment malfunction and hacking that may distort the election results. On the other hand, contrary to popular concerns, during the election voting machines are neither connected to each other nor to the Internet, which eliminates some risks such as system-wide interference, although internal software bugs are still possible; there are also small chances of malware installation prior to the election. In some cases, machines that had been connected to the Internet were

	Description	Opportunities	Challenges and Threats
		therefore making election processes more inclusive.	replaced with disconnected ones after trial and error (Bund, 2016). Lastly, the costs of implementation of such machines, especially the more sophisticated ones, may be too high for less economically developed countries to afford.
Internet voting (i-voting)	Internet voting is brought through servers on designated computers in public places or remotely using personal devices (Górny, 2021). The vote is verified with a digital signature. Large-scale, national-level online voting can be implemented after testing the system on local elections or other samples of lower importance (Kersting, 2012). Even more than e-voting, i-voting relies on legal and social frameworks and needs to be carried out on a prepared ground and accompanied by an information campaign.	I-voting increases voter turnout (though the change is not major) as it is more practical for citizens to participate from home with only a few clicks. This allows more opportunity to vote for people with special needs, expatriates and geographically hard-to-reach populations, military personnel (Hall, 2012) and other groups that may experience difficulties with traditional voting, thus enhancing their representation in politics. It also attracts more younger voters.	Online voting process is more open to the interference of hackers, terrorists, and external agencies, and because of cyber-attacks election results may be counterfeit, certain voters disenfranchised, privacy violated, or the whole election fully or partially disrupted. The digital divide has to be considered in elections conducted online, therefore governments should organise traditional voting in polling stations for those who do not have Internet access – primarily the elderly, lower class, and less educated citizens – to retain their right to vote. Remote voting through the Internet is impossible to supervise and thus guarantee

	Description	Opportunities	Challenges and Threats
			the right to cast a vote privately and secretly.
DT and Accountability and Good Governance			
Official websites of public institutions and public records	The digital age provides more opportunity for top-down communication between the authorities and the people, allowing citizens to keep track of governmental functioning and promoting vertical and horizontal accountability on every level: from local highly specialised establishments to national parliaments. Public records include but are not limited to tax declarations for civil servants, government procurements and tenders, registers of court decisions, data from parliamentary votes, etc. **Examples.** Ukrainian online procurement platform "Prozorro" increased transparency as the space for national and local authorities to announce tenders for the purchase of goods, works and services. The system operates under the principle "everyone	These instruments provide transparency to citizens and keep the government accountable, thus gaining public trust and strengthening civil society as a watchdog. They also publish neutral, official and non-partisan information, which however may be difficult for an average citizen to grasp and analyse due to large volume.	The use of online platforms by the authorities blurs the thin line between public information and communication of individual politicians, and as a result politics rely more and more on the level of personalization and familiarity between the leaders and the people (Wojcik, 2012). Another issue is that requirements of public records can be circumvented: for example, by hiding illegally acquired assets in the case of registers of property declarations of civil servants.

	Description	Opportunities	Challenges and Threats
	can see everything": after the bidding is completed, all information about tender committee decisions, participants, the auction process etc is disclosed (Kerman and Yukins, 2022, p.24). It is estimated that in 2020 Prozorro saved $6 billion, reduced corruption, and enabled civil society to closely monitor government procurements, especially in times of war (2022, 23). Digitalisation of court processes led to the increase in transparency in the Sulaymaniyah Appellate Court in the KRI (Ahmed et al., 2022). Establishing e-courts made case data and documents public to case participants and led to the transparent case allocation system in which judges were selected automatically.		

	Description	Opportunities	Challenges and Threats
E-registries and Electronic Records	E-registries are digital databases or systems used to store and manage various types of records or registrations. Electronic records serve as evidence of the electronic delivery of services and encompass a broader range of data than e-registries. Public registers constitute the basis of all e-governments (Björklund, 2016). **Example.** In Estonia, one of registers is the national population register which contains a broad array of personal data of each individual such as ID code, date and place of birth, residence, marital status, citizenship, legal capacity, and rights of custody, as well as information regarding family documents and court orders.	Apart from increased efficiency and accessibility, the e-registries contribute to transparency by keeping a record of transactions with every change being easily tracked (Veeramani & Jaganathan, 2020). E-governance, if properly used, can ensure better data protection than paper-based data because of its traceability (Nyman-Metcalf, 2019).	One of the threats is inadequate data security safeguards and weak support for core privacy principles. Without proper training, public officials responsible for keeping and updating e-registries may not fully understand the severe implications of personal data security breaches.
Participation in the legislative process	Digitalisation positively contributes to legislature transparency as the public can follow every stage of the process (Mynenko and Lyulyov et al., 2022, p.105) and meaningfully participate in it. Instruments in this sphere include: an opportunity to get acquainted with	The main purpose and advantage of these instruments are to provide citizens with access to legislative and policy making processes in a meaningful way and to ensure transparency and accountability of local and national authorities.	When a potentially large number of citizens' appeals and comments on policy and legislation drafts have to be processed, it would require additional time and other resources. In such situations at least some portion of comments and appeals would contain irrelevant proposals and might be

	Description	Opportunities	Challenges and Threats
	transcripts and minutes of parliamentary sessions; services to comment on policy and legislation drafts that are discussed in parliament or council; online citizen opinion polls, forums and events organised for crowdsourcing for bill drafting, briefings and consultations to committees; the above-mentioned electronic petitions are also among the tools which engage citizens into law-making. Some of these digital mechanisms also offer anonymity for contributors and, therefore, personal safety. **Examples.** In 2018, an open public State budget web-portal was set up in Ukraine. This portal created an opportunity for the government and the citizens to engage in a transparent dialogue with regard to the law on budget planning. Among the data available to online visitors are planned indicators of the state budget, information on the execution of national and all local budgets (income, expenditures, crediting and financing), and data on the state debt.	This enhances trust in public and state institutions by making people part of the legislative process.	even considered spam. Some of them could be qualified as such due to the lack of commenters' expertise and their exposure to the influence of populism and/or propaganda.

	Description	Opportunities	Challenges and Threats
Participatory budgeting	Participatory budgets are a special case of citizens' engagement into the policy making process on a local level. They allow citizens not only to take part in the discussing budgets in their communities, but also to propose projects for implementation, actively select them through voting, and then be involved in the implementation stage. **Example.** In Belgium, in Tielt authorities introduced an online budget platform to involve the community in the multi-annual policy plan. Citizens can choose from the twelve policy areas, and funds are disbursed to policy areas in light of citizens' priorities (European Committee on Democracy and Governance & Mergel, 2021, p. 17).	Strengthen local democracy by encouraging civic participation by direct involvement into the budgeting process and local governance. Underrepresented and marginalised groups get the platform to voice their needs and priorities, ensuring that their concerns are addressed in public spending. Involving a diverse group of community members in budget decisions can lead to more informed and effective allocation of resources, as it reflects a broader range of perspectives and needs. Participatory budgets enhance a sense of ownership and responsibility among residents. Increased transparency and accountability in how public funds are allocated and spent, helping to build trust between citizens and government officials. Participatory budgeting fosters civic education by helping citizens understand the complexities of budgeting and governance.	Limited Participation: The effectiveness of participatory budgeting is contingent upon involvement of diverse and representative groups. If insufficient, it may exacerbate existing inequalities rather than mitigate them. Also, the process is vulnerable to manipulation by organised interest groups, which can skew resource allocation and divert attention from broader community needs. Participatory budgeting sometimes prioritises immediate, visible projects at the expense of long-term or less tangible needs, potentially neglecting important but less immediately gratifying issues. Participatory budgeting might become formal and lack substantive influence on budgetary decisions. Elected officials and other stakeholders may exhibit resistance to participatory budgeting, potentially resulting in conflicts or undermining the process.

	Description	Opportunities	Challenges and Threats
Citizen services	Citizen services are part of the Government-to-Citizen (G2C) communication within the scope of E-government. G2C provides a wide range of services such as information dissemination to the public, delivery of basic services such as licence renewals, issuing of birth/marriage certificates, filing income taxes etc (Hague, Pathrannarakul, 2013, 26). **Example.** Ukrainian mobile applications "Kyiv Tsyfrovyi" and "Diia" that provides citizens with digital access to 120 government services on local and national levels and enables them to engage with the authorities (USAID, 2023).	The improvement of accessibility: the UN E-Government Survey 2020 says that e-government services enhance accessibility to public services for citizens at the local level. E-services promote two-way interaction between authorities and citizens. E-services also improve openness and strengthen transparency of governments (UN E-Government Survey, 2020, p. 105). By providing digital channels for service delivery, governments can overcome geographical barriers.	The main concern is the issue of privacy and potential security breaches or data leaks. Vulnerability to technical or infrastructural glitches and disruptions or overflows. AI tools may discriminate against minorities, potentially reversing decades of progress towards equality. For example, AI in healthcare may harm human health if algorithms are incorrect or biassed, while AI in welfare or migration may make unfair decisions on eligibility (Jones, 2023).
		By transforming the processes of certificate issuing or licence renewals into non-personalised and less time consuming, e-services also minimise the potential corruption. The integration of AI into governance potentially shifts administrative autonomy to the "algorithm level", which may empower decision-makers and facilitate governmental	

	Description	Opportunities	Challenges and Threats
		processes. In turn, the automation and acceleration of governance processes have a positive impact on democratic processes as a whole (Neudert & Howard, 2020).	

How to apply within SHAPEDEM-EU – «Democratic Toolbox» Guiding Questions:

1. Does digital or online communication really transcend social, political, cultural etc. boundaries, or if people are still rather communicating in their 'bubbles' like in their offline communication.
2. Does a particular tool facilitate the exchange of knowledge between communities of practice, particularly between insiders and outsiders?
3. For every tool: are there groups that particularly benefit from it in a case country? Similarly, are there any groups that are excluded or disempowered by it?
4. What are the differences or specifics of how these tools are applied and implemented in the case countries?
5. Are there regional or country differences in how the negative aspects of particular tools are manifested?
6. Has the EU supported development and/or implementation of any of those tools in the case country?
7. Which (is any) of those tools are used for democracy contestation in the case country?

Table 2 Autocratic Toolbox

	Authoritarian or Negative Usage	Potential Positive Usage
Surveillance Systems and Dataveillance	Distinguishing legitimate surveillance from unlawful/authoritarian digital surveillance poses a particular challenge (Feldstein, 2019). The scale and in-depth detailing of the information provided by big data and AI, particularly facial recognition, often surpass those required by security and safety measures thus violating people's freedoms and right to privacy. This gives the authorities the opportunity to monitor the public online and offline, target peaceful demonstration and protest participants, and crack down on independent media and organisations. To describe countries (including democratic) where technologies are widely used with the aim to monitor, identify, and target, the term 'digital welfare state' was coined (Alston, 2020) – and its meaning is not as positive as it seems at first sight. An outstanding example of digital surveillance is China's control over the Uyghur population through the use of such tools as biometrical identification, for which sensitive data such as DNA and iris scans are collected (Głowacka et al, 2021) or AI (Mozur, 2019). Surveillance can be seen in the form of microtargeting. It is monitoring people's online behaviour and using the collected data for delivering personalised content to users (Jovanović, 2023, p.22). Online microtargeting presents challenges to democracy, as it allows political parties to potentially misrepresent themselves as different one-issue entities to distinct individuals. The data collection associated with microtargeting also raises privacy concerns, highlighting potential difficulties for policymakers in regulating this practice (Zuiderveen Borgesius et al., 2018).	Surveillance systems primarily have the potential to enhance public safety. They can contribute to the security of public spaces, helping to detect and prevent crimes, thereby protecting the innocent. Surveillance can expedite responses to emergency situations, such as fires, natural disasters, or other threats to the public. Modern surveillance systems optimise traffic flow and infrastructure management, improving citizens' quality of life and ensuring road safety (Feldstein, 2019; Herbert, 2023). AI serves as a powerful tool for ensuring security. Surveillance systems actively use it for real-time monitoring, data collection, and analysis, face recognition etc., allowing significantly accelerated responses to emergencies in public spaces, such as health crises (Herbert, 2023).

	Authoritarian or Negative Usage	Potential Positive Usage
	Using AI algorithms, users' activity on social media can be tracked by states or corporations thus increasing dataveillance. Thus, authoritarian regimes can then directly pressure opposition-minded citizens singled out based on their activity on social media (Jovanović, 2023, p.11).	
Censorship (and information control)	Authorities, especially in non-democratic countries can have a stronger grip on information flows and opinion formation by imposing strict regulations on web-platforms, moderating the media, and blocking certain types of content (Mantelassi, 2023). These regulations may also have a negative effect on social, cultural or educational rights of individuals and communities. In some cases, the regime's desire to limit the exchange of information and ideas and stop their streams in and out of the country finds its embodiment in creation of governmentally constructed centralised digital spaces where the state narratives dominate, and no opportunity is left for conducting critical discussions. **Example.** The most developed system for Internet censorship in our time is "the Great Firewall" operating in China. It limits data flows to and from the "outer" world and filters content thus creating a 'splinternet' from the global Internet that appeared due to content filtering (Kerner, 2022).	Censorship instruments might be used to fight mis/disinformation and propaganda as well as limit the access to public of terrorist and organised crime groups.
Misinformation and Disinformation	**Misinformation** refers to false or inaccurate information, often spread without the intent to deceive. Examples include rumours, insults, and pranks. Misinformation can result from the lack of media literacy among users, leading to the unintentional sharing of inaccurate content. (The UN Refugee Agency, 2021, p. 230) Additionally, unprofessional or unscrupulous media sources may contribute to the spread of misinformation. **Disinformation** is intentional and includes malicious content such as hoaxes, spear-phishing, and propaganda. It spreads fear and suspicion among the population (The UN Refugee Agency, 2021, p. 230). Disinformation is disseminated with the explicit purpose of deceiving and achieving specific desired results. As a tool of disinformation, authoritarian regimes actively	

	Authoritarian or Negative Usage	Potential Positive Usage
	utilise fake news, defined as "an original article/media report containing completely inaccurate information and content not based on facts." Creating and spreading alternative narratives plays a significant role in distorting perceptions of real events. By reshaping the public discourse with false information, governments lower citizens' tendency to doubt the existing rule and partake in protest activities (Jovanović, 2023). Fake news and disinformation are also used to fuel hatred and discrimination against minority groups, or to convince the people of any other biassed cause. The recent years brought about deepfake technologies performed by AI, which exploit appearance and voice records of trusted persons to generate convincing media materials. **Examples.** Talking about disinformation campaigns, the Trump administration was accused of funding the Iran Disinformation Project, which, as was found out later, had been targeting US journalists that have voiced 'incorrect', as perceived by the authorities, opinions on Iran's development and its relations with the US (by stating that it needs to be democratised using peaceful means). Such targeting was done through bot-mobbing, undermining the work of the journalists and labelling them as Tehran's 'mouthpieces' and 'collaborators' (Rezaian, 2019). Propaganda and fake news are integral components of Russia's current information policy. The Gerasimov Doctrine, a modern Russian informational operations strategy, encompasses hacking services, instrumentalizing media, creating fake news, leaking information, and using conventional and asymmetric military means (Jovanović, 2023, p.19)	
Cyberattacks and hacking	Hacking, generally, is a manipulation of a piece of information without the consent of the owner of said information. Hacking is used by governments all over the world in 3 main ways: messaging control, causing damage to systems and devices, and surveillance or intelligence gathering. Such actions could amount to a whole constellation of human rights violations	

	Authoritarian or Negative Usage	Potential Positive Usage
	ranging from right to private life to right to freedom of assembly. Overall, hacking by the authorities may affect society in a negative way and bring about financial, reputational and other causal harm to individuals. **Example.** Government hacking of dissidents' phones in Saudi Arabia and the United Arab Emirates are great examples of the degree of harm such actions could inflict upon the rights of individuals (Marczak et al, 2018). It can be stated that cyberattacks pose the same degree of harm as hacking when assessing the possibility of grave human rights and democratic principles violations.	
Internet shutdown	In extreme cases, when authoritarian governments are failing to restrain online activities of protesters and opposition, they resort to full shutdown of the Internet and put citizens into digital isolation and informational deprivation for lengthy periods of time. Usually, such measures are used in times of political crises and conflict related scenarios; and potentially, such restrictions could be used as a coverup of genocide, crimes against humanity and other acts that contradict international law. Internet shutdowns have greatly impacted the ability of people to gather for protests, and, according to reports, a correlation between access to the internet and the brutality of protest crackdowns exists. Furthermore, internet shutdown leaves people in an informational vacuum that can negatively affect a myriad democratic institutions, such as hindering elections (Rosson et al, 2022).	
Targeted arrests and violence based on online activity	Freedom on the Net research of 2023 showed that around the globe 78% of people with access to the Internet live in countries where individuals were arrested for posting political, social, or religious content, and 67% live in countries where individuals were physically attacked or killed for their activity online (Shahbaz et al, 2023). **Example.** In 2021, members of Jehovah Witnesses in Russia-occupied Crimea faced extremism charges for holding religious service on Zoom with a penalty of up to 10 years of imprisonment	

	Authoritarian or Negative Usage	Potential Positive Usage
	(Coynash, 2021). Some members of religious minorities were prosecuted for posting videos of religious nature and faced fines and prison sentences while others were fined almost a monthly wage for not posting the full name of their religious organisation on social media or their official websites (Corley, 2020). Such actions by regimes gravely violate rights such as freedom of religion and even might evolve into crimes against humanity.	

How to apply within SHAPEDEM-EU – «Autocracy Toolbox» Guiding Questions:

1. For every tool: are there instances or practices of their usage in the case countries?
2. For every tool: can it be mitigated by democracy support policies?
3. What are the differences or specifics of how these tools are applied and implemented in the case countries?
4. Have the EU policies helped to mitigate any of those tools in the case country?
5. Are any of those tools used in a positive sense or aspect in the case country?

4 Merging Two Cross-cutting Issues: Five Considerations on Gender and Digitalisation

Digital transformation is a cross-cutting and complex issue, and so it affects many aspects of our lives with no exception for gender issues. While there are different challenges, this chapter will focus on the digital gender divide, online violence and harassment, gender-biassed algorithms, data privacy and body politics. Still, while focusing on the challenges, it is important to remember that digital transformation enabled women activism and participation in places and spheres traditionally dominated by males. For example, there is a massive amount of literature on women participation in the Arab Sring and the role blogging and cyberactivism played in it (Newsom and Lengel, 2012). Particularly important for women engagement had been such social media as YouTube, Twitter, Flickr, and Facebook in mobilising supporters, organising events and protests, and in blogging reflections on current issues (Radsch, 2012; Newson and Lengel, 2012).

One of the main assumptions about the digital gender divide is that women and girls are less likely to have access to and use technology than men and boys. For example, the International Telecommunication Union (ITU, 2022) stated that worldwide, the majority of people who are not connected to the Internet are women and girls. The most challenging situation is in the least developed countries where "only 19% of women used the Internet in 2020, compared to 86 per cent in developed countries in 2019". Furthermore, WebFoundation showed that women are less likely than men to have internet access, and there is a need to use a women-centred approach to understand this gap (Iglesias., 2020). Overall, globally, the replication of gender inequalities with new digital technologies also limits women's access to the digital sphere and online participation and engagement in civic processes.

According to the Pew Research Center report (2017), about 40% of Americans have personally experienced online harassment. However, women are more likely than men to experience online harassment, with 21% of women (aged 18-29) reporting being sexually harassed online compared to 9% of men in the same age group. Here online harassment includes cyberstalking, cyberbullying, and revenge porn. Thus, this disproportion also affects women's ability and security to participate in online activities.

Another common challenge is related to algorithms used in recruitment, credit scoring, and advertising can perpetuate gender biases and result in discriminatory outcomes. The classic example of Amazon's biased recruitment algorithms (Dastin, 2018) created a massive public debate, but it is hard to estimate how unbiased any future algorithm will be. While many algorithms remain black boxes, anyone and not only women or other vulnerable groups may be harmed or discriminated against. Thus, new 'black box' algorithms could contribute to social and gender inequalities.

That is also related to data privacy and body politics. For example, the poorest accuracy of facial recognition technologies is often found in relation to subjects who are "female, Black, and 18-30 years old" (Najibi, 2020). However, data privacy concerns are relevant for people of any gender as government surveillance programs or other actors could be collecting personal data without informed consent.

Another issue to consider regarding DT and gender is the representation of women in tech companies. Overall, there is a clear need for evidence-based policymaking regarding gender issues and/in digital transformation.

How to apply within SHAPEDEM-EU – Some Guiding Questions:

1. Which of the mentioned problems linking gender and digital transformation are present in the case country?

2. Are there any gender differences in how digital democracy instruments are utilised in the case country?

3. Are there any EU policies mitigating negative effects of DT on gender equality?

5 EU Policies Regarding Digital Instrument for Civic Engagement and Good Governance

It is important to list EU policies in the domain of digital democracy related to enhancement of good governance and facilitation of people's engagement and meaningful participation. Overall, these policies are aimed at democracy support and, as such, could be extended to other regions, particularly those where the EU is heavily involved in supporting democracy, democratic practices and processes, and democracy learning.

One of the main initiatives is The Digital Service Act package[2], which is composed of "the Digital Services Act" (DSA) and "The Digital Market Act" (DMA). The Digital Services Act (DSA) mandates Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) to conduct thorough assessments and to implement mitigation measures for systemic risks that the use of their services poses to civic discourse and electoral processes (Articles 34 and 35). Still, researchers are already discussing what might be the DSA's potential negative effects on civic discourse and electoral processes and how to assess and mitigate them. Most recent is the analysis by Calabrese and Reich from the European Partnership for Democracy and Liberties. It should be highlighted that risks to civic discourse are identified through the characteristics of civic discourse conducive to a well-functioning democracy. As such, civic discourse must be inclusive, pluralistic and accessible as well as recognize and respect different sociopolitical viewpoints and divisions. Also, it should show a commitment to facts and informed dialogue, must build citizen awareness and knowledge on pertinent issues, and enable citizen engagement and representative attention (Calabrese and Reich, 2024). Digital instruments, especially within Very Large Online platforms and search engines and under DSA and DMA not only can enhance civic discourse and democracy processes, but also to obstruct them, turning the very same regulations that are there to protect them against them. Thus, it is expected that in August 2024, amended guidelines and regulations will be released to better assess and mitigate risks and to facilitate civic discourses and electoral processes digitally.

Other major **comprehensive initiatives** include:

1. The "European Democracy Action Plan"[3] adopted in 2020 aims to build more resilient democracies among Europe. It includes strengthening media freedom and countering disinformation as key to ensure free and fair elections. It is a milestone in the European approach to disinformation, it moves from considering it a mere threat to security to giving the status of one of the three pillars of defence of European democracy.

2. The Defence of Democracy[4] package was put forward on 12 December 2023. "The central piece of this package is a legislative proposal that will enhance transparency and democratic

[2] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
[3] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250
[4] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6453

accountability of interest representation activities on behalf of third countries which are aimed at influencing policies, decision making and the democratic space. It also includes two recommendations which aim to promote free, fair, and resilient elections and the participation of citizens and civil society organisations in policymaking."

3. Human Rights and Democracy Action Plan 2020-2024[5] focuses on five interlinked and mutually reinforced lines of actions opened by new technologies in democratic societies. "It will also identify ways to tackle challenges and to harness opportunities offered by the impact of new technologies on human rights and democracy."

4. The Digital Europe Programme 2030[6] aims to ensure an inclusive, transparent, and open digital environment as well as close the digital gap and incentivise gender equality in digital competencies. Among other things, it aims to ensure "online participation in democratic life for everyone, with public services, health and care services accessible in a trusted and secure online environment, in particular for disadvantaged groups (…) 100% online accessible digital public services and 100% access for EU citizens to their electronic health data and to secure means of electronic identification recognised EU wide".

5. The Digital Democracy Initiative (2023-2026)[7] between Denmark and the EU, with an 11M€ contribution from the EU, promotes digital rights, resilience, and inclusion and empowers individuals. "Led by Denmark, the Digital Democracy Initiative supports the use of digital technologies to strengthen the digital resilience and security of pro-democracy civil society actors and to increase civic engagement in restrictive contexts. The initiative provides civil society with tools to fight disinformation and polarisation and to promote freedom of association and freedom of speech. The initiative also addresses the inequalities in digital access and digital marginalisation that are particularly evident for women and youth."

Two other initiatives are particularly aimed at facilitation of **e-voting and electoral processes**:

1. The European Cooperation network on Elections[8]. To ensure transparent and fair 2019 elections to the European Parliament, the Commission supported member states to establish

[5] https://international-partnerships.ec.europa.eu/policies/peace-and-governance/human-rights_en#human-rights-and-democracy-action-plan-2020-2024
[6] https://eur-lex.europa.eu/En/legal-content/summary/2030-digital-decade-policy-programme.html
[7] https://international-partnerships.ec.europa.eu/news-and-events/news/promoting-inclusive-democracy-digital-age-eu-and-denmark-launch-digital-democracy-initiative-2023-03-29_en
[8] https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/eu-citizenship-and-democracy/democracy-and-electoral-rights/european-cooperation-network-elections_en

the European Cooperation network on elections. This network allows to exchange practical and discussion on topics relevant to free and fair elections, including data protection, cyber-security, transparency, and awareness raising.

2. Electronic Identification and Trust Services[9] (Regulation 910/2014) on electronic identification and trust services for electronic transactions in the internal market. It creates a cross-border legal framework to ensure the interoperability of electronic identification systems in all EU member states removing barriers to grant validity to electronic identification and e-signatures systems.

Several EU initiatives are aimed at enhancing **transparency, accountability, and citizen services** through digital tools:

1. Proposal for a Directive[10] (29 March 2023) aims to further expand and upgrade the use of digital tools and processes in company law and to enhance transparency about companies and trust.

2. The Data Governance Act[11] entered into force on 23 June 2022 and is applicable from September 2023. It seeks to increase trust in data sharing and to increase data availability.

3. The digital gateway and Your Europe[12] provide online access to information, administrative procedures, and assistance service to the EU citizens and businesses.

Still, the implementation of digital tools and policies could not proceed without attention to the protection of people's civil rights. Thus, there are EU initiatives and policies aimed at **regulating online surveillance/dataveillance** and protecting people's right to privacy and other freedoms.

Directive 95/46/EC[13] (24 October 1995) on the protection of individuals with regards to the processing of personal data and on these data free movement states, "(36) Whereas where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established." In 1996, to follow up the Art. 29 of Directive 95/46/EC, the Data Protection Working Party[14] on the Protection of Individuals with regard to the processing of Personal Data was created. It

[9] https://eur-lex.europa.eu/eli/reg/2014/910/oj
[10] https://commission.europa.eu/publications/proposal-directive-further-expand-and-upgrade-use-digital-tools-and-processes-company-law-all_en
[11] https://digital-strategy.ec.europa.eu/en/policies/data-governance-act
[12] https://single-market-economy.ec.europa.eu/single-market/single-digital-gateway_en
[13] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046
[14] https://ec.europa.eu/newsroom/just/document.cfm?doc_id=44100

was an independent European Union advisory body on data protection and privacy and provided expert advice to the Member States regarding data protection. Nowadays, it has been replaced by

Directive 95/46/EC was replaced in 2016 by the Regulation (EU) 2016/679[15] of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Article 56 states: "(56) Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established." Similarly, the Data Protection Working Party of 1996 has been replaced by the European Data Protection Board. The European Data Protection Board[16] is an independent European body with legal personality that ensures cooperation and that the General Data Protection Regulation[17] and the Law Enforcement Directive[18] are applied consistently.

Another set of initiatives is aimed at **combating misinformation and disinformation**.

The High-Level Expert Group on Fake News and Online Disinformation[19] conceptually framed all the EU initiatives dealing with mis/disinformation. In January 2018, the final report of a high-level group of experts set by the European Union to advise on policy initiatives to counter fake news and disinformation spread online was published. It recommended enhancing transparency of online news, promoting media/information literacy and tools for empowering users and journalists, safeguarding the diversity and sustainability of the European news media ecosystem, and promoting continued research on the impact of disinformation in Europe.

One of the most important initiatives has been the introduction of a reinforced EU toolbox to counter foreign information manipulation and interference (FIMI)[20] whose objective is to impose costs on the perpetrators. The FIMI toolbox includes a range of available tools: situational awareness among others through the Rapid Alert System; the Single Intelligence Analysis Capacity, in particular its Hybrid Fusion Cell; resilience and capacity building; regulatory and diplomatic responses.

In 2018 and just ahead of the European Elections, The Action Plan against disinformation[21] was launched. It contains a set of actions to build up capabilities and strengthen cooperation among member states to address disinformation. It includes such measures as investing in digital tools and data analysis skills, regular reporting, the Rapid Alert System to provide alerts on disinformation campaigns, active participation of civil society, etc.

Another initiative set up the StratCom Task Force to address Russia's disinformation campaigns. The action plan on strategic communication was drafted by the High Representative in cooperation with EU institutions and Member States in March 2015. The Task Force is part of the Strategic Communication and Information Analysis Division of the European External Action Service. It includes

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679
[16] https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_en
[17] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679
[18] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680
[19] https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation
[20] https://data.consilium.europa.eu/doc/document/ST-11429-2022-INIT/en/pdf
[21] https://www.eeas.europa.eu/sites/default/files/disinformation_factsheet_march_2019_0.pdf

the Western Balkans Task Force, the Task Force South, the East StratCom Task Force[22], and a horizontal team focusing on emerging threats, data analysis, etc. These task forces are communication teams that collaborate with fact-checkers and foundations to denounce the dissemination of fake news by Russia. The East StratCom Task Force was formalised on May 12, 2018, with the adoption of the Disinformation Action Plan in light of hybrid threats faced by the EU and its member states. It also aims to communicate about the EU policies in the Eastern Neighbourhood, strengthen the media environment and support media freedom. The East StratCom Task Force also set The EUvsDisinfo platform[23] "to better forecast, address, and respond to the Russian Federation's ongoing disinformation campaigns affecting the EU, its Member States, and countries in the shared neighbourhood".

A Strengthened Code of Practice on Disinformation[24] ensures more accountability of online platforms to prevent the spread of disinformation. It was signed on 16 June 2022 following the guidance adopted by the Commission in 2021 on how to strengthen the existing EU code. The Code is a self-regulatory agreement, a non-binding document by the Commission which sets a co-regulatory framework in line with the Digital Services Act[25]. The Code of Practice and Disinformation is a "first-of-its-kind tool": relevant players in the industry, - including major and specialised online platforms, online advertising industry, research and civil society, and fact-checkers, - agreed for the first time in 2018, on self-regulatory standards to fight disinformation. The Code states that "relevant Signatories commit to put in place or further bolster policies to address both misinformation and disinformation across their services, and to agree on a cross-service understanding of manipulative behaviours, actors and practices not permitted on their services" (page 15). It also covers AI uses limitations and Media Literacy initiatives (page 19). This new Strengthened Code is part of a broader regulatory framework, in combination with the legislation on Transparency and Targeting of Political Advertising and the Digital Services Act.

As could be seen, all the EU policies and regulations regarding DT are complex and multidimensional. They are also a work in progress and, as such, are constantly revised to be better tailored to meet emerging challenges. It is also important to keep in mind that all these policies are declared to uphold and safeguard civil rights and democratic practices, thus having a democracy support component.

How to apply within SHAPEDEM-EU – Some Guiding Questions:

1. Could any of these EU policies be reproduced in the case country? What changes (to the policy) might it entail?
2. What communities of practice are needed to adjust any of these EU policies to the local context in the case country?
3. Could any of these EU policies be used for democracy contestation?

[22] https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en
[23] https://euvsdisinfo.eu/about/
[24] https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation
[25] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

4. It is postulated that these policies support democracy and human/civil rights. But could any of these policies or their components limit such rights or contest democracy?

6 Digital Transformation and Media Literacy

The globalised information streams, free access to information, and unprecedented freedom of speech need skills of media literacy, which means to make informed decisions about the content and information individuals encounter daily as well as critically assess media content from various sources, understand media production processes, including data usage, algorithms, and AI influences, and responsibly use digital media services (Chapman, Bellardi, Peissl, 2020, p. 8). Digital technologies play an important role in enhancing media literacy by expanding access to information and providing tools for critically evaluating media content and distinguishing reliable information from manipulation and fake news (Cho et al., 2022). Digital tools make fact-checking and media education easier and more accessible, thus helping citizens develop critical thinking skills and responsible media consumption habits.

In recent years, the concept of media literacy has expanded and become more inclusive. Now, critical media literacy analyses outcomes of social production and struggle and teaches students to be critical of media representations and ideologies while also stressing the importance of learning to use the media as modes of self-expression and social activism (Kellner & Share, p. 6). It is much more than just technological skills, and authors promote a sociological understanding of media literacy as a social practice (Peissl, 2023).

According to Hobbs, media literacy teaches five essential competencies — access, analysis and evaluations, creation, reflection, and action (2010, p. 18). People are taught how to find and use media and technology proficiently (to access) and how to use "critical thinking to analyse message quality, veracity, credibility and point of view" (to analyse and evaluate). Furthermore, once people acquire the skills in processing materials, they learn how to "compose or generate content using creativity and confidence in self-expression" (to create), and then apply "social responsibility and ethical principles to one's own identity and lived experience" (to reflect). The final stage is to act — work alone or as a member of the community to solve problems and share knowledge (Hobbs, 2010, p. 19). Hobbs discusses the following instructional practices of digital and media literacy education: keeping a media-use diary; using information search and evaluation strategies; reading, viewing, listening and discussing; close analysis; cross-media comparison; gaming, simulation and role-playing and multimedia composition (2010, p. 23).

McDougall et al. claim that media literacy is taught at schools in a cross-curricular way and that in the EU, as of 2014, media education is not a separate subject. Therefore, there is a need to create "a spiral and serialist media education" to improve media literacy competencies at different school levels (2018, p. 50). Also, there are different approaches to teaching media education. For example, in Germany, the concept of "media competence" is perceived as a technical media competence in non-educational contexts while in educational contexts it is about "the ability and the willingness to deal with media in an adequate, autonomous, creative and socially responsible way. (2018, p. 42). Although authors (2018, p. 42) characterise media education in the UK as a well-defined and well-developed field, Buckingham expresses its dissatisfaction with it. He points out that media literacy has been used as a solution to the problems when the government is unable or unwilling to regulate the media market (2020, p. 234).

Media literacy is, therefore, used as an alternative to regulation when responsibility passes from the government to the individual. The problem is that instead of looking at the core causes of such problems as cyberbullying, addiction, and drugs, policymakers look at the symptoms and by utilising media literacy practices, they develop "quick fix" solutions. Although media literacy provides a democratic alternative, this "solutionism" is not necessarily beneficial for society (Buckingham, 2020, p. 234). Similarly, O'Neill argues that "children are expected to negotiate the risks and opportunities of the online world with diminishing degrees of institutional support from trusted information sources" (2010, p. 323), and the responsibility of media effects monitoring is put on individuals rather than media creators, social media platforms or regulators (Bulger & Davison, 2018, p. 15).

While there are scholars who have done comprehensive reviews of all the **EU's initiatives and regulations on Media Literacy** (Goodman, 2021), we will list only the major ones here.

Media literacy is an important part of more comprehensive policies. For example, the European Strategy Better Internet for Kids (BIK+)[26] adopted on 11 May 2022 is to ensure that children are protected, respected, and empowered online in the new Digital Decade. It proposes actions around three pillars: 1) safe digital experiences to protect children from harmful and illegal online conduct; 2) digital empowerment to acquire the necessary skills and competencies; and 3) active participation through fostering innovative and creative safe digital experiences. Also, the European Democracy Action Plan[27] (December 2020) proposes that one way to tackle disinformation is through empowering citizens by strengthening their media literacy. Also, there are periodical reports of EU member states regarding their media literacy policies and implementation of relevant initiatives in line with the EU Commission guidelines (National reports on media literacy, 25 May 2023).

The Revised Audiovisual Media Services Directive (AVMSD)[28] was adopted by the Council in 2018. Member States had until September 2020 to transpose the AVMSD into their national legislation. It includes new elements such as an extension of certain audiovisual rules to video-sharing platforms, better protection of minors against harmful content in the online world, reinforced protection against incitement to violence or hatred on television, etc. The European Regulators Group for Audiovisual Media Services (ERGA)[29] function is to ensure the consistent implementation of the Revised AVMS Directive across the European Union.

The European Media Literacy Week[30] is one of the biggest initiatives by the European Commission to promote media literacy skills and projects across the EU. A variety of institutions organise their own events during the week to celebrate and discuss media literacy. Connected to this initiative is the **European Media Literacy Award,** which celebrates inspiring and impactful projects in the field of media literacy. The applicants are invited to Brussels to compete for the three awards at the conference within the European Media Literacy Week. For example, "Superheroes on the Internet!" was among 10 projects selected for the European Media Literacy Awards in 2019. It is a project from the Ministry of Culture of Latvia to build a social campaign for media literacy and Internet safety for 5-8-year-olds. The campaign employs 5 animated videos addressing risks and opportunities on the

[26] https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids
[27] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250
[28] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1464618463840&uri=COM%3A2016%3A287%3AFIN
[29] https://erga-online.eu/
[30] https://digital-strategy.ec.europa.eu/en/library/report-2022-european-media-literacy-week

Internet. The project was launched in schools, offering children the chance to earn "superpowers" and earn a diploma, with teachers and other interested parties being granted free access to the methodological recommendations to use these videos in the school curriculum.

The Media Literacy Expert Group[31] has been formed to identify good practices in the field of media literacy, facilitate networking between different stakeholders and explore ways of coordinating EU policies, support programs and media literacy initiatives.

Another initiative is the Digital Education Action Plan (2021-2027)[32] adopted on 30 September 2020. Its objective is to increase and improve media literacy, help the EU countries' educational systems' adaptation in the digital era, explore the opportunities and advantages of the Internet for online education.

The European Platform of Regulatory Authority[33] is one of the oldest initiatives created in 1995. It is a forum for informal discussion and exchange of views. As it says, "EPRA produces a wealth of comparative working documents, presentations, and information on media regulation. EPRA Website is thus a unique source of non-academic knowledge on the implementation of media regulation in Europe and on regulatory authorities. Powerful search tools allow you to browse through the numerous working documents."

Chapman, Bellardi and Peissl elaborate on how media literacy can be employed to strengthen marginalised communities. Community media sectors regard media literacy as an essential form of their activities, among which are training the public in media production, participating in policy development, and collaborating with other organisations to promote media literacy (2020, 13). One of the media literacy projects is the "Hear We Are Project" in Bradford, UK. Together with Bradford Community Broadcasting and Farnham Children's Centre in the UK, a group of female activists formed a radio production team and involved more women, including Muslim women within local media (Chapman, Bellardi, Peissl, 2020, p. 15).

Thus, media literacy is an important component of democracy support policies. Despite posing several ontological questions whether the major bulk of responsibility lies on the state as the regulator or a person/citizen as consumer and user, the attention should still be paid to the enhancement of media literacy if we perceive democracy as a social practice where an individual/citizen is a key player. Media literacy also may be viewed as an element of democratic learning.

How to apply within SHAPEDEM-EU – Some Guiding Questions:

1. Are there particular media literacy initiatives in the case country? Are they efficient?

2. How do we measure the effectiveness of media literacy programmes?

[31] https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&do=groupDetail.groupDetail&groupID=2541

[32] https://education.ec.europa.eu/focus-topics/digital-education/action-plan

[33] https://www.epra.org/articles/general-information-on-epra

3. Is media literacy a concept that is present and developed in democracies as it directly opposes the 'post-truth' discourse and inherently cynical rhetoric typical for some autocratic regimes that there is no truth, no facts, and that everyone is lying or deceiving for their benefit?

4. Does media literacy require not only critical thinking, but also the ethical and moral dispositions, values and orientations that allow for clear distinction between truth and fake/lie and between right and wrong?

Conclusions

Digital transformation, democracy, democracy support and democracy learning are similar in the sense that they all are complex dynamic processes with many aspects and components. Partly, that is where some of the conceptual challenges lie - as complex, multifaceted, and dynamic phenomena are extremely hard to define and pinpoint to one clear definition or concept or even to a set of concepts.

If we consider the technological side of DT and look at it as an evolution and development of multiple techniques, technologies, and digital instruments, including AI algorithms, such advancement and tools are neither inherently democratic/positive nor autocratic/negative. The same social media platform or AI instrument that allow us to share and search for our personal photos or footage and photos that are publicly important evidence of committed war crimes are also places where fake pictures and films are posted and shared or where some people might become involved into misinformation or disinformation campaigns intentionally or even without their knowledge. As any other instruments, digital ones might be equally used for “good” or for “bad”. Thus, it comes to us to critically assess digital processes by enhancing our media literacy and knowledge of digital solutions and it comes to democracies/democratic states to ensure that democracy support and democracy learning policies are extended to encompass the digital sphere with all its specifics while maintaining and securing human and civil rights of people.

In this paper, we presented a conceptual framework to analyse DT and digital instruments and solutions in the context of democracy, and particularly - democracy support and contestation. Thus, it might be useful for the SHAPEDEM-EU work packages. The theoretical framework could be particularly important for uncovering the differences and regional context of different case countries and the EU neighbourhoods (WP2, WP3, WP4, WP6). The discussion of digital toolboxes can be of use for the analysis of case countries and the ways DS policies are implemented there (WP2 and WP3, also WP5). Also, the double-edged nature of all digital instruments and solutions should be considered in WP5.

References

Abbott, J. (2012). Social media. In Kersting, Stein, & Trent (Eds.), *Electronic Democracy* (1st ed., pp. 77–102). Verlag Barbara Budrich. https://doi.org/10.2307/j.ctvddzwcg.7

Ahmed, R.K., Ahmed, O., Pappel, I., Reitsakas, A., & Draheim, D. (2022). The Role of Digital Transformation in Fostering Transparency: An e-Court System Case Study. In Papagiannidis, S., Alamanos, E., Gupta, S., Dwivedi, Y.K., Mäntymäki, M., Pappas, I.O. (Eds.) *The Role of Digital Technologies in Shaping the Post-Pandemic World*. I3E 2022. Lecture Notes in Computer Science, vol 13454. Springer, Cham. https://doi.org/10.1007/978-3-031-15342-6_17

Alston, P. (2020, January 8). What the "digital welfare state" really means for human rights. *Open Global Rights.* https://www.openglobalrights.org/digital-welfare-state-and-what-it-means-for-human-rights/

Bennett, W. & Segerberg, A. (2012). The logic of connective action: Digital media and the personalization of contentious politics". *Information, Communication & Society*, *15*(5): 739-768. doi: https://doi.org/10.1080/1369118X.2012.670661

Berg, S. & Hofmann, J. (2021). Digital democracy. *Internet Policy Review, 10*(4). https://doi.org/10.14763/2021.4.1612

Berger, J. B. (2015). *E-government harm: An assessment of the Danish coercive digital post strategy*. Roskilde Universitet.

Bernholz, L., Landemore H., and Reich R., eds. (2021). Digital Technology and Democratic Theory. Chicago: University of Chicago Press.

Björklund, F. (2016). E-government and moral citizenship: the case of Estonia. *Citizenship Studies*, *20*(6–7), 914–931. https://doi.org/10.1080/13621025.2016.1213222

Buckingham, D. (2020). Epilogue: Rethinking digital literacy: Media education in the age of digital capitalism. *Digital Education Review*, (37), 230-239. https://doi.org/10.1344/der.2020.37.230-239

Bulger, M., & Davison, P. (2018). The Promises, Challenges, and Futures of Media Literacy. *Journal of Media Literacy Education*, *10*(1), 1–21. https://doi.org/10.23860/jmle-2018-10-1-1

Bund, J. (2016). *Cybersecurity and democracy: Hacking, leaking and voting*. European Union Institute for Security Studies (EUISS). http://www.jstor.org/stable/resrep06791

Calabrese S. and Reich O. (January 2024). Identifying, analysing, assessing and mitigating potential negative effects on civic discourse and electoral processes: A minimum menu of risks very large online platforms should take heed of. European Partnership for Democracy; Civil Liberties Union for Europe (Liberties). https://www.liberties.eu/f/mpdgy5

Castells, M. (2009). *Communication power*. Oxford University Press.

Chapman, M., Bellardi N., & Peissl, H. (2020). *Media Literacy for All. Supporting marginalised groups through community media.* Council of Europe. https://rm.coe.int/cyprus-2020-media-literacy-for-all/1680988374

Cho, H., Cannon, J., Lopez, R., & Li, W. (2022). Social media literacy: A conceptual framework. New Media & Society, 146144482110685. https://doi.org/10.1177/14614448211068530

Corley, F. (2020, November 20). CRIMEA: Fined after prosecutor "told us we'd get a warning". *Forum 18.* https://www.forum18.org/archive.php?article_id=2618

Council of Europe. (2017). *Study on the Use of Internet in Electoral Campaigns*. Council of Europe Publishing. https://rm.coe.int/study-on-the-use-of-internet/1680796298

Coynash, H. (2021 September 21). Violent persecution mounting of Jehovah's Witnesses in Russian-occupied Crimea. *Kharkiv Human Rights Protection Group.* https://khpg.org/en/1608809554

Dastin, J. (2018, October 10). Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters*.https://www.reuters.com/article/idUSL2N1VB1FQ/

Earl, J. (2010). The dynamics of protest-related diffusion on the web. *Information, Communication & Society*, *13*(2), 209–225. https://doi.org/10.1080/13691180902934170

Ellison, N., & Vitak, J. (2015). Social Network Site Affordances and Their Relationship to Social Capital Processes. In S. Sundar (Ed.), *The handbook of psychology of communication technology* (pp. 205-227). Boston: Wiley-Blackwell.https://doi.org/10.1002/9781118426456.ch9

European Committee on Democracy and Governance & Mergel, I. (2021, July 26). *Study on The Impact of Digital Transformation on Democracy and Good Governance.* https://rm.coe.int/study-on-the-impact-of-digital-transformation-on-democracy-and-good-go/1680a3b9f9

Feldstein, S. (2019). *The Global Expansion of AI Surveillance*. Carnegie Endowment for International Peace.*https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf*

Freedom House (2023). *Freedom in the World 2023: Marking 50 Years in the Struggle for Democracy. https://freedomhouse.org/sites/default/files/2023-03/FIW_World_2023_DigtalPDF.pdf*

Froomkin, M. (2004). Technologies for Democracy. In P. Shane (Ed.), *Democracy Online: The Prospects for Political Renewal Through the Internet* (pp. 3–20). https://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=182916

Fukuyama, F. (2000). Social capital and civil society. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.879582

Głowacka, D., Youngs, R., Pintea, A., & Wołosik, E. (2021). Digital technologies as a means of repression and social control. *European Parliament's Subcommittee on Human Rights.* https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653636/EXPO_STU(2021)653636_EN.pdf

Goldenziel, J. (2022, February 27). How to fight Russia's war crimes with your smartphone. *Forbes*. https://www.forbes.com/sites/jillgoldenziel/2022/02/27/how-to-fight-war-crimes-with-your-smartphone/?sh=55aa112fb4a6

Goodman, E. (2021, September). Media literacy in Europe and the role of EDMO, European Digital Media Observatory. https://edmo.eu/wp-content/uploads/2022/02/Media-literacy-in-Europe-and-the-role-of-EDMO-Report-2021.pdf

Górny, M. (2021). I-voting – opportunities and threats. Conditions for the effective implementation of Internet voting on the example of Switzerland and Estonia. *Przegląd Politologiczny*, (1), 133–146. https://doi.org/10.14746/pp.2021.26.1.9

Hacker, K. L. (2002). Network Democracy and the Fourth World. *Communications, 27*(2).https://doi.org/10.1515/comm.27.2.235

Hall, T. (2012). Electronic voting. In Kersting, Stein, & Trent (Eds.), *Electronic Democracy* (1st ed., pp. 153–176). Verlag Barbara Budrich. https://doi.org/10.2307/j.ctvddzwcg.10

Havens, T., & Lotz, A. D. (2016). *Understanding Media Industries*. Oxford University Press.

Herbert, N. (2023, November 2). Council post: Intelligent surveillance as AI tool for social good. *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2023/11/02/intelligent-surveillance-as-a-tool-for-social-good/?sh=bf324b52c1bb

Hobbs, R. (2010). *Digital and Media Literacy: A Plan of Action*. Washington, DC: The Aspen Institute.

Nyman-Metcalf, K. (2019). How to build e-governance in a digital society: the case of Estonia. *Revista Catalana de Dret Públic, 58.* https://www.raco.cat/index.php/RCDP/article/download/357190/449147

Iglesias, C. (2020, March 10). The gender gap in internet access: using a women-centred method. *World Wide Web Foundation*. https://webfoundation.org/2020/03/the-gender-gap-in-internet-access-using-a-women-centred-method/

International Telecommunication Union (ITU). (2022). *Bridging the gender divide*. https://www.itu.int/en/mediacentre/backgrounders/Pages/bridging-the-gender-divide.aspx

Jones, K. (2019, November 6). *Online disinformation and political discourse: Applying a human rights framework*. Chatham House. https://www.chathamhouse.org/2019/11/online-disinformation-and-political-discourse-applying-human-rights-framework

Jones, K. (2023, January 10). *AI governance and human rights*. Chatham House. https://www.chathamhouse.org/2023/01/ai-governance-and-human-rights/02-what-ai

Jones, M. (2022). The Two Faces of Digitalization in Politics: The Role of Social Networks in Political Mobilizations and the Threat of "Digital Authoritarianism" in the MENA Region. *European Institute of the Mediterranean*. https://www.iemed.org/publication/the-two-faces-of-digitalization-in-politics-the-role-of-social-networks-in-political-mobilizations-and-the-threat-of-digital-authoritarianism-in-the-mena-region/

Jovanović, M. (2022). Fighting for Democracy in the Era of Digital Authoritarianism. *Digital Forensic Center.* https://dfcme.me/wp-content/uploads/DM-ENG-WEB.pdf

Karimi, J., & Walter, Z. (2015). The Role of Dynamic Capabilities in Responding to Digital Disruption: A Factor-Based Study of the Newspaper Industry. *Journal of Management Information Systems, 32*(1): 39–81. https://doi.org/10.1080/07421222.2015.1029380

Kellner, D., & Share, J. (2019). The Critical Media Literacy Guide. Engaging Media and Transforming Education. *Brill*. https://doi.org/10.1163/9789004404533

Kerner, S. (2022). Great Firewall of China. *TechTarget.* https://www.techtarget.com/whatis/definition/Great-Firewall-of-China

Kersting, N. (2012). The Future of Electronic democracy. In Kersting, Stein, & Trent (Eds.), *Electronic Democracy* (1st ed., pp. 11–54). Verlag Barbara Budrich. https://doi.org/10.2307/j.ctvddzwcg.5

Koc-Michalska, K. & Lilleker, D. (2016). Digital Politics: Mobilization, Engagement, and Participation. *Political Communication, 34*(1), pp. 1-5, https://doi.org/10.1080/10584609.2016.1243178

Legner, C., Eymann, T., Hess, T., Matt, C., Böhmann, T., Drews, P., Mädche, A., Urbach, N., & Ahlemann, F. (2017). Digitalization: Opportunity and Challenge for the Business and Information Systems Engineering Community. *Business & Information Systems Engineering*, *59*(4), 301–308. https://doi.org/10.1007/s12599-017-0484-2

MacKinnon, R. (2011). China's "Networked Authoritarianism". *Journal of Democracy*, *22*(2), 32–46. https://doi.org/10.1353/jod.2011.0033

Mantelassi, F. (2023, February 16). Digital Authoritarianism: How Digital Technologies Can Empower Authoritarianism and Weaken Democracy. *Geneva Centre for Security Policy.*

https://www.gcsp.ch/publications/digital-authoritarianism-how-digital-technologies-can-empower-authoritarianism-and

Marczak, B., Scott-Railton, J., Senft, A., Razzak, B., & Deibert, R. (2018). The Kingdom Came to Canada. How Saudi-Linked Digital Espionage Reached Canadian Soil. *The Citizen Lab.* https://tspace.library.utoronto.ca/bitstream/1807/95329/1/Report%23115--Kingdom%20Came.pdf

McCormack, C. B. (2016). Why Use Electronic Voting? *Democracy Rebooted: The Future of Technology in Elections*(pp. 6–8). Atlantic Council. http://www.jstor.org/stable/resrep03645.8

McDougall, J., Zezulkova, M., van Driel, B., & Sternadel, D. (2018). Teaching media literacy in Europe: evidence of effective school practices in primary and secondary education. *NESET II report.* Publications Office of the European Union. doi: 10.2766/613204

Moro Visconti, R. (2020). Corporate governance, digital platforms, and network theory: information and risk-return sharing of connected stakeholders. *MANAGEMENT CONTROL*, (2), 179–204. https://doi.org/10.3280/maco2020-002009

Morozov, E. (2012). *The net delusion: The dark side of Internet freedom*. New York, NY: PublicAffairs.

Mozur, P. (2019, April 14). One month, 500,000 face scans: How China is using A.I. to profile a minority. *The New York Times*. https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

Mynenko, S., Lyulyov, O. (2022). The Impact of Digitalization on the Transparency of Public Authorities. *Business Ethics and Leadership, 6*(2), 103-115. https://doi.org/10.21272/bel.6(2).103-115.2022

Najibi, A. (2020, October 24). Racial Discrimination in Face Recognition Technology. *Science In The News.* https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

National reports on media literacy measures under the Audiovisual Media Services Directive 2020-2022. (2023, 25 May). https://digital-strategy.ec.europa.eu/en/library/national-reports-media-literacy-measures-under-audiovisual-media-services-directive-2020-2022

Neudert, L.-M., & Howard, P. (2020). *Four Principles for Integrating AI & Good Governance*. Oxford Internet Institute. https://www.oii.ox.ac.uk/news-events/reports/four-principles-for-integrating-ai-good-governance/

Newsom, V. A. and Lengel, L. (2012) "Arab Women, Social Media, and the Arab Spring: Applying the framework of digital reflexivity to analyze gender and online activism," Journal of International Women's Studies: Vol. 13: Iss. 5, 31–45. https://vc.bridgew.edu/jiws/vol13/iss5/5

Norris, P. (2012). Political mobilization and social networks: The example of the Arab spring. In Kersting, Stein, & Trent (Eds.), *Electronic Democracy* (1st ed., pp. 55–76). Verlag Barbara Budrich. https://doi.org/10.2307/j.ctvddzwcg.6

Noveck, B. S. (2009). *Wiki Government: How Technology Can Make Government Better, Democracy Stronger, and Citizens More Powerful*. Brookings Institution Press.

O'Neill, B. (2010). Media Literacy and Communication Rights. *International Communication Gazette*, *72*(4-5), 323–338. https://doi.org/10.1177/1748048510362445

Opinion on democracy in the digital age (2023). European Commission, Directorate-General for Research and Innovation, European Group on Ethics in Science and New Technologies, Biller-Andorno, N., Céu Patrão Neves, M., Laukyte, M. et al., Publications Office of the European Union. https://data.europa.eu/doi/10.2777/078780

Peissl, H. (2023, September 12). Critical Media Literacy: From Concepts to Practice. *European Commission, EPALE.* https://epale.ec.europa.eu/en/blog/critical-media-literacy-concepts-practice

Pew Research Center. (2017). *Online harassment 2017*. https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/

Phillips, J. (2023, October 25). Telegram and Russia's FSB: An Uncomfortable Relationship. *Polynom*. https://www.polynom.app/blog/telegram-and-russia-fsb-relationship

Poiran, Syah Amin Albadry, Burhanuddin, & Sasmita Rusnaini. (2023). Digital Transformation and Its Role in Improving Democracy: A Systematic Literature Review. *Open Access Indonesia Journal of Social Sciences, 6*(3), 1004-1009. https://doi.org/10.37275/oaijss.v6i3.164

Radsch, C. (17 May 2012). "Unveiling the Revolutionaries: Cyberactivism and the Role of Women in the Arab Uprisings". James A. Baker III Institute for Public Policy. https://www.bakerinstitute.org/research/unveiling-the-revolutionaries-cyberactivism-and-the-role-of-women-in-the-arab-uprisings

Raja, D. (2016). *Bridging the disability divide through digital technologies*. Background Paper for the 2016 World Development Report: Digital Dividends. https://pubdocs.worldbank.org/en/123481461249337484/WDR16-BP-Bridging-the-Disability-Divide-through-Digital-Technology-RAJA.pdf

Reddick, C. G., & Aikins, S. K. (2012). Web 2.0 technologies and democratic governance. Public administration and information technology (Pp 1–7). Springer New York. https://doi.org/10.1007/978-1-4614-1448-3_1

Rezaian, J. (2019, June 4). The State Department has been funding trolls. I'm one of their targets. *The Washington Post.* https://www.washingtonpost.com/opinions/2019/06/04/state-department-has-been-funding-trolls-im-one-their-targets/

Römmele, A. (2012). Electronic political campaigning. In Kersting, Stein, & Trent (Eds.), *Electronic Democracy* (1st ed., pp. 103–124). Verlag Barbara Budrich. https://doi.org/10.2307/j.ctvddzwcg.8

Rosson, Z., Anthonio, F., & Tackett, C. (2023). *Weapons of Control, Shields of Impunity. Internet shutdowns in 2022.* Access Now. https://www.accessnow.org/wp-content/uploads/2023/05/2022-KIO-Report-final.pdf

Schiller, D. (2011). Power under pressure: Digital capitalism in crisis. *International Journal of Communication, 5*, 924–941. https://ijoc.org/index.php/ijoc/article/view/1226/577

Shahbaz, A. (2018). The Rise of Digital Authoritarianism. Freedom House. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

Shahbaz, A., Funk, A., Brody, J., Vesteinsson, K., Baker, G., Grothe, C., Barak, M., Masinsin, M., Modi, R., & Sutterlin, E. eds. (2023). Freedom on the Net 2023. Freedom House. https://freedomhouse.org/sites/default/files/2023-11/FOTN2023Final.pdf

Shenkoya, T. (2023). Can digital transformation improve transparency and accountability of public governance in Nigeria? *Transforming Government: People, Process and Policy, Vol. 17*(1), pp. 54-71. https://doi.org/10.1108/TG-08-2022-0115

Smith, B. (2022, February 28). Digital technology and the war in Ukraine. *Microsoft On the Issues*. https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/

Srnicek, N. (2017). *Platform Capitalism*. Polity Press.

The UN Refugee Agency. (2021). *Using social media in community-based protection: A Guide*. https://www.unhcr.org/innovation/wp-content/uploads/2021/01/Using-Social-Media-in-CBP.pdf

United Nations E-Government Survey *2020.* https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf

USAID. (2023, January 18). *A U.S.-Supported E-Government App Accelerated the Digital Transformation of Ukraine; Now Ukraine is Working to Scale the Solution to More Countries.* https://www.usaid.gov/news-information/press-releases/jan-18-2023-us-supported-e-government-app-accelerated-digital-transformation-ukraine-now-ukraine-working-scale-solution-more-countries

Van Dijck, J., & Poell, T. (2016). Understanding the promises and premises of online health platforms. *Big Data & Society*, *3*(1), 205395171665417. https://doi.org/10.1177/2053951716654173

Veeramani, K., & Jaganathan, S. (2020, September 30). Land Registration: Use-case of e-Governance using Blockchain Technology. *KSII Trans. Internet Inf. Syst., 14*, 3693-3711. https://doi.org/10.3837/tiis.2020.09.007

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems, 28*(2), 118–144. http://dx.doi.org/10.1016/j.jsis.2019.01.003

Wojcik, S. (2012). Open government and open data. In Kersting, Stein, & Trent (Eds.), *Electronic Democracy* (1st ed., pp. 125–152). Verlag Barbara Budrich. https://doi.org/10.2307/j.ctvddzwcg.9

Zuiderveen Borgesius, F. J., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., Bodo, B., & De Vreese, C. (2018). Online political microtargeting: Promises and threats for democracy. *Utrecht Law Review, 14*(1), 82. https://doi.org/10.18352/ulr.420