5 Transforming public governance for digital democracy

Digitalisation has opened new channels for citizen empowerment, political participation, and government transparency, enhancing people's civil liberties and political rights. At the same time, it has brought new risks to the effective exercise of civil liberties and political rights. This chapter looks at the role of public governance institutions in enabling and enhancing digital democracy, while mitigating the risks of digitalisation to democracy. In particular, it discusses how to safeguard the integrity of elections and protect the democratic debate, foster citizen participation in the digital age, promote government transparency and accountability in the digital era, and adapting institutions and legal frameworks for digital democracy.

5.1. Introduction: Getting the Future Right

The rapid digitalisation of societies, economies and governments is changing and challenging the traditional institutional mechanisms supporting the functioning of democracies. Digital technology is a fundamental driver of change in this century. It is reshaping all parts of society, including economies and governments, and impacting almost every aspect of people's lives. The way the digital transformation has proceeded has provided new opportunities to empower citizens but is also increasingly eroding traditional intermediation and the respect of human and civic rights and affecting polarisation significantly. Concerns about 'digital democracy' have emerged in recent years, with Governments being seen as slow in responding to these challenges. Developed for the analogue world where change is less rapid, institutional change regarding the democratic functioning of government also carries a fundamental weight for the future of societies and cannot be expected to take place as fast as digitalisation is proceeding. Nevertheless, low levels of trust and the many signs of citizens' disaffection in the way democracies are currently functioning require better leveraging the large potential of digitalisation for democracies while addressing the many challenges it has created.

The concept of digital democracy is still lacking a clear academic or political definition. In this paper, digital democracy refers to the functioning of democracy in the digital era and "how the use of digital technologies may influence the conditions, institutions and practices of political engagement and democratic governance" (Berg and Hofmann, 2021[1]; Daly, 2019[2]; Bermeo, 2016[3]).

From one perspective, digitalisation has opened new channels for citizen empowerment, political participation, and government transparency, enhancing people's civil liberties and political rights. It provides immense opportunities to make democracy work better bringing government institutions closer to people and centred on their needs while enabling new modalities and channels of citizen participation in public policy and democratic political life. It has also promoted transparency and openness in government practices and strengthened the accountability and oversight over public institutions. In particular, by opening government data and enabling its reuse, the "data revolution" (UN, 2014[4]) has boosted transparency in government, enabled greater responsiveness, and increased accountability through new analytics tools (OECD, 2020[5]; OECD, 2018[6]). Giving its cross-border nature, digitalisation also has important global dimensions affecting international relations and the conduct of diplomacy, with the emergence of digital foreign policies.

From another perspective, digitalisation has also brought new risks to the effective exercise of civil liberties and political rights, destabilised information ecosystems and democratic debate, further exacerbating the polarisation of societies, and increased the possibilities of (domestic and foreign) undue influence in open democratic processes. How democracy is exercised in the digital era is also affected by the degree of digital inclusion and the ability of all, including vulnerable groups, to participate in democratic processes. While progress has been made to expand connectivity, digital inequalities within and between countries remain. OECD countries show progress with 70% to 95% of adults using the Internet and smartphones becoming the favoured device for Internet access by 2019 (OECD, 2020[7]). Additionally, fixed broadband penetration (32.5 subscribers per 100 inhabitants in OECD countries) was more than twice the world's average (14.9 per 100) by June 2020 (OECD, 2021[8]). However, in many countries, digital exclusion affects the quality of democracy, limiting people's capacity to use the digital space as a tool for citizen empowerment. Around the world, 2.9 billion individuals, mostly women and girls, are missing out on the benefits of digital transformation to participate in democratic processes and voice their expectations about public services (ITU, 2021[9]). In authoritarian regimes, these risks are exacerbated with the abuse and misuse of new technologies as a tool for repression to control people, supress rights, stifle dissent, and, increasingly, undermine democracies abroad.

We are at a critical juncture for defining the digital future we want. The fundamental challenge, is defending digital democracy and ensuring a rights-based future, building a trust-based digital society and a value-based digital government. Governments in democratic societies are ultimately responsible for advancing the common interest and maintaining the legal, regulatory, and institutional frameworks and safeguards guaranteeing the respect of civil and political rights essential to the functioning of democracies. Individual parts of government should ensure this on a continuous basis as they develop policy and draft legislation. This includes considerations of where the legal and institutional frameworks may need to be adapted, revised, or replaced to respond to a rapidly changing context, along with the regulatory enforcement capacity.

The governments of OECD countries are increasingly taking steps to ensure a rights-based approach to digital transformation that is aligned with democratic principles and values and protects individual and collective rights. The work on these rights is currently being carried out at the OECD under the purview of the OECD Committee on Digital Economy Policy (CDEP). This debate typically emphasises the role of companies, governments, and regulators in upholding existing rights in the digital space and considering new rights for the digital era (or "digital-only rights").

This chapter essentially looks at the role of public governance institutions in enabling and enhancing digital democracy, while mitigating the risks of digitalisation to democracy. It reviews how digital tools and innovations positively and negatively affect the public governance mechanisms that underpin the functioning of advanced democracies. It takes stock of existing and emerging initiatives, and adjustments to regulatory frameworks, standards, and institutional mechanisms that governments are putting in place to strengthen the resilience of our democratic systems and values, and to better protect and promote democracy in the digital age. This chapter focuses on a subset of rights that underpin the functioning of democracy and are critical to its vibrancy in the digital era, namely civil and political rights, individual and collective.[1] As work in progress, it provides an initial perspective on the state of play and issues at hand, complementing the rest of the analysis of the OECD Reinforcing Democracy Initiative on Pillar 1 on Public Governance for Combating Mis and Dis-information (Chapter 1), Pillar 2 on Enhancing participation, representation and openness (Chapter 2) and Pillar 3 on Embracing the Global Responsibilities of Governments and Building Resilience to Foreign Influence (Chapter 3).

This chapter is the OECD's first attempt to look at the challenges of digitalisation to democracy from a public governance perspective. Section 5.2 addresses the impact of digitalisation of core electoral processes and the democratic debate; Section 5.3 discusses the transformation of citizen participation in the digital era; Section 5.4 analyses how digital democracy is enabling more openness, transparency, and accountability in government; while Section 5.5 reviews the refitting of public governance institutions for digital democracy, including the need for greater global co-operation and multilateral approaches.

5.2. Safeguarding the integrity of elections and protecting the democratic debate

Participation in elections is an important aspect of participation in public life. Free and fair elections form the very foundations of democracy and their underlying processes are increasingly digitalised. These encompass both the electoral administration and the electoral process itself - from voter registration, vote casting, and vote counting, through to civic education and engagement, political advertising and campaign financing during electoral campaigns. Provided the right safeguards are in place, the use of digital technologies and data in the electoral process can bring important benefits to enlarge participation, including higher voter turnout, greater inclusion of disadvantaged groups, as well as greater efficiency and reliability of the electoral process. Electoral Management Bodies (EMBs) thus need to develop an adequate regulatory framework for digital technologies used throughout the electoral cycle and upgrade their own digital capabilities to manage electoral administration and oversee the digitalisation of the electoral process

to ensure that the right safeguards are in place, in terms of cybersecurity, identify theft, and voter manipulation (Driza Maurer, 2020[10]).

More broadly, the democratic political debate, that is the way in which people form and express their political opinion, is also undergoing a major transformation in the digital era. Information intermediation and media ecosystems that enable fact-based engagement are necessary for democracies to thrive, contributing to healthy democratic debate and allowing for political compromises and consensus building. Freedom of expression online and the increased availability of digital platforms to connect, share views and consume information has been a game changer for people's ability to engage in public debates and decision making, but bringing unforeseen new risks to democracy in terms of dis-information and polarisation, as well as undue influence and skewed participation. Chapter 1 delves further into the risks of mis- and dis-information for democratic elections, political campaigns, and democratic debate.

With a view that Parliaments are a core institution where the democratic debate is taking place, the use of online tools by parliaments to get closer to their constituencies, promote openness and citizens' participation or continue operating in times of crisis (Forteza, 2020[11]; Piccinin, 2021[12]) represent an opportunity for progress. Parliaments that harness the power of digital tools can now connect better with those they represent. Social networks and open data are important tools, allowing citizens to engage more effectively with their elected representatives (IPU, 2022[13]). Digital technologies, in particular teleworking technologies, have allowed parliaments to continue operating during the pandemic (IPU, 2021[14]).

5.2.1. Enlarging electoral participation

Voting is a *sine qua non* condition of democracy that digital technologies can help facilitate through the digitalisation of the administration of elections and the conduct of the vote, provided the right safeguards are in place. Digitalisation has permeated the various stages of the electoral cycle, from voter registration, to vote casting, to vote counting. For instance, worldwide various countries are making use of electronic means to cast or count votes in national or local elections (Table 5.1). Nevertheless, it is important to note that internet voting systems and technologies — including email and mobile voting apps — remain to be fully secured in terms of cybersecurity and identity theft, so that the integrity of the process is guaranteed.

The digitalisation of electoral processes includes both the automation of the voting process and the digitisation of electoral data. Digitalisation has become central to election information and management systems. Digitised data include voter registers, registers of candidates, results entered in electronic format. Digitised processes include e-registering, e-identification of voters, e-voting on voting machines in polling stations or over the internet, e-counting (i.e. software used to register and calculate results and allocate seats). They also include software used for statistical purposes, and e-transmission of preliminary and/or final results, for example, from polling stations to a central unit managed by the EMB. Digitisation of processes is more challenging when they transit over the internet, due to cybersecurity risks.

Table 5.1. E-voting use in OECD member countries and key partners

ICTs in Elections Database by the International Institute for Democracy and Electoral Assistance (IDEA)

Scope of E-Voting	Countries
Politically-binding national elections (elections for public office or direct democracy initiatives)	Belgium, Brazil, Estonia, France, India, New Zealand, Peru, United States
Politically-binding sub-national elections (e.g. elections for regional legislature or executive office)	Belgium, Bulgaria, Canada, Estonia, India, Mexico, Peru, United States
Other elections with electoral management bodies participation (e.g. election of trade union leaders, non-binding referendums)	France, South Korea
No e-voting currently used in any elections with electoral management bodies participation	Australia, Austria, Chile, Colombia, Costa Rica, Czech Republic, Denmark, Finland, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Slovak Republic, Slovenia, South Africa, Spain, Sweden, Switzerland, Türkiye, United Kingdom

Note: Data collection for the ICTs in Elections Database was initially done between 2014 and 2016. Since then, the data is continuously updated as much as possible by IDEA following the changes in regulations of countries related to the use of ICTs in elections.
Source: Adapted from (International IDEA, 2022[15]) and country comments on draft report.

The process for **voter registration** depends heavily on the country's identity infrastructure. The voter register in many countries is connected to or compiled from the population register or other trusted government data sources, with automated sharing of necessary identity attributes such as citizenship, age, and address. For example, in Sweden, data about eligible voters is transferred from the digitalised population register to the electoral roll 30 days before election day, with voter cards sent out automatically to the registered voters' addresses to facilitate their participation. Anyone who is, or has been, registered in the population register, and is a Swedish citizen above age 18, is therefore automatically registered to vote and receives her or his voter card automatically (Valmyndigheten, 2021[16]). Countries without connected central registers are instead relying more on citizens themselves to register to vote and to update their information as needed, including when they move to another electoral district. While this approach may cause more barriers to voter registration, these countries might still be working with digital means, including digital identity, to make that process easier and more convenient for citizens.

Once citizens are registered, the next step is **vote casting.** E-voting comprises the e-casting of the vote and the e-counting of paper ballots. Voting is the most supervised use of new technologies in the electoral cycle as it covers the most sensitive process of an electoral cycle, in particular the actual vote and the counting of electoral results (Council of Europe, 2020). It is also the most advanced example of the use of new technologies to facilitate democratic elections because usually it is not just the digitisation of the voting and counting processes, but it ideally implies that all involved documents and processes are digitised so that transactions can take place seamlessly without media discontinuity. E-casting of the vote includes both voting on electronic voting machines in polling stations and voting via the Internet from an uncontrolled environment. E-casting implies e-counting, while e-counting can be undertaken without e-voting using optical scanners which digitise the paper ballot and then proceed to the counting. E-voting is practiced in a few countries, yet not for all elections, as shown in Table 5.1. However, the digitisation of data, documents and processes of the electoral cycle is widespread.

To cast their ballot, eligible voters need to prove their identity, or the identity of others in cases where they are representing someone who is unable to cast their vote for particular reasons. Physical voting and the use of physical identity credentials (as opposed to e-voting using digital authentication) remains a standard practice in most countries. The reasons include political consideration, identity infrastructure, digital maturity, cybersecurity risks, and new risks of fraud, tampering, or coercion which could undermine electoral integrity. For example, as e-voting can take place outside the polling station, there are challenges related to maintaining the principle of one-person-one-vote, and ensuring that citizens can cast their vote

free from duress (ACE project/International IDEA, 2014[17]). Moreover, major challenges exist related to the verification and *ex post* auditing of election results: reviews of e-voting infrastructure used in some OECD countries revealed weaknesses arising from insufficient transparency measures such as end-to-end verifiability, gaps in the system that left it exposed to interference or tampering, as well as subversion of the verification mechanism (Springall et al., 2014[18]; Feldman, Halderman and Felten, 2007[19]; Specter, Koppel and Weitzner, 2020[20]; Halderman and Teague, 2015[21]).

Measures to mitigate these risks include secure digital identification and authentication, and the integration of election audits into the electoral system. Any efforts to increase uptake of e-voting will be reliant on solutions for digital identity that are inclusive, robust, reliable, and secure, as well as preserve the anonymity that is at the core of vote casting. Election audits can take the form of receipts generated by end-to-end auditable voting systems that enables citizens to verify whether the system detected their vote correctly. Post-election audits are also able to act as a fraud and corruption deterrent (Mulroy, 2019[22]). Moreover, new technologies represent further challenges that need to be carefully considered when applied to the electoral process. For example, biometric identification of voters could potentially augment electoral rolls, ensure the unique identification of voters, and prevent multiple voting. Nevertheless, EMBs have refrained from using it due concerns over data protection, vote secrecy, as well as voter disenfranchisement due to errors in biometrical identification. The use of biometry in elections also raises questions in terms of compliance with the right to free expression.

E-voting has potentially many advantages, including lower costs and greater convenience, flexibility, and accessibility for citizens, including those living remotely or with certain disabilities (The Electoral Knowledge Network, n.d.[23]; OSCE/ODIHR, 2013[24]; Council of Europe, 2017[25]; Petitpas, Jaquet and Sciarini, 2021[26]; Anett Numa, 2021[27]). Several governments have held e-voting trials (Switzerland, the United Kingdom, and the United States). In 2005 Estonia became the first country to hold legally-binding general elections over the internet for municipal elections and for parliamentary elections in 2007. This system allows voters to cast their ballots from any internet-connected computer, it ensures anonymity and allows voters to change their vote until the end of the voting period to prevent fraud.[2] In some cases, e-voting has also been found to have a positive impact on voter turnout (Petitpas, Jaquet and Sciarini, 2021[26]). In the 2021 local elections, as many as 55% of voters in Estonia's biggest county voted online (Anett Numa, 2021[27]). It is important to underscore that e-voting is not replacing traditional physical voting but complementing it providing alternative ways to cast one's ballot. Additionally, governments need to address security and system accountability challenges when deploying e-voting systems to ensure the legitimacy of the democratic process.

E-voting can be particularly appealing for younger voters and digital natives. As younger people tend to participate less in elections, yet are more often digitally literate, e-voting may be a means to increase youth voter turnout. Evidence is mixed, however. Currently across OECD countries, only 68% of young people go to the polls, compared to 85% of people aged 54 and above (OECD, 2020[28]). E-voting can facilitate the electoral participation of the youth but is not the only factor. In Estonia, a high-trust society, 43.8% of all votes were casted online in the 2019 parliamentary elections, of which 29.2% of e-voters were aged 18-34.[3] Only a small percentage of young Europeans use digital technologies to engage in civic and political life (OECD, 2018[29]; Mickoleit, 2014[30]).

Finally, digitalisation can improve the scrutiny of electoral processes, the counting of ballots and the dissemination of election results. In particular, open data can facilitate electoral integrity and accountability by enabling voters and civil society to access and analyse data on elections-related matters such as electoral boundaries, political party platforms, party affiliations of candidates, political party positions, and campaign finance contributions (International IDEA, 2017[31]) . Moreover, open data on election results (provisional and final), by constituency or district for national, regional and local elections, including registered and invalid votes, can help stakeholders validate the legitimacy of the election, can as well help identify necessary reforms for improving future electoral processes. Concerns about foreign interference in elections have nevertheless led to closer scrutiny of the security of digital solutions used in electoral

processes, in particular voter registration and results transmission, as was the case in Germany and the Netherlands in 2017.

5.2.2. Protecting electoral campaigns

Digitalisation presents new opportunities for engaging citizens during election campaigns, in particular through online campaigns and political advertisements. Political representation institutions face the lowest levels of trust among OECD countries, according to the OECD Survey on the Drivers of Trust in Public Institutions (OECD Trust Survey) (OECD, 2022[32]). On average, only 24.6% of respondents trust political parties and 55.5% say they do not trust them. Additionally, only 38.9% of respondents report trusting their country's representative legislative institution – parliaments and congresses. Through online campaigning, political parties, candidates or third-party campaigners can reach a broader audience of both supporters and voters with political messages (International IDEA, 2021[33]). This form of campaigning can be conducted at a lower cost than traditional campaigns, which can facilitate access by smaller parties with fewer resources to potential voters. Moreover, political parties can use online platforms to reach out to more voters with more targeted messages (International IDEA, 2021[33]).

However, digitalisation also presents a number of risks to the integrity of election campaigns, and thereby elections as a whole. Democratic institutions can be targeted by cyber threats[4] especially during an election. Threat actors may take advantage of the state of affairs during the campaign process to launch cyberattacks to exfiltrate data, obtain administrative access to systems and potentially infect democratic institutions with malware. Cyberattacks on electoral campaigns and their media coverage in the digital space are of increasing concern through, for example, through information manipulation and selective attacks on political campaign media through malware.[5] Electoral cyber-risks include both cyberattacks on elections in established democracies by foreign state-sponsored actors often linked to authoritarian governments abroad, as well as the use of cyber threats by political parties during the electoral process within democracies, in particular fragile democracies. Any of these actions could undermine the public confidence in the election results.

According to the Canadian Centre for Cyber Security,[6] cyber risks and threat actors in the electoral process and campaigns include: (i) disrupt election infrastructure using distributed denial of service (DDoS) attacks; (ii) compromise or mimic user identities to spread false information on social media or perpetuate voter fraud; (iii) exploit the current work-from-home environment to compromise systems and gain unauthorised access to election management and/or political party systems; (iv) launch online foreign influence campaigns to discredit the democratic process; and (v) use ransomware-based attacks to disrupt access to election data and systems leading to interruption of election services.

Misinformation and disinformation attacks may also be used to target voters and discredit the outcome of the electoral process. Public debate can be threatened when bots, troll armies or other forms of inauthentic online behaviour are used to manipulate public opinion, for example by spreading mis- and dis-information, targeting support for opposition parties, or artificially inflating the popularity of a candidate or salience of a policy issue (Bradshaw and Howard, 2017[34]). This requires a whole of society approach and various policy measures identified in Chapter 1.

Political parties can gain voter insights through campaign analytics to better target political advertising. Recent elections in OECD democracies have raised concerns on data-driven political campaigns, political micro-targeting, and voter manipulation in the era of big data analytics, as reflected in the scandal surrounding *Cambridge Analytica* misuse of Facebook personal data to devise a profiling system for a deeper knowledge of the target audience. Political micro-targeting which consists of targeting an individual or a small group of individuals with political messages according to some of their perceived preferences or interests that their online behaviour may reveal, poses particular challenges to data protection, personal privacy and individual free will.

As a result, governments are introducing stricter rules on political advertising and electoral micro-targeting in the digital sphere. In Europe, the European Commission is seeking clear rules for, and greater transparency of, targeting of online political advertising. In November 2021, it put forward a proposal for a regulation on various political advertising techniques including targeting, as part of measures aimed at protecting election integrity and open democratic debate. In its opinion of January 2022, the European Data Protection Supervisor concurred with the need for stricter rules concerning online targeted political advertising to ensure free and fair elections and recommends a full ban on micro-targeting for political purposes.

Digitalisation has also opened new avenues for the financing of political parties and elections campaigns that need to be better regulated. Through online platforms and crowdfunding mechanisms, small donors can contribute more easily to electoral platforms and campaigns. Yet digital technologies also present a number of risks, in part because the regulation of online political funding is almost non-existent. While most OECD countries have a mature regulatory framework in place to regulate campaign financing, including spending limits, bans on funding from certain private contributors, access to public funding, as well as others, the regulatory framework has not adapted to the challenges posed by online campaigning (OECD, 2021[35]). For example, while a third of OECD countries place limits on traditional advertising spending in relation to election campaigns (for both political parties and candidates), only two countries place limits on online media advertising spending in relation to election campaigns for political parties, and four place limits for candidates (International IDEA, n.d.[36]). Moreover, digital campaigns can be used to circumvent rules related to campaign financing in a number of different ways. For example, foreign state or non-state actors, including foreign civil society organisations, can avoid bans by organising the campaign outside the respective country, and targeting voters within. As the funds were not spent within country, it can be very difficult for law enforcement and electoral oversight bodies to detect and sanction non-compliance (Council of Europe, 2018[37]).

Addressing the risks posed by digital technologies to online campaigning and campaign finance requires closing regulatory gaps, and leveraging existing tools to identify potential breaches. Priority areas would include (i) defining what constitutes online campaigning to improve clarity amongst political parties, candidates and platforms; (ii) making use of various control measures, including data analytics and audits, to improve oversight; (iii) enabling open access to data on payments made to political parties or candidates via online platforms to oversight bodies and the public; and (iv) addressing gaps in existing regulation for online campaigning, as well as third-party funding.

5.2.3. Nurturing democratic deliberation

Information plays a central role in building a healthy and trustworthy democratic public debate. A vibrant democracy is based on the constructive deliberation between contrasting views on key political vision and policy issues. It is also based on capacity to generate compromises and forge consensus based on fact-based, in good faith contestation and negotiation.[7]

The increasing mediation of public debate by digital platforms is also bringing additional challenges to democracy. After television and newspaper, the third most common news source, on average, is social media, according to the OECD Trust Survey (OECD, 2022[32]). 44% of respondents reported that they get news from social media at least once a week, and in some countries this number goes up to 60%. This additional source of information, with content shared and re-shared by citizens and all types of organisations, has in principle allowed more scrutiny of governments, access to a variety of information as well as increased participation, but with unforeseen consequences on the spread of mis- and dis information, polarisation and trust (Table 5.2).

Table 5.2. Potential indirect effects of digital platforms on public opinion and political institutions

No Responsibility	Partial Responsibility
Increase in "constitutional hardball"	Decline in mutual tolerance
Erosion of administrative state	Increase in views of the opposition as illegitimate
Erosion of the rule of law	Erosion of public faith in democratic rule
Increase in state control of the media	Loss of gatekeeping in party nominating process
Decline in institutional forbearance	Furthering state and ruling party media co-ordination
	Decrease in public faith in institutions
	Decreased accountability of political elites in institutions

Source: (Barrett, Dommett and Kreiss, 2021[38]).

The spread of mis- and dis-information threatens democracy by undermining free and fact-based exchange of information and reinforcing polarisation; it also affects genuinely free expression and free will. Nevertheless, governments are starting to build the tools to prevent and combat mis-and dis-information and favour a governance of information ecosystems that strengthens democracies. Chapter 1 offers an extensive discussion on the matter.

Of particular concerns are special interest groups, as well as state and non-state domestic or foreign actors, who can abuse social media to manipulate information, misinform the public and communicate biased opinions. Some companies are using social media advertisements to influence the political narrative, with positive messaging through targeted Facebook and Instagram ads promoting the benefits of increased fossil fuel production (InfluenceMap, 2019[39]). Currently, only Canada and the EU require lobbyists to disclose information on the use of social media as a lobbying tool: in Canada, lobbyists must disclose any communication techniques used, which include social media, whereas in the EU, activities aimed at indirectly influencing EU institutions, such as social media, must be reported in the EU Transparency Register (OECD, 2021[35]).

The war in Ukraine, has also revealed the extent of the use by some foreign actors of social media (mainly) for disinformation and propaganda to act on information outcomes in democracies. While trust in information about the war by EU governments, the EU or NATO seems to be quite high according to the Flash Euro Barometer (74% of EU citizens either fully trusted or tended to trust these sources of information in April 22) as well as trust in journalists (56%), early research is also showing that Russian propaganda is potentially exacerbating polarisation, even in the most mature democracies (European Commission, 2022[40]). Research conducted by IFOP (*Institut d'Études Opinion et Marketing en France et à L'international*) published in March 22 shows that about half of French people believe that at least one Russian theory about the war is true, with those voting on the extreme right and extreme left being significantly more likely to adhere to Russian Propaganda on the origins of the Ukraine crisis (IFOP, 2022[41]). This is despite the strong measures taken by many OECD democracies limiting access to disinformation spread by Russian sources, collaborating with social media platforms, and tracking and responding through NATO and the EU's Recovery and Resilience Facility (RFF) mechanisms. The penetration of Russian propaganda about the war and its global consequences is likely to be higher in developing economies.

The growing polarisation of the political debate in many democracies is of particular concern to OECD governments. Many of the tensions and challenges found throughout society are aggravated on social media platforms, which channel user content via algorithms designed to promote engagement and share similar content, which can reinforce users' existing perceptions rather than challenge them (Smith, 2019[42]). Algorithmic determinism segregating the news and information people see and interact with online might exacerbate the effects of "echo chambers" and confirmation bias, limiting exposure to diverse perspectives and reinforce presupposed narratives. Confirmation bias is the tendency of people to favour information that confirms or strengthens pre-existing beliefs and values, and is difficult to dislodge once

affirmed (Wason and Johnson-Laird, 1972[43]). Evidence from behavioural science shows that information overload and confirmation bias can, in part, explain behaviours relating to group-thinking and polarisation, and even undermine the most compelling, fact-based messages (Sunstein, 1999[44]; Currin, Vera and Khaledi-Nasab, 2022[45]).

There is growing, although inconclusive, evidence that such mechanisms might be taking a toll on the polarisation of public debate in democratic countries. Based on V-Dem's polarisation of society indicator,[8] 11 OECD countries experienced an increase in polarisation between 2011 and 2021, and 7 OECD countries are currently categorised as experiencing "serious polarisation", the worst category (OECD, 2022[46]). A review of causal evidence about the effects of digital media on democracy found that, in more established democracies, there were more pronounced trends likely to be detrimental to democracy (i.e. growing polarisation, but also declining political trust and advantages for populists) (Lorenz-Spreen et al., 2021[47]). On the contrary, some trends more likely to be beneficial for democracy (i.e. increases in political participation and information consumption) were often observed in emerging democracies. Social media's effects on polarisation are likely to be reinforcing increased polarisation caused by a multiplicity of other factors, including political disaffection and the impact of media fragmentation (DellaVigna and Kaplan, 2007[48]; Van Aelst et al., 2017[49]), although it is difficult to measure which factor is the most important and what would constitute a tipping point of polarisation for democracy.

These complex findings suggest that there should be a wide range of efforts to reduce polarisation, focused on all relevant actors in the media, platforms, and information ecosystems (see Chapter 1). There is some evidence of the potential for depolarising effects of social media, due to potential exposure to diverse information (Beam, Hutchens and Hmielowski, 2018[50]; Yarchi, Baden and Kligler-Vilenchik, 2020[51]). Furthermore, there is evidence that social media platforms themselves may be used as tools to effectively share a wide range of information and potentially build resilience of online civic space (Kubin and von Sikorski, 2021[52]).

5.2.4. Fostering political inclusion

Digital technologies hold great potential for political empowerment, contributing to closing gaps in political participation and engagement of under-represented groups (see Chapter 2). The OECD Trust Survey indicates that only 29.8% of respondents on average say that their political system lets them have a say in what the government does, while a majority in eight surveyed countries are not confident (OECD, 2022[32]). Over the last years, digital media have revolutionised the way policymakers interact with citizens, offering political parties and elected politicians greater tools and opportunities to connect with their constituencies, engage in dialogue, and increase their impact. Thanks to very low entry costs, social media has particularly benefited traditionally marginalised groups such as women and minorities, who often have to face barriers of entry when competing for resources in the political sphere (Women in Parliaments Global Forum, 2016[53]).

However, the growing use of digital fora also presents threats for women and other under-represented groups in politics, reducing further their incentives to participate in politics. Women and under-represented can be significantly more likely to experience online abuse, harassment, hate speech and gender-based dis-information (Institute for Strategic Dialogue, 2020[54]). They can be victims of cyber violence, that is defined as "the use of computer systems to cause, facilitate, or threaten violence against individuals that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities" (Council of Europe, 2018[55]). As such, social media platforms have become, according to the Inter-Parliamentary Union (IPU), "the number one place in which psychological violence is perpetrated against women parliamentarians (IPU, 2016[56]),[9] with substantial consequences for women's participation in public life as they may be discouraged from running from office, be pushed out of politics, and be prevented from achieving leadership positions.

5.2.5. Way forward

Looking ahead, a number of priorities stand out for governments to protect and promote democratic institutions in the digital age, while acknowledging the need to ensure public transparency and preserve the foundations of healthy elections and democracy:

- Ensure the integrity elections throughout the electoral process that is increasingly relying on digital tools (from voter registration to vote counting), leveraging open data to increase its credibility and strengthening the oversight capabilities of electoral management bodies.
- Strengthen the digital capabilities of electoral management bodies in the conduct and oversight of elections, in particular their cybersecurity capacities to administer electoral processes, manage electoral processes and protect electoral data and campaigns from cyber threats.
- Close regulatory gaps in election-related processes, such as online campaign finance, online political advertising and data-driven political micro-targeting, and enable appropriate enforcement and redress mechanisms in case of breaches.
- Build the necessary safeguards so that digital platforms do not enable or allow for disrupting the political playing field and protect the domestic political debate from undue foreign interferences and cyberattacks.
- Protect the democratic debate by reducing political polarisation, before, during and beyond elections, by fighting mis and dis information and adopting specific actions to shield women and under-represented groups from politically motivated abuse and harassment.

5.3. Fostering citizen participation in the digital age

Active citizen participation in democratic processes, beyond the ballot box, is central to the vitality of democracy. Pillar II of the Reinforcing Democracy Initiative looks at the main evolutions in this field in greater detail and depth (see Chapter 2).

Digitalisation opens a range of opportunities to increase citizens' voice in policy making and service delivery. Digital participation, that is the use of digital channels for citizen participation in the political arena, the civic space and public decision-making, has the potential to allow for more innovative and effective levels of participation and engagement of citizens. From the early days of digital government experimentation, "the use of new information and communication technologies (ICT) to increase and enhance citizen's engagement in the democratic process" (Parliamentary Office of Sciences and Technology, 2009[57]) was present in public sector foresight reports. At present, it ranges from the provision of information, to agenda setting mechanisms (such as e-petitions, where citizens can address and solve issues with public services or raise concerns with government directly), to consultation procedures and more intensive forms of engagement (e.g. online deliberative processes or crowdsourcing of citizen challenges). Digital participation allows for more immediate and continuous political debate and the creation of fluid spaces for discussing, deliberating and reaching decisions (OECD, 2017[58]).

The digital age is also expanding the number and types of actors willing to engage with all levels of government to better serve society. The characteristics of digital participation, especially its non-geographical delimitation and a-synchronicity, can allow for far bigger audience to engage in a single process. It has also created interest from new types of actors. For example, the open data movement has allowed for a growing number of engaged citizens and civic start-ups to work with public authorities directly to co-deliver services of public interest and oversee local authorities, especially at city level. Digital tools for citizen participation can also enhance collective action, societal mobilisations and support virtual communities. However, achieving meaningful participation that articulates proposals beyond protests, is inclusive and representative, has a tangible impact in the decision-making process, remains a challenge. In this evolving context, digital participation presents a broad range of opportunities to be nurtured and

challenges that need to be addressed to bolster inclusive participation and further engage, or re-engage, disengaged groups and young people. These range from data protection to building citizens' capacity to use digital tools and data.

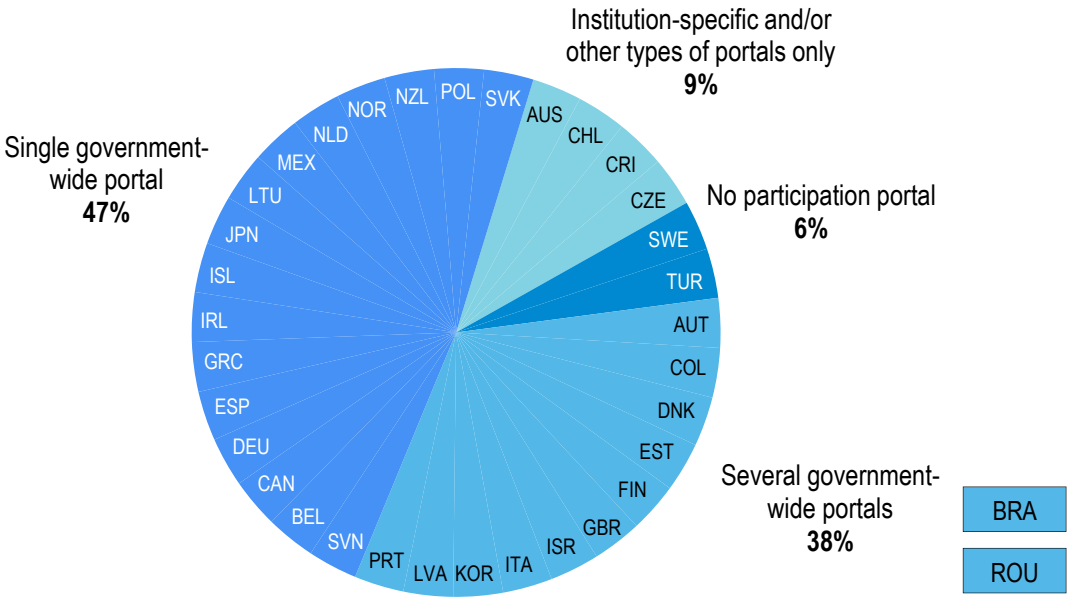
5.3.1. Empowering citizens beyond elections

Digital platforms, channels and tools are enabling alternative spaces for consultation, discussion and deliberation on public policies, also promoting citizens' policy initiative. They increasingly complement the action of traditional forms of citizen participation, both at the individual and collective levels. For instance, in Estonia, the Citizen Initiative Portal *rahvaalgatus.ee* enables citizens to develop, send, and track legislative proposals and regulatory improvements to parliament or local authorities. Collective petitioning right emerged in Estonia in 2014. Similarly, *Kansalaisaloite*, Finland's platform for citizen initiatives created in 2012 and managed by the Ministry of Justice, enables citizens to present legislative proposals that, if they garner sufficient support, can be tabled in parliament for debate. A similar e-petition system exists in the United Kingdom,[10] where citizens have submitted over 28 000 e-petitions to call for action on specific issues which the government or parliament are responsible for, either seeking a response or suggesting consideration for debate. Such digital solutions can circumvent restrictions and help overcome obstacles to the direct participation of specific groups of citizens. For example, two different initiatives in Mexico can be cited as successfully engaging "hard to reach groups" such as women, youth and marginalised city dwellers. "*Block by Block*" is an UN-Habitat initiative that uses Minecraft – a computer game – as a tool to promote participation for urban planning and the *Mexico City Mapathon* was a gamified crowdsourcing experiment to involve public transport users in mapping the city bus routes.

The use of digital platforms to encourage and facilitate citizen participation has become a widespread practice at all levels of government (NESTA, 2017[59]). The United Nations E-Government Survey found that recent years have witnessed the proliferation of e-consultation mechanisms, national e-petition platforms, citizens' initiatives and crowdsourcing initiatives (UNDESA, 2020[60]). For example, Portugal has developed *Participa Portugal* to promote public consultations. Digital platforms were also deployed by government to continue engaging with citizens during the COVID-19 lockdowns, as done in Scotland local governments.

An increasing number of governments at national and local levels are moving from ad-hoc platforms developed for one particular participatory process, to more comprehensive and integrated digital ecosystems for citizen participation. In 2020, 27 out of 32 OECD countries (85%) had government-wide participation portals used by all ministries at the central and federal levels of government as a "one-stop shop" for citizens to participate (Figure 5.1), according to the OECD 2021 *Government at a Glance* report (OECD, 2021[61]). This centralisation supports uptake from citizens, facilitates communication, enhances co-ordination, and reduces overlaps between public institutions.

Figure 5.1. Availability of government-wide portals to facilitate citizen and stakeholder participation, 2020



Note: Data for France, Hungary, Luxembourg, Switzerland, and the United States are not available.
Source: OECD (2021[61]), *Government at a Glance 2021*, OECD Publishing, Paris, https://doi.org/10.1787/1c258f55-en

Digital tools are being used to increase the impact of established participatory practices such as participatory budgeting or social accountability. In this case, open digital platforms can be used both to inform citizens and allow them to submit or vote on proposals online. Government-led initiatives, such as Portugal's Participatory Budget, have adopted technology as a way to bring citizens closer to decision-making and to ensure a deeper nation-wide cohesion between regions, rural and urban areas.[11] Many public institutions have set up digital channels, to increase the uptake of social accountability mechanisms and create more continuous feedback loops. For example, Brazil deployed the *fala.br* platform as a central point for citizens to provide feedback or complaint about a public service (OECD, 2022[62]).

Digital technologies can also promote more innovative approaches to citizen participation. During the COVID-19 pandemic in 2020 and 2021, online deliberation became the most used medium for conducting deliberative processes (OECD, 2021[63]). For example, Finland has organised several online deliberative processes to gather recommendations from a representative group of Finnish citizens on issues such as tackling online hate speech or infrastructure (Grönlund et al., 2020[64]). This trend is likely to continue, whether in a full online or in hybrid settings. Other innovative features that digital can introduce include the use of artificial intelligence to map citizens' contributions as done in Taiwan (GovLab, 2019[65]), the use of virtual reality or the gamification of participatory processes to fight low motivation and disengagement (Tseng, 2022[66]), and active social listening platforms such as in Spain through the civic-tech solution Citibeats. Digital participation tools and crowdsourcing platforms are also increasingly adopted at supranational level, as shown among others by the Conference on the Future of Europe or the Global Citizen Assembly for COP26, as it can be a particularly effective tool to facilitate citizen engagement on regional and global issues, increasing the reach despite physical distance and language barriers.

Technology is also enabling increasingly direct and interactive relationships between citizens and institutions in the co-design and co-delivery of solutions to public problems, in particular at the city level. For instance, there are solutions spreading across the world that replicate and adapt the *FixMyStreet* app

developed in the United Kingdom, which enables citizens to report infrastructure or service delivery problems to the corresponding local public authority. *FixMyStreet* is a map-based platform developed by mySociety that allows people to inform their local authority of problems needing their attention, such as potholes and broken streetlamps. At a national level, the National Association of State Procurement Officials (NASPO) in the United States issued in 2021 a call for tenders to source suppliers able to provide versatile citizen engagement platforms for the benefits of seven States (NASPO, 2021[67]).

Social impact investors, too, are increasingly supporting these tech4good initiatives developed by civic-techs. In May 2022, Globant, a global venture fund, launched the Be Kind Tech Fund, a USD 10 million fund to invest in start-ups that tackle the negative collateral impacts and the misuse of technology in society. Venture philanthropies are also stepping in, creating dedicated funds to invest in public interest technology deployed by civic organisations to solve societal problems and improve government.[12] For example, in 2019 the Ford Foundation established a USD 50 million Public Interest Technology Catalyst Fund that has leveraged a further USD 150 million in complementary grant-making by partnering foundations since 2020.

Digital solutions are also used to enhance the traditional democratic representative institutions. Legislative institutions are increasingly championing digital democracy initiatives, moving from *ad hoc* platforms to integrated digital ecosystems. Digital technologies are contributing to modernise legislative processes, facilitate committees' work, enable remote deliberations, increase transparency of parliamentary practices, enhance constituency relations, and changing the ways laws are drafted (Mohun and Roberts, 2020[68]). For example, in 2020, the UK Parliament adopted a 5-year Digital Strategy to modernise its international functioning and enhance its external constituency relations. Similarly, Australia's Parliament Digital Strategy for 2019-2022 provides a roadmap to digitally enhance the work of parliamentarians and their engagement with their constituencies.

Regarding the implementation of technologies, the OECD's 2018 OECD Survey on Parliamentary Budgeting Practices analysed public participation in the budget process. Seven countries parliaments reported using e-petitions (Estonia, Finland, Germany, Korea, Luxembourg, New Zealand, and Portugal); while parliaments in France, Greece and Switzerland reported holding "digital debates on social media platforms" (OECD, 2019[69]). Countries such as France and Argentina have established an institutional digital platform for petitions and consultations, and whilst others, such as Chile and Brazil, have set up a digital infrastructure including streaming applications, collaborative drafting tools and mobile apps to increase citizen participation throughout the legislative cycle.

City governments have been particularly successful in leveraging digital platforms and tools to create a digital ecosystem that enhances citizen participation. The UN 2020 E-Government Survey found that citizen participation through city portals was most commonly done through social network features (79%), submission of feedback or complaints (72%), deliberative and decision-making processes (45%), and information on public meetings of the city or municipal councils (43%). Only a few participate through voting forums (28%) or provide feedback about consultation processes (23%) (UNDESA, 2020[60]). These platforms are typically part of broader open innovations embedded in smart city strategies and open government initiatives. For example, the main pillars of Barcelona's Digital City strategy include digital transformation, digital innovation, and digital empowerment, including the promotion of civic rights in cities. In Colombia, Bogotá's citizen participation platform *Yo Participo*[13] is part of the city's open government strategy.

A myriad of cities around the world have adopted digital citizen participation platforms. These platforms allow citizens to be involved in a diverse set of participatory mechanisms, including local budgets, consultations, citizen assemblies, townhalls or opinion polls. In addition, they centralise and thus facilitate access to information about the right to participate, allow for collective discussions, provide feedback on closed processes, and are progressively being combined with other digital solutions such as digital identity or government chatbots.

- In 2015, the city of Madrid launched its online platform, Decide Madrid, to encourage greater citizen participation in local governance, participatory budgets, and investment projects. It is based on an open-source software developed by the municipality of Madrid Consul and now deployed in 135 cities in 35 countries.
- The city of Barcelona developed its own participatory platform *Decidim Barcelona*, originally focused on participatory budgeting and the monitoring of public works which allows the city government to interact with citizens through diverse mechanisms including information and data, public consultations, town hall meetings and participatory budgets. It is based on an open-source and open-code software (*Decidim*) now used by cities and regions such as Helsinki, Mexico, Milano, and New York.[14] It is a digital space forming part of a participatory process in which to debate, respond and gather proposals.
- "Better Reykjavik" in Iceland is a platform that promotes greater transparency and enlarges the role of citizens in the definition of the city's budget, with local authorities supporting and embedding the solution into their administrative processes and establishing a constant dialogue with citizens regarding their proposals and initiatives.

Last but not least, non-governmental organisations are also leveraging digital tools to increase citizen oversight of public institutions, often partnering with civic-tech start-ups. In the United Kingdom, for instance, to move beyond access to information and enforce social accountability, mySociety has developed open-source digital democracy tools such as TheyWorkForYou releasing voting records to increase parliamentarians' accountability and WriteToThem to allow citizens to engage with their elected representatives, whom they often do not know, using a software that matches postcodes with constituency boundaries. In Brazil, the civic-tech *Serenata de Amor* uses artificial intelligence to audit public accounts and support social control of parliamentarians' emoluments. It created Rosie, an artificial intelligence robot, to analyse parliamentarians' expenses and detect suspicious spending.

Nevertheless, the design of these digital tools and platforms needs to be inclusive, engaging and accessible to all. The design of a digital tool can impact the way citizens interact and how they express their opinions. This includes considerations about the format of discussions (text only, ranking of comments, etc.) or the identification of the participants (Shortall, 2020[70]). For the design of the *Decide Madrid* platform, user-friendliness and usability were key factors. To improve the design of its digital infrastructure, the Brazilian Chamber of Deputies has set up a physical space (Hacker Lab) where different stakeholders including developers, data scientists, designers, social scientists and elected representatives can collaborate, creating an integrated digital ecosystem that allows for a continuous participation in the law-making process.

Digital tools can enhance and improve a participatory process, only if the process itself is well designed and implemented. Governments should be clear about the purpose and the expected outcomes of those initiatives, integrating the digital solutions into government processes and ensuring administrative responsiveness to citizens' inputs. To support public authorities in this matter, building on the 2020 report on *Innovative Citizen Participation and New Democratic Institutions: Catching the Deliberative Wave* (OECD, 2020[71]), the OECD will publish the *OECD Citizen Participation Guidelines*, which offer a ten-step path to properly design, implement and evaluate a participatory process. The Guidelines include one step to help public authorities decide the right approach to using digital tools in their process, as well as guidance on how to implement and which tool to use.

Despite its promises, however, technology is not a panacea that will replace the necessary reshaping of government institutions for improved representation and participation (see Chapter 2), nor will the offer of digital channels compensate for citizens' low interest in engaging in policy-level discussions. Rather, digital tools complement traditional participation mechanisms that are still relevant today, especially for marginalised and vulnerable communities with low digital literacy, as they help diversify the profiles of citizens engaged through digital channels and prevent or minimise additional exclusions brought by any

"digital divides". Digital solutions themselves should be open to democratic rules, principles and scrutiny; be accountable, transparent and responsible in their impacts; engage citizens throughout their development so that they are fit-for-purpose; and provide security and protection for citizens' engagement and participation. In addition, building 'democratic fitness' by bolstering citizens' capacities, trust and engagement remains a key factor in improving participation in the democratic system (see Chapter 2). However, citizen engagement must be carried out within the checks and balances provided by legislatures and systems must be in place to safeguard programmes against capture by organised groups seeking to serve their own interest.

5.3.2. (Re-)engaging the digital natives

Strengthening citizen participation through digitally enabled consultation and participation is particularly relevant for young people. The OECD Trust Survey shows that on average, 37.9% of people aged 18 to 29 tend to trust the government, compared to 41.8% of those aged between 30 and 49, and 45.9% aged 50 and over (OECD, 2022[32]). Whereas a significant share of young people today has grown up as "digital natives", they continue to be significantly underrepresented in public institutions and institutionalised forms of political participation such as electoral platforms or political party membership. In turn, with the proliferation of digital tools, young people have increasingly diverted to non-institutionalised forms of political engagement, including through digital channels such as social media (OECD, 2020[72]; OECD, 2022[73]). The OECD *Communication Guide on Engaging Young People in Open Government,* for instance, was developed to support countries to better communicate with young people to engage them in open government reforms, drawing on research and case studies from across OECD member countries (OECD, 2018[29]).

In response to the COVID-19 crisis, numerous governments launched digital participation opportunities, including online consultations, to involve young people in the design of response and recovery measures. For example, Germany, Estonia, Lithuania, Poland, and Switzerland, among others, have organised or supported virtual hackathons in the early stages of the COVID-19 crisis to generate innovative ideas for mitigating the health, social and economic implications of the crisis (OECD, 2020[74]). Findings show that digital engagement strategies that prioritise two-way interaction, where young people feel a sense of empowerment and agency, and where collaborative approaches are prioritised are more likely to effectively engage young people in public participation processes (OECD, 2018[29]).

Digital participation platforms can get inspiration from digital channels or spaces populated by young people to bring this underrepresented group back into institutionalised participation. Digital natives are present in social media and have integrated online communications and channels in their daily interactions. Digital participation could look closer to the existing digital spaces to make these participatory opportunities more appealing to the younger generations. This can include adopting functionalities such as ranking, multimedia interaction, and gamification. For example, during the French presidential elections in 2022, Ministers and candidates used the videogame streaming platform Twitch to engage with the younger voters, and civic tech communities created "Tinder-like" applications such as *Elyzee* to increase information on electoral campaigns and programmes.

The *OECD Recommendation of the Council on Creating Better Opportunities for Young People* adopted in June 2022 underscores that digital government tools can be used to apply more innovate methods to communicate and engage with organised and non-organised young people. It also acknowledges that digital means are important to engage the youth in all stages of the policymaking cycle and that young people and structures such as youth advisory bodies should be created or strengthened in areas such as digital technology policy and governance. Governments can also take specific actions to develop capacity for young people to participate and enhance democratic dialogue with young people on policies to address climate change, rising inequality, and threats to democratic institutions (OECD, 2022[73]).

Finally, there is growing recognition of the importance to build digital citizenship and strengthen digital citizenship education to promote youngsters' civic engagement in the digital space (OECD, forthcoming[75]; Mossberger, Tolbert and McNeal, 2007[76]). This need stems from the new and multiple ways in which young people are engaging in and communicating about civic issues through the use of social media. According to the Council of Europe (2016), "digital citizenship refers to the ability to engage positively, critically and competently in the digital environment, drawing on the skills of effective communication and creation, to practice forms of social participation that are respectful of human rights and dignity through the responsible use of technology" (Council of Europe, 2016[77]). Initiatives to reinforce responsible digital citizenships include partnering with platforms where the narrative against democratic values is being mainstreamed to target the political education of the young people in the digital age, or collaborating with schools to support students' digital civic engagement. To that end, the Council of Europe is developing a *Reference Framework of Competences for Democratic Culture,* to be adapted for use in primary and secondary schools and higher education and vocational training institutions throughout Europe as well as national curricula and teaching programs.[15]

5.3.3. Ensuring digital inclusion

Digital technologies can also help increase the representation and participation of under-represented groups in democratic processes. They can widen the scope of any participatory process by increasing the reach beyond physical distances, allowing for asynchronous interaction, and enabling new features such as automatic translation. However, they can also create new forms of exclusion, as for example, men, urban residents, and young people are more likely to be participate online than women, rural populations, and older persons (ITU, 2021[78]; OECD, 2021[79]; OECD, 2020[80]).

For digital democracy to flourish, public authorities should thus address the digital inequalities (Schradie, 2018[81]), both in terms of access to and the capability to use digital technologies for civic and political participation by providing analogue alternatives, ensuring access to the internet, and levelling digital literacy among all citizens. As digital tools and technology become central to political activity and the civic space, citizens must have the sufficient digital skills to be comfortable with and effectively leverage digital participation tools and platforms. Mitigating the risks of exclusion from digital participation mechanisms and leaving no one behind the digital transition require enhancing digital literacy. As such, digital participation should not be exclusive and incompatible with, but complementary to more traditional channels to (re-)engage citizens in civic life and political processes.

Countries are taking steps to respond to the digital skills challenge and fight digital exclusion, which is central for inclusive democracies in the digital era. Digital inclusion is essential to ensure that no one is left behind in the digital transition in terms of access, affordability, and ability to use digital tools productively. It requires approaches tailored to the needs of different populations, in particular vulnerable groups, older people and people with disabilities. For example, in 2018, France launched a national plan for digital inclusion (*Plan national pour un numérique inclusif*) aiming to develop a safe and human-centric digital society. By providing digital competences to 4.5 million French citizens, the goal is to achieve digital inclusion of one third of the French population over the next 10 years. These initiatives are particularly important at the local level, both in rural areas and city contexts. The Scottish government set up an inclusion program called *No One Left Behind Digital Scotland*[16] and adopted in 2014 a Digital Participation Charter[17] to promote citizen participation in the digital space.

A more complex issue is that of digital literacy efforts aimed at empowering citizens to use technology or navigate the internet in a responsible and safe fashion. This is essential, as services are increasingly accessed online and the use of digital identity is becoming more and more pervasive in people's lives. Reducing digital inequalities requires multiple efforts including improved existing digital infrastructure, specialised training, and digital security awareness programmes. All these initiatives aim to provide targeted

support for citizens to effectively and safely leverage digital tools to enhance their participation in local politics and civic life (OECD, 2019[82]). For instance, Portugal offers cybersecurity training for citizens.[18]

5.3.4. Way forward

Looking ahead, a number of priorities stand out for governments to consider so as to harness the potential of new technologies to enhance the quality and impact of citizen participation in the digital era:

- Constantly monitor, and upgrade and update digital democracy tools to meaningfully empower citizens, in particular the youth, in decisions affecting their everyday life, partnering with a wide range of stakeholders including innovative civic-techs, users and technical communities.
- Provide the necessary resources (human, financial and technical) to develop, maintain and use digital tools for democratic purposes, including the analysis of citizen inputs received through these tools.
- Support a move towards integrated ecosystems of tools and platforms that enable a coherent space for digital participation, in particular at the city level.
- Ensure the technologies and tools used in participatory processes are fit-for-democracy, meaning they are transparent and accountable, follow ethical standards and apply robust data protection and algorithm transparency.
- Demonstrate and communicate the results of citizen participation in decision-making and the co-design of policy responses s, especially at the local and city levels.
- Ensure solid governance of participatory processes to avoid capture by special interest, warrant representativity, solid linkages with traditional democratic institutions in particular parliament, and make sure expectations are met on the outcomes of the participatory processes including with solid *ex ante* and *ex post* communication.
- Take steps to decrease the digital divides by ensuring equal access to democracy tools emerging in the digital age and foster inclusion of marginalised communities and vulnerable groups so that no one is left behind, using a combination of digital and analogue tools.

5.4. Furthering government transparency and accountability in the digital era

Digitalisation offers a wealth of opportunities for improving transparency, accountability, and integrity in government. Government digitalisation allows for the automation of processes and the digitation of data within public administrations that improve not only the efficiency and reliability of government operations but also their transparency and decreased opportunities for breaches in integrity. It also enables more agile service windows to interact with users that improves responsiveness, transparency, and accountability in the delivery of public services. From the proactive provision of open data, AI-powered auditing, and integrity analytics, through to live streaming of government and parliamentary debate, the opportunities are vast to leverage new technologies to modernise government.

Nonetheless, designing transparency mechanisms that are fit-for-purpose in a digital context is not always straightforward. For example, increased availability of government data and civic technologies may not in itself lead to greater empowerment of citizens in the absence of an adequately responsive institutional context to process demands. Greater government data openness and more effective anticorruption analytics might lead, in the short-term, to increased citizen perceptions of corruption. It might neither lead to more effective external oversight by civic organisations and accountability institutions, which may not have the skills or means to use these digital innovations effectively, nor the political incentives to act on them. Furthermore, the benefits of emerging technologies, especially data analytics and artificial intelligence, for increasing transparency and accountability of government activities need to be coupled with new ways of ensuring trustworthiness of their use by governments.

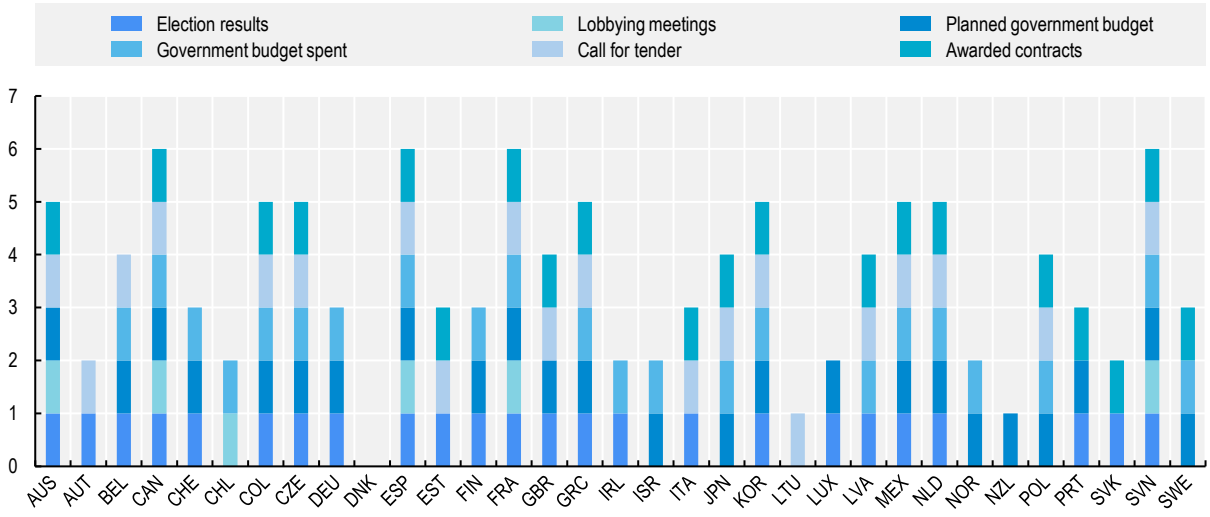
5.4.1. Opening up government data

Many governments have made considerable progress to open government data to support transparency policy making processes (G8, 2013[83]). Good open government data is critical for delivery units within centres of government to better oversee and monitor government's overall performance. Open data arrangements refer to "*non-discriminatory data access and sharing arrangements, where data is machine readable and can be accessed and shared, free of charge, and used by anyone for any purpose subject, at most, to requirements that preserve integrity, provenance, attribution, and openness*" (OECD, 2021[84]). Open government data is helping governments improve the operational efficiency of public administrations, the quality of public spending, and targeting of social programs. It has also been critical in improving the design, delivery, and responsiveness of public services, better tailoring them to users' needs (OECD, 2019[85]). Furthermore, it has proved a critical tool to increase transparency and accountability of government policies and programs, contributing to anchor integrity and mitigate fraud in high-risks policies areas such as taxation, budgeting, and procurement.

Countries are opening election, lobbying, budgeting, and procurement data to increase transparency and accountability in public governance (Figure 5.2). As highlighted in Section 5.2 of this chapter, open electoral data is key to enhance the integrity of elections and hold electoral actors accountable. It can include data about the elections results, as well as data about electoral boundaries, campaign finance, voter registration, and disputes resolution. Besides facilitating participation, opening up data related to political parties can contribute to restoring trust in political parties and improving the accountability of party-based representative democracy (Scarrow, Webb and Poguntke, 2017[86]). Additionally, publishing open lobbying data can help enhance transparency and trust in public decision-making processes by mitigating the risks of undue influence. The European Commission and Parliament have implemented a comprehensive approach to open lobbying data, including a register of lobbyists, meetings, and external activities of public officials with lobbyists. Civil society re-uses this data to develop oversight mechanisms, such as the Integrity Watch EU portal.[19]

Governments are making a range of open budgetary data available, including data on revenue management, public investment, and government procurement. This open budget data contributes both to improve the functioning of government and to enable external oversight. Centres of governments themselves, in particular finance ministries, have a strong incentive in making public finances information more reliable, accessible and re-usable, especially those of local governments and municipalities, as the trend towards greater fiscal decentralisation has significantly increased the share of public resources managed and executed by local authorities and state-owned enterprises. Civil society, professional organisations and software developers are also using the data to develop tools to monitor revenue and spending details, producing freely available apps and visualisations to increase budget transparency. Governments have adopted open government actions plans with specific commitment to increasing fiscal transparency and adhered to voluntary initiatives and standards that have significantly advanced budget transparency.[20] The *OECD Budget Transparency Toolkit* (OECD, 2017[87]) sets out a range of minimum standards for open budget data. Finally, open data containing lobbying information, using standards and identifiers, has great potential to facilitate government transparency and integrity, for instance in supporting the cross-checking of data from different sources, such as political finance contributions (OECD, 2021[35]).

Figure 5.2. Availability of open budget-, procurement-, election- and lobbying data on the central/federal government one-stop-shop portal for open data



Note: Data is not available for Costa Rica, Hungary, Iceland, Türkiye and the United States. The Figure shows countries who responded yes to the question "On the federal/central government one-stop-shop portal are the following data publicly available (either directly or indirectly)?". Countries who responded no might still have had the type of data available as open data, but not on a central one-stop-shop portal for open data.
Source: OECD Survey on Open Government Data 4.0. Final responses were submitted and validated in 2019.

Digital innovations leveraging data are also being deployed by national and city governments, as well as oversight agencies, to track the financial and physical implementation of public works. Geo-referencing platforms, often developed or used by finance ministries and oversight institutions, has been used to track progress with public investment spending. For example, in Latin America several governments, including Argentina, Colombia, Costa Rica, and Peru, have upgraded their public investment management systems to better track public works and make government contracts transparent. Colombia has developed a mobile application called *Elefantes Blancos*, inviting citizens to monitor neglected, abandoned, or overbilled public works projects.

The relevance of open contracting data has become well recognised for anchoring integrity in the public sector. A wide range of OECD countries have made considerable progress in recent years in leveraging digital tools to open government procurement data, including France, Italy, the Netherlands, Mexico and Colombia (Open Contracting Partnership, 2022[88]). With public procurement accounting for approximately 12.6% of GDP in OECD countries in 2019 (OECD, 2021[61]), the publication of such data is an important driver of strengthening transparency but also improving effectiveness of government spending in times of budget constraints and economic slowdown. Even though various OECD countries have made considerable progress in publishing such data, data containing all relevant public procurement information beyond government contracting information are still largely unavailable in many countries worldwide, especially in standardised formats that facilitates its reuse for secondary purposes (Open Contracting Partnership, 2022[88]). Improving the quality of underlying data is critical for its effective re-use by government entities, oversight agencies and civil society.

Central government bodies (ministries of finance and central government procurement agencies, as well as independent oversight institutions) are increasingly developing integrity analytics tools leveraging open procurement data. Finance ministries, tax authorities, and central procurement agencies are developing and deploying data analytics and artificial intelligence platforms to better monitor public spending by line ministries and subnational governments. Independent oversight agencies such as audit offices and anticorruption agencies are resorting to artificial intelligence robots to red-flag irregularities in government

procurement, in particular at the subnational level. These tools have been particularly useful during the pandemic to uncover anomalies in emergency health spending, as well as to facilitate continued and effective oversight in remote working environments (OECD, 2022[89]). In Brazil, ALICE (*Analisador de Licitações, Contratos e Editais,* or Bids, Contracts and Public Notices Analyser), deployed by the Office of the Comptroller General of the Union (CGU) and the Federal Court of Accounts (TCU), has been generating a significant positive impact by identifying integrity risks in Brazil and fighting corruption in public procurement at the federal public administration. More than 100 000 procurement notices have been analysed and, between December 2018 and November 2019, 8 bids had been revoked, totalling approximately BRL 3.2 billion. In addition, 14 bids had been suspended due to signs of corruption uncovered by ALICE, totalling BRL 470 million. In 2021, 139 566 bids were assessed, 35 461 notices (OECD, 2022[90]).

Oversight agencies are teaming-up with govtech start-ups to mine a wealth and diversity of data to uncover suspicious trends and raise red flags. Increasingly, tech-based, data-powered start-ups are seeking social impact partnering with civil society to leverage data against corruption. For example, the French startup Linkurious and the Swedish Neo Technology helped the International Consortium of Investigative Journalists make sense of the trove of data leaked from Panamanian law firm Mossack Fonseca that led to the so-called Panama Papers global scandal. The availability of civic technologies re-using open data has reduced information asymmetries between citizens and governments, and enhanced citizen engagement in public integrity and anti-corruption. Citizens can leverage digital innovations to spot potential irregularities in public services and government contracting, ask questions about complicated bureaucratic processes, and generate and disseminate information on irregularities in the public sector (OECD, 2017[91]; Bauhr and Grimes, 2013[92]; GIZ, 2018[93]).

For example, online reporting and disclosure systems on political financing allow citizens to see donations to political parties and their annual financial reports, and to campaign for finance reporting for both parties and candidates (International IDEA, 2017[94]). Likewise, mobile applications provide whistle-blowers a safe and anonymous channel to communicate unlawful and unethical activity they encounter at their workplace. Other examples of civic-tech platforms that help monitor and promote transparency and integrity in democratic institutions and representatives include the *Vouli Watch* in Greece or *Parlameter* in Slovenia, the accountability and positioning of elected officials such as the United Kingdom's *Who can I vote for*, or public procurement procedures such as Romania's *Harta Banilor PubliciM*.

Finally, open justice reforms can foster trust in the administration of justice and the justice system itself (Lelièvre, 2017[95]; OECD, 2022[96]). The rule of law is central to democracy and trust in institutions. Yet, the OECD Trust Survey indicates that, while citizens' overall trust in the judiciary is relatively high, only about 4 in 10 respondents, on average, believe that a court in their country would make a decision free from political interference or influence (OECD, 2022[32]). Pro-activeness in publishing relevant open data, while protecting privacy of the affected parties and easy to use self-help tools to triage legal issues, can help reinforce transparency in the administration of justice and inclusive access to justice, as it can support comprehensibility and traceability of judicial decisions and applicable norms (e.g. through using plain language in legal information available online). These strategies empower people and businesses to understand, access and enforce their rights and track the resolution of legal issues. In addition, countries are increasingly developing plain language legal guidance for citizens, such as the United Kingdom's judiciary website "You and the judiciary", which provides clear information and advice in relation to going to court, sentencing, appealing decisions, addressing members of the judiciary and how to make a complaint, including helpful links to needed forms and organisations to turn to for free legal assistance (UK Courts and Tribunals Judiciary, n.d.[97]).

Digital innovation is central to achieve smarter judicial systems and the digital transformation of judicial systems has quickened its pace in recent years. Many OECD countries, such as Colombia, Latvia, Portugal New Zealand, Spain, and the United Kingdom have embarked on people-centred reforms of the administration of justice, leveraging digital and data solutions to improve transparency, efficiency, and delivery. For example, Portugal has developed a comprehensive digitally-driven program to modernise

its justice sector to make it more transparent, accessible and effective. Recent initiatives include the *Justiça + Próxima* program, the Tribunal+ project and the horizontal project, Simplex+ that are aimed at promoting innovation and user-centred services through the use of digital technologies and data interoperability, complemented by administrative simplification and digitisation (OECD, 2020[98]). These reforms are aimed at improving the experience of court users through for instance the traceability of cases, reducing the time it takes to hear and resolve matters in a tribunal, and simplifying and standardising processes to improve efficiency.

5.4.2. Leveraging emerging technologies

Emerging technologies can, if tested appropriately and used responsibly, help increase transparency and accountability of government activities. For example, the immutability aspect of Blockchain technology has made it a useful tool for increasing transparency in high-risk transactions, such as property registration and land titling, public contracting, cash transfers, and distribution of aid funds (Berryhill, Bourgery and Hanson, 2018[99]). It has also been deployed to counter fraud and prevent corruption in commodity trading, for example in illegal logging that damages the environment or the trading of "blood diamonds" from conflict zones. However, the use of Blockchain technology in the public sector remains limited, and recent research has evidenced that, despite strong interest and greater awareness, blockchain has had minimal impact on the public sector, where few projects have moved beyond small pilots (Lindman et al., 2020[100]).

When based on good quality data, artificial intelligence technology offers immense opportunities to enhance and automate efforts to identify and predict potential fraud and corruption in a wide range of sectors, such as mapping networks of relations, use of shell companies, off-shore jurisdictions, and banking information of bidders to address potential risks before a contract is issued (OECD/CAF, 2022[101]). Data analytics for both structured and unstructured data can help experts across a range of disciplines to identify, analyse, and prevent strategic, operational, and reputational risks, including the risk of corruption, fraud, waste and abuse. As mentioned previously, central oversight agencies and independent watchdogs are developing and deploying artificial intelligence tool to better identify suspicious patterns and raise red-flags, in particular in government procurement. For example, government entities responsible for health and unemployment benefits make use of analytics to assess risks and ensure public funds go to their intended beneficiaries, whilst ensuring efficient service delivery. In Spain, the Comptroller General is also using AI and ML models to identify high-risk instances of potential fraud in grant and subsidies programmes (OECD, 2021[102]).

While there are many benefits of using data and artificial intelligence to improve public services, their use also needs to be transparent, trusted, and proactively mitigating risks. Predictions and performance of algorithms can be constrained and biased by the decisions and values of those who design them, the quality of the training data they use, and their intended goals. Data analytics in the public sector moreover creates complex legal, ethical, and technical issues surrounding data collection, processing, and re-use. As public authorities at all levels of government are increasingly making use of algorithmic decision making to shape and deliver public services, the use of algorithms is itself becoming the new frontier of government fairness, accountability, and also liability. Such use will also need to consistently and proactively reduce the legal, fiscal, and political risks of badly used AI algorithms in the public sector, as illustrated by Netherlands' recent experience with the use of AI algorithms in social welfare, tax, and other sectors (Box 5.1). As a result, many governments are developing standards for algorithm accountability in the public sector, though, for instance, public registers of algorithms by public agencies, as also mentioned in the next section of this chapter. In 2020, the cities of Amsterdam and Helsinki launched AI registers to detail how they use algorithms to deliver public services. Each algorithm cited in the registry lists datasets used to train a model, a description of how an algorithm is used, how humans utilise the prediction, and how algorithms were assessed for potential bias or risks. The registries also provide citizens a way to monitor the algorithms their local government uses, enabling them to evaluate, examine, or question governments' application of AI.

Box 5.1. Detecting risks in Dutch public sector algorithms

In 2022, the Dutch Court of Audit found that various government algorithms did not provide sufficient safeguards, exposing the government to various risks. In previous years, two other algorithms were also detected to be infringing legal requirements. The System Risk Indication (SyRI) algorithm system, a legal instrument that the Dutch government used to detect fraud in areas such as benefits, allowances, and taxes, was prohibited after it was found to violate the right to respect private and family life. In another case, the Dutch Data Protection Authority (AP) imposed a fine of 3.7 million euros on the Tax and Customs Administration, finding illegal processing of personal data in the Fraud Signalling Facility (FSV). The FSV acted as a blacklist on which the Tax and Customs Administration kept track of signs of fraud, but it had severe consequences for many of the individuals who were wrongfully listed.

Sources: https://www.loc.gov/item/global-legal-monitor/2020-03-13/netherlands-court-prohibits-governments-use-of-ai-software-to-detect-welfare-fraud/; https://eulawenforcement.com/?p=7941; https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-belastingdienst-voor-zwarte-lijst-fsv; https://www.cliffordchance.com/insights/resources/hubs-and-toolkits/talking-tech/en/articles/2022/04/dutch-government-fraud-scandal-leads-to-record-breaking-gdpr-fin.html; https://english.rekenkamer.nl/publications/reports/2022/05/18/an-audit-of-9-algorithms-used-by-the-dutch-government.

5.4.3. Reducing discretion and improving fairness

By digitalising government services end-to-end, governments can increase fairness and equal treatment. The OECD Trust Survey indicates that only 4 out of 10 respondents (39.8%) across OECD countries believe rich and poor people are treated equally by a public employee (OECD, 2022[32]). Furthermore, only 15 of the surveyed OECD countries has over 50% to 75% of the respondents expecting to be treated fairly in applying for a government benefit or using a public service. Government digital services contribute to standardise and equalise citizens' access to public services – but there is still room for improvement. Fair access to online digital services requires universal access and capacity to use digital channels, to "leave no-one behind", which is not the case in most countries. This is why governments combine online and offline service channels to ensure universal access. Nevertheless, the digitalisation of back-office administrative processes has significantly improved service delivery. It has also contributed to increase the reliability of governments and can also enhance its responsiveness to users' needs. From the design perspective, embedding the needs and limitations of citizens through a user-centred approach can help producing more accessible and highly usable services, and act as a direct gateway for a wider range of users into the democratic process. These dimensions are central to the forthcoming OECD *Good Practices Principles on Public Service Design and Delivery in the Digital Age*.

The expansion of government services that are directly accessible on-line and end-to-end contributes both to the reliability and integrity of public services. By digitalising public services, governments aim first to improve the effectiveness and efficiency of service delivery, but by limiting discretion, these reforms also reduce red-tape and thus petty corruption (Aiolfi, 2017[103]). This is especially important in emerging economies for widely-used critical services around people's life events, such as birth certificates, drivers' licenses, construction permits and business licenses – high-impact public services that are particularly vulnerable to bribe solicitation. The digitalisation of government services also reduces information asymmetries between governments and users (citizens and businesses) that often enable corruption (Charoensukmongkol and Moqbel, 2014[104]; Adam and Fazekas, 2018[105]). It generates better data on bottlenecks and vulnerabilities in service delivery, critical to improve service quality and user satisfaction.

The digitalisation of government services helps reduce regulatory burden, simplify administrative procedures, and generates important integrity benefits. Reliable, corruption-proof public services contribute, in turn, to increase trust in government and its ability to provide services in a continuous, fair and equal manner. The combination of digitalisation and simplification of bureaucratic procedures tends to improve both their transparency and reliability in the delivery of public services and equalise users' access to administrative services. The automation of bureaucratic processes and decreased reliance on paper cuts discretion and reduces arbitrary interference, making government transactional services less prone to tampering. In particular, digital solutions to pay for public services significantly reduce bribe solicitation risks for citizens and firms.

5.4.4. Way forward

Looking ahead, a number of priorities stand out for governments to consider:

- Intensify efforts to advance the availability, accessibility and re-use of open government data, and ensure the ethical and responsible use of data and artificial intelligence solutions in the public sector;
- Expand the reuse of data and the application of new technologies along the whole policy cycle and in particular by integrity institutions to improve value-for-money, strengthen accountability, and prevent the misuse of public resources;
- Embed open government principles in particular through the generalisation of open budgeting and open contracting practices at all levels of government as well as in state-owned enterprises;
- Reduce discretion and improve fairness in policy making and access to services by designing government digital services that are people-centred and digital by design.

5.5. Refitting public governance for digital democracy: Institutions and legal frameworks

Governments have the primary responsibility to steer the digital transformation in a way that reinforces democracy, establishing governance models and standards that reflect democratic values, enabling the monitoring of compliance, and providing effective remedies when rights are infringed upon. While digitalisation can pose threats to democratic institutions, a more mature digital governance can also leverage it to help re-intermediate and reinforce democratic institutions, when supported by the adequate institutional and governance arrangements as discussed (Berg and Hofmann, 2021[1]).

To achieve this, governments are adjusting the democratic architecture and strengthening their institutional capacities to better foster digital democracy and mitigate digital risks to democracy. In recent years, governments in OECD democracies have introduced a number of initiatives in that direction. Making the most of the digital transition for democracy requires governments to upgrade and transform public sector institutions, revise normative frameworks and develop new ways of working both domestically and internationally. This section looks at how governments are refitting public governance for digital democracy by adapting existing and creating new i) policy institutions; ii) legal and regulatory frameworks; iii) regulatory bodies and arrangements; iv) forms of international co-ordination.

5.5.1. Policy institutions for digital democracy

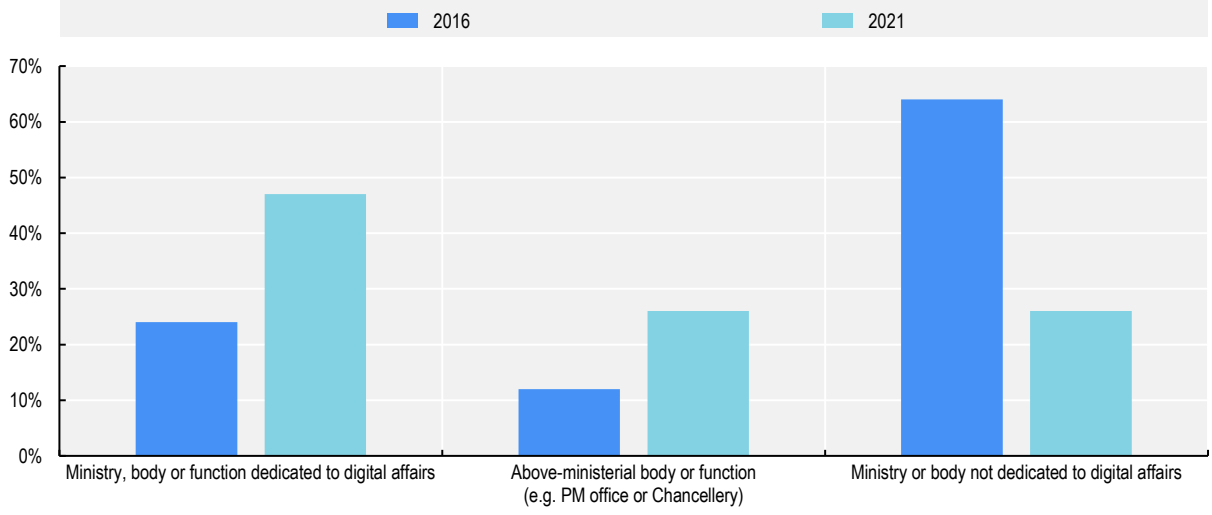
Whatever the choice of institutional model, it is important to ensure the capacity of governments to steer whole-of-government approaches to digitalisation that protect individual and collective rights, promote democratic values and enforce the ethical use of technology across public institutions. Keeping pace with technological advancements and evolving mandates may also require changes to resourcing skills, building institutions' regulatory capacity, and adapting existing institutional set-ups. It also requires making sure the civil service remains fit for purpose (OECD, 2020[106]; OECD, 2021[107]; OECD, 2021[108]), fostering civil servants' empathy for digital inclusion and their awareness on the ethical use of data.

Throughout the OECD and beyond, countries are pursuing different national and international governance models to co-ordinate the design and delivery of policies to enable the digital transition. Responsibilities of existing bodies are being adjusted, or new institutions, roles and functions are beginning to emerge. In many cases adjustments to existing institutional settings are being made to ensure whole-of-government approaches to policy development and enforcement. Centres of government and key line ministries play a critical role in steering and leading on policy design, development and implementation.

Centres of government, in particular, are playing a critical role in setting a national digital strategy and driving its implementation across government. Between 2016 and 2021, the share of countries that allocated the responsibility for developing and overseeing their national digital strategy to a dedicated ministry, body or function increased from 24% to 47% (Gierten and Lesher, 2022[109]). The share of countries that allocate this responsibility to their centre of government (presidency or prime minister's office) or an above-ministerial function (e.g. a deputy prime minister) has also increased markedly, from 12% to 26% (Figure 5.3) (Gierten and Lesher, 2022[109]). In Spain, the Vice Presidency of Economic Affairs and Digital Transformation plays a pivotal role in the development and deployment of digital transformation strategies. In the United States, the White House Office of Science and Technology Policy (OSTP) advises the President and appoints innovative officers such as the Chief Tech Officer and the Chief Data Scientist.

Figure 5.3. Allocation of responsibility for developing the country's national digital strategy

% of countries by allocation of responsibility for strategy development, 2016 and 2021



Source: Gierten and Lesher (2022[109]), "Assessing national digital strategies and their governance", *OECD Digital Economy Papers*, No. 324, OECD Publishing, Paris, https://doi.org/10.1787/baffceca-en.

The strengthening of governments' central steering functions has also focused on the most influential technologies or policy concerns. The governance of AI provides a good example. France co-ordinates AI policy implementation from within the Prime Minister's Office, while Colombia set up an AI Task Force in the Presidency. In the United States, the White House Office of Science and Technology Policy oversees the United States' national AI strategy. Similarly, in order to ensure the ethical use of data as part of the whole-of-government digital transformation agenda, Ireland's Chief Information Officer has taken a leading role in establishing and co-ordinating the activities of a Data Governance Board designed to support the drafting and implementation of the Data Governance Act across the whole public sector.

The acceleration of digital transformation has required the strengthening and adjustment of the central steering and co-ordination functions to ensure whole-of-government alignment, including at times through dedicated ministries. Countries have established inter-ministerial co-ordination committees to ensure coherence across policy areas and created positions of chief digital officers and chief data officers in the centre of government to steer whole-of-government approaches. Some countries such as Greece, Luxembourg, and Norway have gone further and created dedicated ministries for digitalisation and established or strengthened autonomous government agencies responsible for digital transformation, such as Australia, Denmark, Italy, Japan, and Sweden. These mechanisms are designed to strengthen synergies and foster whole-of-government approaches to digitalisation.

While the lead on strategy, policy development and design rests largely on centres of government and key line ministries, several countries have also set-up specialised advisory bodies, which incorporates advice in support of democracy. Examples include Germany's Data Ethics Commission, the Data Ethics Advisory Group in New Zealand, the UK's Centre for Data Ethics and Innovation, and the Singapore's Advisory Council on the Ethical Use of AI and Data. In the United Kingdom, the *Centre for Data Ethics and Innovation* (CDEI), a government advisory body, is working with government and external actors to understand public attitudes towards the use of data and AI, and the values that citizens want reflected in models of data and AI governance.[21] Some countries also report more detailed monitoring assessments of the implementation of their AI strategies and policies, including information such as budgets, funding, and specific targets. In addition, several countries have established AI observatories to oversee the implementation of national AI strategies and policies at the national or subnational levels. For example, the German Labour Ministry launched the KI-Observatorium; Quebec's International Observatory on the Social Impacts of Artificial and Digital Intelligence; France's Observatory on the Economic and Social Impact of Artificial Intelligence; the Italian Observatory on Artificial Intelligence; and the Czech Republic's AI Observatory and Forum.

5.5.2. Legal and regulatory frameworks for digital democracy

As the pace of digital transformation accelerates, OECD countries are adapting their legal and regulatory frameworks to digital complexity. At the top level, this entails ensuring that their legal frameworks are fit to harness the opportunities and challenges that the digital age brings for the protection of fundamental rights and fundamental pillars of democracy (Box 5.2). This trend is part of a debate on digital rights being led under the purview of the OECD Committee on Digital Economy Policy (CDEP).

Box 5.2. Protecting fundamental rights in the digital era

In some OECD countries constitutions provisions reaffirm democratic rights in the digital space, for instance around human dignity, privacy and data protection. Legislation has also gradually evolved in the same direction. In 2014, Brazil became the first country to pass a Civil Rights Framework for the Internet (Marco Civil da Internet) into law, to protect internet privacy, free expression, and net neutrality. In Spain, the 2022 Integral Law for Equal Treatment and Non-Discrimination contains the first regulation on the use of AI by public administrations to prevent discrimination. Similarly, in 2021, Portugal approved a Charter of Human Rights in the Digital Era enshrined into law. Often, these laws and regulation follow the adoption by countries of non-binding international instruments reaffirming their commitment to guaranteeing civil and political rights in the digital era.

Regulation at the regional level is also emerging to set common standards. In particular, in the EU current wave of digital regulation includes the European Digital Markets Act (DMA), the Digital Services Act (DSA) and the Artificial Intelligence (AI) Act. They all incorporate new principles and mechanisms for protecting fundamental rights in the digital sphere. In 2020, the European Council presented a draft Charter of Fundamental Rights in the Context of Artificial Intelligence and Digital Change, to anchor the EU's fundamental values and advance rights-based approaches to digitalisation. Similarly, in January 2022, the European Commission tabled a proposal for a European Declaration on Digital Rights and Principles for the Digital Decade to ensure that the EU's values and citizens' rights guaranteed by EU's law are respected and upheld both offline and online. The draft declaration covers key principles for the digital transformation, such as fostering participation in the digital public space, supporting inclusion, and increasing citizen empowerment.

Source: Author's own elaboration

At the same time, policy specific laws and regulation remain a key lever for governments to face the digital age. For this to take place governments need to ensure that their legal and regulatory frameworks are fit to face the challenges brought by digital technologies, including on how they are designed, implemented, and enforced.

To ensure that regulations meet their desired objectives and overcome the challenges presented by the digital transition, regulatory practice must be underpinned by the necessary principles, mechanisms and institutions (OECD, 2012[110]). At the same time, governments need to embed long-standing principles of better regulation in their responses to digital markets and services. These include ensuring that regulatory responses are proportional, risk-based and do not over-burden economic actors. Their design should be based on an assessment of impact as well as non-regulatory options, and an inclusive consultation of stakeholders. A sound regulatory framework also needs to measure the effectiveness of the government response.

The pace and scope of the digital transition may call for an even more ambitious approach to regulating. Moving away from a 'set and forget' approach to rule-making, governments will need to propose more adaptive, flexible and iterative assessment cycles, constant monitoring of regulations (i.e. *ex post* evaluation), and continuous stakeholder engagement, adaptive, iterative, and flexible regulatory assessment cycles, as per the *OECD Recommendation on Agile Regulatory Governance to Harness Innovation* (OECD, 2012[110]; OECD, 2021[108]). The goal will be to create regulatory frameworks that are agile enough to accommodate innovations and ensure that rules don't become outdated, irrelevant, or an undue burden on public and private actors.

Developing policy standards and guidelines is especially relevant for public sector use of emerging technologies in particular artificial intelligence. Some countries are developing and deploying specific ethical standards to this effect, aimed at allowing the public to better understand and monitor the use and functioning of algorithms and data by government agencies.[22] In the United States, for example, the National AI Initiative Act of 2020 provides an integrated framework to co-ordinate the development and deployment of AI, both in the public and private sectors.[23] Through Executive Order 13960 of 2020, the United States has established guidelines for promoting the use of trustworthy AI across the federal government. In France, the 2016 *Digital Republic Law* mandates transparency of public algorithms that compels public agencies to publicly list the main decision-making algorithmic tools and to publish their rules. More recently, in New Zealand, the government adopted a set of *Principles for the Safe and Effective use of Data and Analytics* in 2019 to guide government agency practices and increase confidence in how government agencies use algorithms[24] and in 2020, released the *Algorithm Charter for Aotearoa New Zealand* as an evolving guidance on the use of algorithms by government agencies. In the United Kingdom, the *Data Ethics Framework* and the Service Manual[25] provide guidance for teams across government to make an appropriate and responsible use of data and AI and build and manage user centred services to enhance digital inclusion and improve equitable access.

Open public registers and *ex ante* impact assessments can help national and local governments implement transparency standards and increase public confidence about the use of algorithms. York, Amsterdam, and Helsinki have created open registries of algorithms used by municipal authorities. *Ex ante* assessments of the potential impact of algorithm on civil rights is also a tool being developed by democratic governments to mitigate risks. The Netherlands, for example, the *Fundamental Rights and Algorithms Impact Assessment* adopted in 2021 is a tool for public institutions considering developing or purchasing an algorithmic system that requires them to assess the likely impact of the use of algorithms on specific human rights. Similarly, Canada's *Algorithmic Impact Assessment* (AIA) developed in 2022 helps determine potential impacts of an automation project on individuals and communities, including rights and freedoms.

Finally, allowing citizens to prove their identity online, claim their rights, and exercise their duties is central to democracy. This suggests a central role for government-led digital identity (Box 5.3).

Box 5.3. Digital identity as an important enabler

Securing universal access to digital identification and authentication is a critical institutional enabler to reinforce democracy in the digital age. With the caveat of having the right safeguards for privacy and security, the role of digital identity in allowing citizens to prove their identity online, claim their rights, and exercise their duties is central to democracy. It is also required to foster equal access to both offline and online services, ensuring equal treatment and digital inclusion. For example, digital identity can provide easier and more inclusive ways to access health services, open a bank account, or claim access to government benefits while ensuring high levels of trust in those interactions and transactions.

For marginalised groups and communities that may lack analogue proofs of legal identity, new technologies and means for identity registration, identification, and authentication may be used to help these individuals be included faster in society. For example, in **India**, the rollout of the national digital identity number Aadhaar proved to be an efficient way to support the world's largest democracy in facilitating the delivery of social benefits payments to eligible citizens amidst the COVID-19 pandemic, while simultaneously reducing risks of fraud (Sengupta, 2022[111]). On March 30, 2020, the Indian government recorded the highest number of transactions of a single day in the public financial management system, largely driven by the direct benefit transfers enabled by Aadhaar.

While there are vast opportunities for digital identity to support digital inclusion, there are also certain risks of full reliance on digital identity affecting inclusion negatively. This is especially the case when some groups in society prefer analogue channels, or a combination of analogue and digital channels, which remains the case in most countries - even those with high digital maturity and digital identity adoption.

Collaborating around a common understanding and set of principles on the "management of digital identity as a service" can help empower citizens to move more freely, to more easily access different services, and to be able to take more control over their personal data also across borders. If designed and delivered right, digital Identity may enable citizens to prove who they are and their possession of specific attributes, improving their local and international democratic engagement.

Since 2017, the OECD Working Party of Digital Government Officials has been mapping practices, challenges and opportunities for developing digital identity domestically and for achieving cross-border mutual recognition of national digital identities and credentials. Given that the 38 OECD member countries all follow common democratic principles, such as the right to privacy, freedom of expression, and freedom of movement, they are particularly fit to agree on what makes digital identity successful in terms of supporting democracy, and how the process for cross-border mutual recognition of digital identity can be designed and delivered while maintaining or even strengthening the implementation of democratic principles.

The OECD also works with other international fora to support international collaboration on digital identity that aligns with democratic principles, including with the G20, through the Digital Economy Task Force - that the OECD assisted through the development of the G20 Collection of Digital Identity Practices (G20, 2021[112]; OECD, 2021[113]).

5.5.3. Regulatory and oversight bodies for digital democracy

Regulatory agencies are at the delivery end of the policy cycle and play an increasingly important role in delivering digital policy objectives as well as being tasked with regulating the complex digital sphere. From a democracy perspective, regulatory authorities are increasingly at the forefront of ensuring greater democratic control, state sovereignty, and oversight over digital platforms (e.g. social media, e-commerce platforms) and the mitigation of systemic risks such as manipulation or disinformation.

Ensuring that regulators are effective in the digital sphere is raising important issues in terms of the **mandate and powers** of regulatory agencies, their **capacity** to deliver their functions, and well as how they **co-ordinate** with other public authorities.

- ***Mandate and powers*****:** For many regulatory authorities, regulating the digital sphere and digital platforms will require a new or significantly expanded mandate. For example, until recently, many digital activities and platforms had not been subject to external regulation or fell between regulatory siloes. New mandates will need to be matched with appropriate powers – most notably powers for data collection and publication – to ensure that regulators can deliver on their new role.
- ***Capacity*****:** The capacity of regulators to deliver effectively is multidimensional. Regulators' workforces need to have the right skills and knowledge to keep pace with rapidly evolving technologies and business models, bolstering their expertise in fields beyond traditional regulator profiles, from data science and cybersecurity to cloud computing, algorithms and more. Funding arrangements will determine whether regulators have adequate financial resources to carry out their functions effectively. The ability to access and process data and information from digital platforms will also underpin the success of regulatory implementation.
- ***Co-ordination between public authorities*****:** Regulating the digital sphere and digital platforms raise concerns in several regimes concurrently, meaning that any individual regulator will need to

have a broad view of the multiple issues at stake to avoid issues falling between regulatory siloes. For example, in the competition area, "non-traditional concerns" such as privacy, consumer protection or misleading information are entering into competition investigations and decisions. Regulatory co-operation between different jurisdictions will also be needed both for regulatory coherence and for effective enforcement, given the cross-border nature of digital platforms.

While some of the challenges posed by the digital transition may be novel, long-standing democratic principles and good practices in terms of the governance of regulatory agencies remain as valid as ever. Lessons learned on role clarity, independence, transparency and accountability, stakeholder engagement, and resourcing can be applied to the regulatory institutions and systems that governments are putting in place today. Good governance provides the bedrock for impartial, evidence based-decision making that builds trust in public institutions. The OECD's Network of Economic Regulators brings a decade of accumulated experience in discussing and examining the governance and performance of regulators to together define what makes a world class regulator.

Different governance arrangements are emerging in response to these issues. For example, when it comes to digital platforms, countries are following various paths. Many jurisdictions are opting for a statutory regulator over self-regulation.[26] Statutory regulation introduces an independent, impartial and accountable regulatory and adjudication regime and empowers an authority that has long experience in balancing different fundamental freedoms and rights. A number of countries have *leveraged existing independent regulatory authorities*. For example, many communication and broadcasting regulators have responsibility for the delivery of several policy objectives that are relevant to digital democracy.[27] An OECD survey showed that communication regulators have taken on at least partial responsibility for digital security (65% of those surveyed), privacy (53% of those surveyed) and online platforms (40% of those surveyed).[28] For example, the UK's communication regulator Ofcom already has responsibility for regulating video-sharing platforms and is now preparing to take on a new role in regulating online safety more broadly. The regulator is considering how its existing toolkit of regulatory techniques and approaches will need to be adapted to meet the challenges ahead (OFCOM, 2021[114]). In Germany, the 2021 Act to Regulate Data Protection and Privacy in Telecommunications and Telemedia clarified the role of the multisector regulator Bundesnetzagentur (BNetzA), which includes responsibilities on enforcement regarding data and privacy protection in online services.

In other cases, countries have *merged authorities to exploit synergies*. For example, France merged the Supreme Authority for the Distribution and Protection of Intellectual Property on the Internet (HADOPI) and the Audio-Visual Council (CSA) in order to create the Audio-Visual and Digital Communications Regulatory Authority (Arcom).

Additionally, several countries are considering the establishment of a new type of regulatory body to tackle digital issues in a holistic manner. This reform, in turn, raises questions on how the new body would interact with existing regulators with responsibilities in relevant fields, such as content regulation.

In some policy areas, responsibility for regulatory delivery and enforcement may be shared between several institutions. In the area of the regulation of artificial intelligence, the **United Kingdom** is laying the groundwork for its future model of AI regulation along with its new Data Protection and Digital Information Bill. Unlike the EU's approach, in which enforcement of the AI Act falls with a single national regulator in each member state, the United Kingdom plans to give responsibility to several of them: the UK communications regulator (OFCOM), the Competition and Markets Authority (CMA), the Information Commissioner's Office (ICO), the Financial Conduct Authority (FCA) and the Medicines and Healthcare products Regulatory Agency (MHRA) are on the list. Some of them could see their competences and powers updated.

In other areas, the specific roles and responsibilities of authorities are still to be defined. For example, in the EU, discussions are underway on how national authorities should or should not increase their functions and how they will co-ordinate with the future agencies in charge of the implementation of the European digital market regulation architecture articulated in the Data Act, Digital Markets Act, Digital Services Act, Data Governance Act and AI act.

Governments are also exploring *more formalised cross-sectoral co-operation among regulators* given that digitalisation cuts across a number of regulatory regimes, including communications, data, content, financial services, consumer protection and competition (OECD, forthcoming[115]; OECD, 2021[108]; OECD, 2021[116]). Notable examples include the United Kingdom's Digital Regulation Co-operation Forum (DRCF),[29] the Dutch Digital Regulation Co-operation Platform,[30] and the joint guidance on big data regulation and platforms developed by three Italian regulators.[31] Such structures go beyond mere information sharing and can include pooling of expertise and resources, reporting on results and mutual support to enforcement procedures. In a first case involving a digital platform, the UK's DRCF is helping balance privacy and competition concerns, for example. The European Union's Digital Services Act legislative proposal provides for a co-operation and co-ordination mechanism for the supervision of the obligations it imposes on online services and platforms (European Commission, 2020[117]).

Importantly, without adequate co-ordination across borders, regulatory initiatives that focus solely on the domestic level risk undermining the effectiveness of regulators and regulatory regimes reducing the benefits for democratic societies. In particular, regulators are confronted with major asymmetries of information when dealing with digital platforms and their algorithm driven business models. Regulatory enforcement is challenged by the transboundary nature of platforms and the uncertainty around liability from digital platforms to individual market participants. Moreover, the pace and scope of innovation in these markets often renders traditional boundaries and existing governance regimes outdated. Most national regulators are not empowered to regulate digital platforms and lack adequate institutional capacity and resources to do so. Furthermore, several of these enforcement challenges are also faced by courts and other actors in the judicial system (Box 5.4). Multi-dimensional challenges ranging from competition to data protection to content moderation require wide reaching co-ordination at both the national and global level as well as clarity of roles across government agencies and actors. Broader international co-operation is covered in more depth in the following section.

Box 5.4. Justice administration and law enforcement in the digital age

An effective rule of law and justice system plays a crucial role in protecting and enforcing rights in the digital sphere, including new emerging rights and obligations prompted by digital transformation. The constant development of new technologies and related regulations pose challenges for the judiciary to learn and adapt in order to fairly adjudicate party interests in this area. On the other hand, the accessibility of the justice system is a key determinant of the ability of people to bring forward their claims and uphold their rights. Therefore, efficient and effective justice systems able to channel claims in a timely manner to sustain citizen trust in courts in the face of digital transformation, coupled with enhancements to the overall accessibility and efficiency of the system, can be key levers to protect rights.

The courts themselves and justice systems more broadly are increasingly leveraging digital technologies to make judicial administration more efficient, transparent and user-centred. The digitalisation of justice administration has accelerated in recent years, especially to maintain access to justice in the wake of pandemic restrictions. In this context, the responsible and ethical use of new technologies by the courts themselves is also paramount to guaranteeing trust in the judiciary and the right to due process and to a fair trial. For instance, challenges have been reported in OECD countries concerning the needed balance between the right to a public hearing, which in a digital format may mean broadcasting court sessions, and the potential negative impacts that trial streaming may have on some parties, especially victims, witnesses and the accused (OECD, 2020[118]).

Courts increasingly use algorithms to analyse large datasets to make predictions, which can prompt efficiency gains but has also raised concerns of bias and lack of transparency. Risks to the right to non-discrimination have been raised in relation to AI systems used in crime prevention and judicial proceedings in particular. The main challenges created by AI-based predictions are related to bias resulting from originally biased datasets (for instance, those containing a majority of accused defendants from particular ethnicities or neighbourhoods) and lack of transparency of the process and reasoning followed to reach the decision (Reiling, 2020[119]). Similarly, law enforcement agencies increasingly use predictive policing through algorithmic processing of historical crime data and other sources to reveal patterns of criminal activity and identify targets for police intervention (Lander and Nelson, 2021[120]; AlgorithmWatch, 2020[121]; Gonzalez Fuster, 2020[122]; Wilson, 2018[123]; Perry, 2013[124]).

As a result, algorithmic risk assessments are increasingly being used in law enforcement and justice administration. Several regulatory authorities are advancing a set of rules, principles and guidance to regulate AI platforms in judicial systems. For example, the European Ethical Charter on the use of Artificial Intelligence in Judicial Systems of the European Commission for the Efficiency of Justice (CEPEJ) provides a set of principles to be used by legislators, law professionals and policymakers when working with AI/ML tools.

In addition to regulatory bodies, oversight of enforcement in the public sector has also been strengthened to make institutions fitter for the digital age. Independent oversight institutions are taking an increasingly active role in the monitoring of government digitalisation and the protection of citizen rights. Through the *ex post* auditing of government use of digital technologies, Supreme Audit Institutions (SAIs) can play an important role in enforcing compliance with standards and contributing to refine them, for example by ensuring compliance with guiding principles and ethical rules in the use of digital innovations and artificial intelligence by public agencies. Furthermore, SAIs themselves are increasingly relying on data analytics and artificial intelligence tools to perform their oversight functions more effectively.

This new, emerging role goes beyond audit agencies' traditional oversight role in terms of legal and financial compliance, to include compliance with ethical principles in the deployment of digital innovations and the responsible use of algorithms by government agencies. In 2020, the SAIs of Finland, Germany,

the Netherlands, Norway, and the United Kingdom put forward a white paper for public auditor on auditing machine learning algorithms.[32] In 2021, the US Government Accountability Office (GAO) developed an AI Accountability Framework to ensure responsible use of AI in government programs and processes.[33] In 2021, the Netherlands Court of Audit developed an audit framework for assessing whether algorithms meet quality criteria[34] applied to investigate the Dutch government's use of algorithms, arguing that such use requires better scrutiny and stronger safeguards (especially when outsourced). In 2022, it audited 9 government algorithms and found that 6 of those did not comply with basic requirements and exposed the government to various risks, from inadequate control over the algorithm's exposure to bias, data leaks, and unauthorised access in particularly sensitive policy areas such as justice, policing, migration, and identity (Box 5.1).

Ombudsman offices are taking a more active role in the defence of citizen rights in the digital era. In Finland, for example, in 2017 the Non-Discrimination Ombudsman, which supervises compliance with non-discrimination provisions in the use of artificial intelligence and algorithms, took a case concerning automated decision-making in bank lending to the National Non-Discrimination and Equality Tribunal. The Tribunal concluded that the practice was discriminatory and imposed a conditional fine on the party found guilty of discrimination.[35]

5.5.4. International co-operation for digital democracy

The standards, norms, and regulations governing digital are on the frontlines in the contest for technological supremacy between democracies and autocracies. Data - and its governance - is thus a geostrategic asset and informs the development of new technologies and artificial intelligence.

Some regions and like-minded groups of countries have promoted common approaches to digital transformation based on shared values. Global approaches have been advanced through various settings. Many on-going initiatives reflect the need to promote international co-operation and global convergence among like-minded countries on actions, standards and principles to better align digital transformation with democratic values while strengthening democratic institutions and digital sovereignty.[36] This will help not only avoid unnecessary barriers slowing down progress and the benefits of digital technology, but also will avoid regulatory fragmentation.

An increasing number of countries, mainly democracies, are mainstreaming digital diplomacy in their foreign policy, establishing "tech ambassadors" whose mandate originally focused on cybersecurity to include a mandate for engaging the tech industry in Silicon Valley and, more recently, promote rights-based approaches to digital development. Whilst adopting different models and having diverse mandates, Australia, Denmark, Estonia, France, the United Kingdom, Germany, Brazil, have created tech ambassadors. In November 2020, Switzerland adopted its first Digital Foreign Policy Strategy for the period 2021–24 overseen by an ambassador for digital affairs. In July 2022, the EU announced it will establish a tech envoy to Silicon Valley, in line with the European Council's conclusion on digital diplomacy.

To enhance global co-operation, like-minded countries have created platforms for collaboration and special initiatives on "digital democracy", among which, for example:

- The Digital Nations is an international forum founded in 2014 of leading digital governments to harness the potential global power of digital technology for better government and services. It currently comprises 10 governments (Estonia, Israel, Korea, New Zealand, UK, Canada, Uruguay, Mexico, Portugal, and Denmark). Participating governments are connected by public governance principles of user needs, open standards, open source, open government, and digital inclusion, enshrined in its founding charter updated in 2021. For example, in 2018, it endorsed a common approach to the responsible use of artificial intelligence in government services, based on the principles of transparency, accountability, and procedural fairness.

- The Agile Nations Network, established in 2020 to foster global co-operation on rulemaking in response to innovation and enhance international co-operation to improve the resilience and readiness of governments for the future in key transnational policy areas such as data assets, financial transaction technology and green-tech. Currently chaired by the UAE, it comprises 7 governments (Canada, Denmark, Italy, Japan, Singapore, UAE, and UK).
- In December 2021, the US-led global Summit for Democracy discussed the challenges and opportunities facing democracies in the digital era.[37] It provided an opportunity to build global consensus on a positive vision of digital democracy - including through International Grand Challenges on Democracy-Affirming Technologies - and international co-operation to counter "digital authoritarianism."[38] Participating governments announced a wide range of commitments in support of democratic renewal that included commitments to invest in the development, use, and governance of technology that advances democracy and human rights. The follow-up Summit for Democracy in 2023 will provide an important opportunity to advance this initiative.
- The Danish-led initiative on "Tech for Democracy", launched in November 2021 provides a platform for multi-stakeholder dialogue on technology for democracy and human rights, bringing together governments, multilateral organisations, tech industry and civil society.[39]
- In the area of artificial intelligence, the Global Partnership on AI (GPAI)[40] is a multi-stakeholder and inter-governmental alliance of 25 members developed in 2020 that aims to deliver on the shared commitment to the *OECD Recommendation of the Council on Artificial Intelligence* and support cutting-edge research and applied activities on AI-related priorities, including in the public sector.
- The private sector, including tech industries, are also launching initiatives aimed at promoting democracy-enhancing initiatives as part of the tech4good movement. For example, Microsoft Democracy Forward initiative aims "to protect open and secure democratic processes and preserve access to trusted journalism to help build a healthier information ecosystem." In terms of elections, for example, it aims to protect the security of critical electoral institutions, the integrity of elections, and open-source elections software.

At the global level, in 2020 the United Nations adopted a Roadmap for Digital Cooperation that seeks to advance a rights-based approach to digital transformation embedded in rights and trust. In September 2021, it released a report on *Our Common Future* that proposes a *Global Digital Compact* to be agreed at the Summit of the Future in September 2023. This Compact is expected to "outline shared principles for an open, free and secure digital future for all". Acknowledging the importance of technology as a fundamental global issue, the UN Secretary General appointed in 2021 a UN Envoy on Technology.

Governments can also co-operate to advance global digital public goods and share digital public infrastructure for a fairer digital transition (United Nations, General Assembly, 2020[125]). The OECD 2021 Global Development Cooperation Report *Shaping a Just Digital Transformation* (OECD, 2021[126]) outlines the many global and regional initiatives in that direction, including:

- The Global Public Goods Alliance and the Digital Impact Alliance, are multi-stakeholder initiatives to accelerate the attainment of the sustainable development goals in low- and middle-income countries by facilitating development and use of digital public goods, enabling countries to build safe, trusted, and inclusive digital public infrastructure at scale.
- The GovStack initiative aims at accelerating digital transformation in developing countries by developing and sharing foundational building blocks of digital government through open-source solutions for identification, registration and payments systems.
- The EU is considering a European Initiative for Digital Commons.[41] Digital commons are non-rivalrous and non-exclusive digital resources defined by shared production, maintenance and governance. The initiative seeks to promote digital commons and open-source software and encourage their use within European institutions and Member States' public services.

Many international policy commitments and standards have emerged that aim to reaffirm and reinforce the democratic values underpinning digital transformation. The EU Tallinn, Berlin and Lisbon Declarations on digital democracy; G7 Digital and Tech Ministerial declaration of 2021; and the G20 Digital Ministerial Declaration of 2021 all reflect the increased awareness of the need to promote international co-operation and global convergence among like-minded countries on actions, standards and principles that can advance common approaches to digital transformation based on shared values and can make democratic institutions more fit for the digital age (see Chapter 3).

Similarly, some regions, or like-minded groups of countries, have set common principles or rules through multilateral organisations to address the transnational nature of digitalisation.

- The OECD, under the purview of its Committee on Digital Economy Policy (CEDP), has developed a number of ground-breaking principles over time. In the case of artificial intelligence, the OECD AI Principles adopted in 2019 have been endorsed by 46 governments.[42] They include 5 principles to ensure that AI systems are trustworthy and human-centric and respect democratic values and human rights, in both the private and public sectors. They are accompanied by 5 policy recommendations that policy makers should consider to foster thriving artificial intelligence ecosystems that respect human rights and democratic values. The OECD *Good Practice Principles for Data Ethics in the Public Sector* (OECD, 2021[127]) were also developed to support the ethical use of data in government services.
- The European Union (EU) has developed a set of guidelines[43] and is working towards a risk-based framework, the AI Act that would demand some additional checks for "high risk" uses of artificial intelligence that can produce the most potential harm to people, including uses in the public sector (e.g. recruiting people, grading in schools, helping judges make decisions).
- The Council of Europe has long worked towards an application of new technologies based on human rights, the rule of law and democracy, in line with the European Convention on Human Rights. In 2019, its Committee of Ministers adopted a Declaration on the manipulative capabilities of algorithmic processes and, in 2020, a Recommendation on the human rights impacts of algorithmic systems.
- At a global level, UNESCO's General Conference adopted the *Recommendation on the Ethics of Artificial Intelligence* in November 2021,[44] a global standard containing relevant principles guided by ethical values. It is aimed at assisting States and non-State actors in the formulation of instruments to promote artificial intelligence for human dignity and the prevention of harm.

The mismatch between the primarily national nature of democratic guarantees and the global challenges of digital transformation requires closing the gap in multilateral digital governance. In terms of global regulatory co-operation, for example, the 2022 *OECD Recommendation of the Council on International Regulatory Co-operation to Tackle Global Challenges* intends to support governments in this transition. To reinforce digital democracy, the *Recommendation of the Council for Agile Regulatory Governance to Harness Innovation* of 2021 invites governments to consider the broad "international innovation ecosystem" and also lay the "institutional foundations to enable co-operation and joined-up approaches, both within and across jurisdictions" (OECD, 2021[108]).

Looking ahead, two priorities stand out to ensure effective international regulatory co-operation. It will be key to reduce loopholes resulting from the fragmented international normative landscape and give greater visibility to the breadth of standards that already exist in relation to digital governance and ensure their implementation. Taken as a whole, the diverse and dynamic "international innovation ecosystem" described above has the potential of being flexible and agile in responding to the complex challenges posed by digitalisation, as long as there is true co-ordination and complementarity.

5.5.5. Way forward

Several priorities stand out for like-minded OECD governments to strengthen public governance in support of democracy in the digital age:

- Consider the need for the upgrading and adjusting mandates, functions and resources of policy, regulatory and oversight bodies to ensure they have the appropriate capacity to design and implement standards for democracy-enhancing digital transformation.
- Foster international regulatory co-operation to reduce gaps and close loopholes resulting from the fragmented international normative landscape and give greater visibility to emerging standards on digital governance.
- Invest in digitally-enabled democratic innovation through the diverse and dynamic international innovation ecosystem that has the potential of being flexible and agile responses to the complex challenges posed by digitalisation for democracy.

An Action Plan to support the transformation of public governance for digital democracy will be developed by the OECD Public Governance Committee in due course (see www.oecd.org/governance/reinforcing-democracy/).

References

ACE project/International IDEA (2014), *Electoral Management*, https://aceproject.org/ace-en/topics/em/emi/emi03/emi03b (accessed on 28 April 2022). [17]

Adam, I. and M. Fazekas (2018), "Are emerging technologies helping win the fight against corruption in developing countries?", *Pathways for Prosperity Commission Background Paper Series*, No. 21, University of Oxford, Oxford UK, https://doi.org/10.13140/RG.2.2.17930.52162 (accessed on 23 May 2022). [105]

Aiolfi, G. (2017), "New perspectives in e-government and the prevention of corruption", *Basel Institute on Governance Working Paper*, No. 23, Basel Institute on Government, https://baselgovernance.org/publications/working-paper-23-new-perspectives-e-government-and-prevention-corruption (accessed on 23 May 2022). [103]

AlgorithmWatch (2020), *Automating Society Report 2020*, https://automatingsociety.algorithmwatch.org/wp-content/uploads/2020/12/Automating-Society-Report-2020.pdf. [121]

Anett Numa (2021), "Another record-high i-voting turnout at the local elections", *e-Estonia*, https://e-estonia.com/another-record-high-i-voting-turnout-at-the-local-elections/ (accessed on 13 September 2022). [27]

Barrett, B., K. Dommett and D. Kreiss (2021), "The capricious relationship between technology and democracy: Analyzing public policy discussions in the UK and US", *Policy and Internet*, Vol. 13/4, https://doi.org/10.1002/poi3.266. [38]

Bauhr, M. and M. Grimes (2013), "Indignation or Resignation: The Implications of Transparency for Societal Accountability", *Governance*, Vol. 27/2, pp. 291-320, https://doi.org/10.1111/gove.12033. [92]

Beam, M., M. Hutchens and J. Hmielowski (2018), "Facebook news and (de)polarization: reinforcing spirals in the 2016 US election", *Information, Communication & Society*, Vol. 21/7, pp. 940-958, https://doi.org/10.1080/1369118x.2018.1444783. [50]

Berg, S. and J. Hofmann (2021), "Digital democracy", *Internet Policy Review*, Vol. 10/4, https://doi.org/10.14763/2021.4.1612. [1]

Bermeo, N. (2016), "On Democratic backsliding", *Journal of Democracy*, Vol. 27/1, pp. 5-19, https://doi.org/10.1353/jod.2016.0012. [3]

Berryhill, J., T. Bourgery and A. Hanson (2018), "Blockchains Unchained: Blockchain Technology and its Use in the Public Sector", *OECD Working Papers on Public Governance*, No. 28, OECD Publishing, Paris, https://doi.org/10.1787/3c32c429-en. [99]

Bradshaw, S. and P. Howard (2017), *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation, Computational Propaganda Research Project*, http://governance40.com/wp-content/uploads/2018/11/Troops-Trolls-and-Troublemakers.pdf (accessed on 27 April 2022). [34]

Charoensukmongkol, P. and M. Moqbel (2014), "Does Investment in ICT Curb or Create More Corruption? A Cross-Country Analysis", *Public Organization Review*, Vol. 14/1, pp. 51-63, https://doi.org/10.1007/S11115-012-0205-8. [104]

Council of Europe (2018), *Internet and Electoral Campaigns: Study on the use of internet in electoral campaigns*, Council of Europe, Strasbourg, https://edoc.coe.int/en/internet/7614-internet-and-electoral-campaigns-study-on-the-use-of-internet-in-electoral-campaigns.html (accessed on 27 April 2022). [37]

Council of Europe (2018), *Mapping study on cyberviolence with recommendations adopted by the T-CY on 9 July 2018*, Council of Europe, Strasbourg, https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914. [55]

Council of Europe (2017), *Recommendation CM/REC (2017)5 of the Committee of Ministers to members States on standards for e-voting*, Council of Europe, Strasbourg, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f (accessed on 27 April 2022). [25]

Council of Europe (2016), *Competences for Democratic Culture*, Council of Europe, Strasbourg, https://book.coe.int/en/human-rights-democratic-citizenship-and-interculturalism/6871-competencies-for-democratic-culture-living-together-as-equals-in-culturally-diverse-democratic-societies.html. [77]

Currin, C., S. Vera and A. Khaledi-Nasab (2022), "Depolarization of echo chambers by random dynamical nudge", *Scientific Reports*, Vol. 12/1, https://doi.org/10.1038/s41598-022-12494-w. [45]

Daly, T. (2019), "Democratic Decay: Conceptualising an Emerging Research Field", *Hague Journal on the Rule of Law*, Vol. 11/1, pp. 9-36, https://doi.org/10.1007/s40803-019-00086-2. [2]

DellaVigna, S. and E. Kaplan (2007), "The Fox News Effect: Media Bias and Voting", *The Quarterly Journal of Economics*, Vol. 122/3, pp. 1187-1234, https://doi.org/10.1162/qjec.122.3.1187. [48]

Driza Maurer, A. (2020), *DIGITAL TECHNOLOGIES IN ELECTIONS Questions, lessons learned, perspectives Council of Europe*, Council of Europe, Strasbourg. [10]

European Commission (2022), *Flash Eurobarometer 506: EU's response to the War in Ukraine*, European Commission, Brussels, https://webgate.ec.europa.eu/ebsm/api/public/deliverable/download?doc=true&deliverableId=81594. [40]

European Commission (2020), *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*, European Commission, Brussels, https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN. [117]

Feldman, A., J. Halderman and E. Felten (2007), *Security Analysis of the Diebold AccuVote-TS Voting Machine*, https://www.usenix.org/legacy/event/evt07/tech/full_papers/feldman/feldman_html/index.html (accessed on 21 April 2022). [19]

Forteza, P. (2020), "Digital parliaments: Adapting democratic institutions to 21st century realities", *Participo series*, https://medium.com/participo/digital-parliaments-adapting-democratic-institutions-to-21st-century-realities-99214d352063 (accessed on 25 April 2022). [11]

G20 (2021), *Declaration of G20 Digital Ministers*, https://assets.innovazione.gov.it/1628084642-declaration-of-g20-digital-ministers-2021final.pdf. [112]

G8 (2013), *G8 Open Data Charter and Technical Annex*, https://www.gov.uk/government/publications/open-data-charter/g8-open-data-charter-and-technical-annex. [83]

Gierten, D. and M. Lesher (2022), "Assessing national digital strategies and their governance", *OECD Digital Economy Papers*, No. 324, OECD Publishing, Paris, https://doi.org/10.1787/baffceca-en. [109]

GIZ (2018), *Embracing digitialisation: How to use ICT to strengthen anti-corruption*, https://www.giz.de/de/downloads/giz2018-eng_ICT-to-strengthen-Anti-Corruption.pdf (accessed on 28 April 2022). [93]

Gonzalez Fuster, G. (2020), *Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights*, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf. [122]

GovLab (2019), *The Open Policymaking Playbook*. [65]

Grönlund, K. et al. (2020), *Implementing a democratic innovation: Online deliberation on a future transport*. [64]

Halderman, J. and V. Teague (2015), "The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election", https://arxiv.org/abs/1504.05646 (accessed on 21 April 2022). [21]

IFOP (2022), *Volet 1 : Désinformation, complotisme et populisme à l'heure de la crise sanitaire et de la guerre en Ukraine*, Institut français d'opinion publique, https://www.ifop.com/wp-content/uploads/2022/03/Rapport_Ifop_REBOOT_VOL_1_2022.03.24.pdf. [41]

InfluenceMap (2019), *Big Oil's Real Agenda on Climate Change: How the oil majors have spent $1B since Paris on narrative capture and lobbying on climate*, https://influencemap.org/report/How-Big-Oil-Continues-to-Oppose-the-Paris-Agreement38212275958aa21196dae3b76220bddc (accessed on 27 April 2022). [39]

Institute for Strategic Dialogue (2020), *Public Figures, Public Rage. Candidate abuse on social media*, https://www.isdglobal.org/wp-content/uploads/2020/10/Public-Figures-Public-Rage-4.pdf. [54]

International IDEA (2022), *ICTs in Elections Database*, International Institute for Democracy and Electoral Assistance, https://www.idea.int/data-tools/data/icts-elections (accessed on 27 May 2022). [15]

International IDEA (2021), *Regulating Online Campaign Finance: Chasing the Ghost?*, International Institute for Democracy and Electoral Assistance, https://www.idea.int/publications/catalogue/regulating-online-campaign-finance (accessed on 27 April 2022). [33]

International IDEA (2017), *Digital Solutions for Political Finance Reporting and Disclosure*, International Institute for Democracy and Electoral Assistance, https://www.idea.int/sites/default/files/publications/digital-solutions-for-political-finance-reporting-and-disclosure-a-practical-guide.pdf (accessed on 28 April 2022). [94]

International IDEA (2017), *Open Data in Electoral Administration*, International Institute for Democracy and Electoral Assistance, https://www.idea.int/sites/default/files/publications/open-data-in-electoral-administration.pdf. [31]

International IDEA (n.d.), *Political Finance Database*, International Institute for Democracy and Electoral Assistance, https://www.idea.int/data-tools/data/political-finance-database (accessed on 27 April 2022). [36]

IPU (2022), *IPU Innovation Tracker*, Inter-Parliamentary Union, Geneva, https://www.ipu.org/knowledge/ipu-innovation-tracker (accessed on 18 August 2022). [13]

IPU (2021), *World e-Parliament Report 2020*, Inter-Parliamentary Union, Geneva, https://www.ipu.org/resources/publications/reports/2021-07/world-e-parliament-report-2020. [14]

IPU (2016), *Sexism, harassment and violence against women parliamentarians*, Inter-Parliamentary Union, Geneva, https://www.ipu.org/resources/publications/issue-briefs/2016-10/sexism-harassment-and-violence-against-women-parliamentarians. [56]

ITU (2021), *Digital inclusion*, International Telecommunication Union, Geneva, https://www.itu.int/en/ITU-D/Digital-Inclusion/Pages/about.aspx. [78]

ITU (2021), *Measuring digital development, Facts and figures*, International Telecommunication Union, Geneva, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf. [9]

Kubin, E. and C. von Sikorski (2021), "The role of (social) media in political polarization: a systematic review", *Annals of the International Communication Association*, Vol. 45/3, pp. 188-206, https://doi.org/10.1080/23808985.2021.1976070. [52]

Lander, E. and A. Nelson (2021), *ICYMI: WIRED (Opinion): Americans Need a Bill of Rights for an AI-Powered World Eric Lander*, The White House, Washington DC, https://www.whitehouse.gov/ostp/news-updates/2021/10/22/icymi-wired-opinion-americans-need-a-bill-of-rights-for-an-ai-powered-world/. [120]

Lelièvre, C. (2017), "Trust and access to justice", in *Trust and Public Policy: How Better Governance Can Help Rebuild Public Trust*, OECD Publishing, Paris, https://doi.org/10.1787/9789264268920-10-en. [95]

Lindman, J. et al. (2020), "The uncertain promise of blockchain for government"*, OECD Working Papers on Public Governance*, No. 43, OECD Publishing, Paris, https://doi.org/10.1787/d031cd67-en. [100]

Lorenz-Spreen, P. et al. (2021), *Digital Media and Democracy: A Systematic Review of Causal and Correlational Evidence Worldwide*, Center for Open Science, https://doi.org/10.31235/osf.io/p3z9v. [47]

M. Heller, A. (ed.) (2022), *Towards Open Justice in Latin America and the Caribbean: an OECD perspective*, JUSBAIRES Editorial. [96]

McGuinness, T. and H. Schank (2021), *Power to the public : the promise of public interest technology*, Princeton University Press, https://press.princeton.edu/books/ebook/9780691216638/power-to-the-public (accessed on 17 August 2022). [128]

Mickoleit, A. (2014), "Social Media Use by Governments: A Policy Primer to Discuss Trends, Identify Policy Opportunities and Guide Decision Makers", *OECD Working Papers on Public Governance*, No. 26, OECD Publishing, Paris, https://doi.org/10.1787/5jxrcmghmk0s-en. [30]

Mohun, J. and A. Roberts (2020), "Cracking the code: Rulemaking for humans and machines", *OECD Working Papers on Public Governance*, No. 42, OECD Publishing, Paris, https://doi.org/10.1787/3afe6ba5-en. [68]

Mossberger, K., C. Tolbert and R. McNeal (2007), *Digital Citizenship*, The MIT Press, https://doi.org/10.7551/mitpress/7428.001.0001. [76]

Mulroy, S. (2019), "Barriers at the ballot box symposium issue", *University of Memphis Law Review*, Vol. 49/4. [22]

NASPO (2021), *Citizen engagement platforms*, https://www.naspovaluepoint.org/portfolio/citizen-engagement-platforms/ (accessed on 31 May 2022). [67]

NESTA (2017), *Digital Democracy: The Tools Transforming Political Engagement | Nesta*, https://www.nesta.org.uk/report/digital-democracy-the-tools-transforming-political-engagement/ (accessed on 25 April 2022). [59]

OECD (2022), "Delivering for youth: How governments can put young people at the centre of the recovery", *OECD Policy Responses to Coronavirus (COVID-19)*, OECD Publishing, Paris, https://doi.org/10.1787/92c9d060-en. [73]

OECD (2022), *Modernising Integrity Risk Assessments in Brazil: Towards a Behavioural-sensitive and Data-driven Approach*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/ad3804f0-en. [90]

OECD (2022), *OECD Survey on Drivers of Trust in Institutions: Main Findings Report*, OECD, Paris. [32]

OECD (2022), *Open Government Review of Brazil : Towards an Integrated Open Government Agenda*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/3f9009d4-en. [62]

OECD (2022), *Strengthening Analytics in Mexico's Supreme Audit Institution: Considerations and Priorities for Assessing Integrity Risks*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/d4f685b7-en. [89]

OECD (2022), *V-Dem's Polarisation of Society Indicator*. [46]

OECD (2021), "Bridging connectivity divides", *OECD Digital Economy Papers*, No. 315, OECD Publishing, Paris, https://doi.org/10.1787/e38f5db7-en. [8]

OECD (2021), *Countering Public Grant Fraud in Spain: Machine Learning for Assessing Risks and Targeting Control Activities*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/0ea22484-en. [102]

OECD (2021), *Development Co-operation Report 2021: Shaping a Just Digital Transformation*, OECD Publishing, Paris, https://doi.org/10.1787/ce08832f-en. [126]

OECD (2021), *G20 Collection of Digital Identity Practices: Report for the G20 Digital Economy Tak Force, Trieste, Italy, August 2021*, OECD Publishing, Paris, https://doi.org/10.1787/75223806-en. [113]

OECD (2021), *G20 survey on Agile approaches to the regulatory governance of innovation: Report for the G20 Digital Economy Tak Force, Trieste, Italy, August 2021*, OECD Publishing, Paris, https://doi.org/10.1787/f161916d-en. [116]

OECD (2021), *Government at a Glance 2021*, OECD Publishing, Paris, https://doi.org/10.1787/1c258f55-en. [61]

OECD (2021), *Lobbying in the 21st Century: Transparency, Integrity and Access*, OECD Publishing, Paris, https://doi.org/10.1787/c6d8eff8-en. [35]

OECD (2021), *OECD Database of Representative Deliberative Processes and Institutions*. [63]

OECD (2021), *OECD Good Practice Principles for Data Ethics in the Public Sector*, OECD, Paris, https://www.oecd.org/gov/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.htm (accessed on 13 September 2022). [127]

OECD (2021), *Policy Framework for Gender-Sensitive Public Governance*, OECD, Paris, https://one.oecd.org/document/C/MIN(2021)21/en/pdf. [79]

OECD (2021), "Recommendation of the Council for Agile Regulatory Governance to Harness Innovation", *OECD Legal Instruments*, OECD/LEGAL/0464, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0464. [108]

OECD (2021), "Recommendation of the Council on Enhancing Access to and Sharing of Data", *OECD Legal Instruments*, OECD/LEGAL/0463, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463. [84]

OECD (2021), *The E-Leaders Handbook on the Governance of Digital Government*, OECD Digital Government Studies, OECD Publishing, Paris, https://doi.org/10.1787/ac7f2531-en. [107]

OECD (2020), "Access to justice and the COVID-19 pandemic", *OECD Policy Responses to Coronavirus (COVID-19)*, OECD Publishing, Paris, https://doi.org/10.1787/09a621ad-en. [118]

OECD (2020), "Digital transformation and the futures of civic space to 2030", *OECD Development Policy Papers*, No. 29, OECD Publishing, Paris, https://doi.org/10.1787/79b34d37-en. [80]

OECD (2020), *Governance for Youth, Trust and Intergenerational Justice: Fit for All Generations?*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/c3e5cb8a-en. [72]

OECD (2020), *How's Life? 2020: Measuring Well-being*, OECD Publishing, Paris, https://doi.org/10.1787/9870c393-en. [28]

OECD (2020), *Innovative Citizen Participation and New Democratic Institutions: Catching the Deliberative Wave*, OECD Publishing, Paris, https://doi.org/10.1787/339306da-en. [71]

OECD (2020), *Justice Transformation in Portugal: Building on Successes and Challenges*, OECD Publishing, Paris, https://doi.org/10.1787/184acf59-en. [98]

OECD (2020), *OECD Digital Economy Outlook 2020*, OECD Publishing, Paris, https://doi.org/10.1787/bb167041-en. [7]

OECD (2020), "Open, Useful and Re-usable data (OURdata) Index: 2019", *OECD Public Governance Policy Papers*, No. 01, OECD Publishing, Paris, https://doi.org/10.1787/45f6de2d-en. [5]

OECD (2020), *Shaping the Future of Regulators: The Impact of Emerging Technologies on Economic Regulators*, The Governance of Regulators, OECD Publishing, Paris, https://doi.org/10.1787/db481aa3-en. [106]

OECD (2020), "Youth and COVID-19: Response, recovery and resilience", *OECD Policy Responses to Coronavirus (COVID-19)*, OECD Publishing, Paris, https://doi.org/10.1787/c40e61c6-en. [74]

OECD (2019), *Budgeting and Public Expenditures in OECD Countries 2019*, OECD Publishing, Paris, https://doi.org/10.1787/9789264307957-en. [69]

OECD (2019), "Digital inclusion", in *Measuring the Digital Transformation: A Roadmap for the Future*, OECD Publishing, Paris, https://doi.org/10.1787/8b47adfe-en. [82]

OECD (2019), *The Path to Becoming a Data-Driven Public Sector*, OECD Digital Government Studies, OECD Publishing, Paris, https://doi.org/10.1787/059814a7-en. [85]

OECD (2018), *Engaging Young People in Open Government: A communication guide*, OECD, Paris, https://www.oecd.org/mena/governance/Young-people-in-OG.pdf. [29]

OECD (2018), *Open Government Data Report: Enhancing Policy Maturity for Sustainable Impact*, OECD Digital Government Studies, OECD Publishing, Paris, https://doi.org/10.1787/9789264305847-en. [6]

OECD (2017), *Compendium of good practices on the use of open data for Anti-corruption*, OECD, Paris, https://www.oecd.org/gov/digital-government/g20-oecd-compendium.pdf. [91]

OECD (2017), *OECD Budget Transparency Toolkit: Practical Steps for Supporting Openness, Integrity and Accountability in Public Financial Management*, OECD Publishing, Paris, https://doi.org/10.1787/9789264282070-en. [87]

OECD (2017), "Recommendation of the Council on Open Government", *OECD Legal Instruments*, OECD/LEGAL/0438, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0438. [58]

OECD (2012), *Recommendation of the Council on Regulatory Policy and Governance*, OECD Publishing, Paris, https://doi.org/10.1787/9789264209022-en. [110]

OECD (forthcoming), *Communication Regulators of the Future*. [115]

OECD (forthcoming), *The Protection and Promotion of Civic Space: Strengthening Alignment with International Standards and Guidance*. [75]

OECD/CAF (2022), *The Strategic and Responsible Use of Artificial Intelligence in the Public Sector of Latin America and the Caribbean*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/1f334543-en. [101]

OFCOM (2021), *How we're preparing to regulate for online safety - Ofcom*, https://www.ofcom.org.uk/news-centre/2021/preparing-to-regulate-online-safety (accessed on 8 June 2022). [114]

Open Contracting Partnership (2022), *Worldwide*, https://www.open-contracting.org/worldwide/ (accessed on 13 May 2022). [88]

OSCE/ODIHR (2013), *Handbook for the Observation of New Voting technologies*, https://www.osce.org/files/f/documents/0/6/104939.pdf (accessed on 27 April 2022). [24]

Parliamentary Office of Sciences and Technology (2009), *E-democracy*, POST, https://www.parliament.uk/globalassets/documents/post/postpn321.pdf (accessed on 30 September 2022). [57]

Perry, W. (2013), *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, RAND Corporation, https://www.jstor.org/stable/10.7249/j.ctt4cgdcz. [124]

Petitpas, A., J. Jaquet and P. Sciarini (2021), "Does E-Voting matter for turnout, and to whom?", *Electoral Studies*, Vol. 71, p. 102245, https://doi.org/10.1016/j.electstud.2020.102245. [26]

Piccinin, M. (2021), "Embracing digital parliaments: An international perspective | by Mariane Piccinin Barbieri | Participo | Medium", *OECD Participo*, https://medium.com/participo/embracing-digital-parliaments-an-international-perspective-7bb74994d110 (accessed on 25 April 2022). [12]

Reiling, A. (2020), "Courts and Artificial Intelligence", *International Journal for Court Administration*, Vol. 11/2, https://doi.org/10.36745/ijca.343. [119]

Scarrow, S., P. Webb and T. Poguntke (eds.) (2017), *Organizing Political Parties*, Oxford University Press, https://doi.org/10.1093/oso/9780198758631.001.0001. [86]

Schradie, J. (2018), "The Digital Activism Gap: How Class and Costs Shape Online Collective Action", *Social Problems*, Vol. 65/1, pp. 51-74, https://doi.org/10.1093/SOCPRO/SPX042. [81]

Sengupta, D. (2022), *Direct Benefit Transfer – A blessing during the time of Pandemic*, https://www.nic.in/blogs/direct-benefit-transfer-a-blessing-during-the-time-of-pandemic/. [111]

Shortall, R. (2020), "Designing text-based tools for digital deliberation", *Participo*, https://medium.com/participo/designing-text-based-tools-for-digital-deliberation-95e9679ea79d. [70]

Sieghart, P. (1985), *The Lawful Rights of Mankind: An Introduction to the International Legal Code of Human Rights*, Oxford University Press. [129]

Smith, R. (2019), *Rage Inside the Machine: The Prejudice of Algorithms and How to Stop the Internet Making Bigots of Us All*, Bloomsbury. [42]

Specter, M., J. Koppel and D. Weitzner (2020), *The ballot is busted before the blockchain: a security analysis of voatz, the first internet voting application used in U.S. federal elections*, https://dl.acm.org/doi/abs/10.5555/3489212.3489299 (accessed on 21 April 2022). [20]

Springall, D. et al. (2014), "Security Analysis of the Estonian Internet Voting System". [18]

Sunstein, C. (1999), "The Law of Group Polarization", *Law & Economics Working Papers*, https://chicagounbound.uchicago.edu/law_and_economics/542 (accessed on 3 June 2022). [44]

The Electoral Knowledge Network (n.d.), *E-voting: benefits, risks and costs*, https://aceproject.org/ace-en/focus/e-voting/benefits-risks-and-costs/mobile_browsing/onePag (accessed on 27 April 2022). [23]

Tseng, Y. (2022), "Rethinking gamified democracy as frictional: a comparative examination of the Decide Madrid and vTaiwan platforms", *Social & Cultural Geography*, pp. 1-18, https://doi.org/10.1080/14649365.2022.2055779. [66]

UK Courts and Tribunals Judiciary (n.d.), *You and the judiciary*, https://www.judiciary.uk/you-and-the-judiciary/ (accessed on 18 August 2022). [97]

UN (ed.) (2014), *A World that Counts Mobilising the Data Revolution for Sustainable Development*, The United Nations Secretary-General's Independent Expert Advisory Group on a Data Revolution for Sustainable Development (IEAG), https://www.cepal.org/en/publications/40319-world-counts-mobilising-data-revolution-sustainable-development (accessed on 20 May 2022). [4]

UNDESA (2020), *2020 United Nations E-Government Survey*, United Nations, https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf. [60]

United Nations, General Assembly (2020), *Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation: Report of the Secretary-General, A/74/821*, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/102/51/PDF/N2010251.pdf?OpenElement (accessed on 17 August 2022). [125]

Valmyndigheten (2021), *The right to vote*, https://www.val.se/servicelankar/otherlanguages/englishengelska/voting/therighttovoteandvotingcards.4.1dac782216e1e29d789189f.html. [16]

Van Aelst, P. et al. (2017), "Political communication in a high-choice media environment: a challenge for democracy?", *Annals of the International Communication Association*, Vol. 41/1, pp. 3-27, https://doi.org/10.1080/23808985.2017.1288551. [49]

Waldron, J. (2016), "5. The Principle of Loyal Opposition", in *Political Political Theory*, Harvard University Press, https://doi.org/10.4159/9780674970342-005. [131]

Wason, P. and P. Johnson-Laird (1972), *Psychology of reasoning: Structure and content*, Harvard U. Press. [43]

Wikipedia (2022), *Civil and political rights*, https://en.wikipedia.org/wiki/Civil_and_political_rights (accessed on 17 August 2022). [130]

Wilson, D. (2018), "Algorithmic patrol: The futures of predictive policing", in Završnik, A. (ed.), *Big Data, Crime and Social Control*, Routledge, https://www.taylorfrancis.com/chapters/edit/10.4324/9781315395784-6/algorithmic-patrol-dean-wilson. [123]

Women in Parliaments Global Forum (2016), *Social Media: Advancing Women in Politics?*, https://www.womenpoliticalleaders.org/wp-content/uploads/2016/10/WIP-Harvard-Facebook-Study_Oct2016.pdf. [53]

Yarchi, M., C. Baden and N. Kligler-Vilenchik (2020), "Political Polarization on the Digital Sphere: A Cross-platform, Over-time Analysis of Interactional, Positional, and Affective Polarization on Social Media", *Political Communication*, Vol. 38/1-2, pp. 98-139, https://doi.org/10.1080/10584609.2020.1785067. [51]

Notes

[1] Civil and political rights are a class of rights that protect individuals' freedom from infringement by governments, private actors, and social organisations. They ensure one's entitlement to participate in the civil and political life of society and the state without discrimination or repression, and, as such, are the foundations of democracy. Unlike other rights concepts, such as human rights and natural rights, in which people acquire rights inherently, civil and political rights must be given and guaranteed by the power of the state. Civil rights include the ensuring of peoples' physical and mental integrity, life, and safety; protection from discrimination on grounds such as sex, race, sexual orientation, national origin, colour, age, political affiliation, ethnicity, social class, religion, and disability; and individual rights such as privacy and the freedom of thought, speech, religion, press, assembly, and movement. Political rights include procedural fairness in law, such as the rights of the accused, including the right to a fair trial; due process; the right to seek redress or a legal remedy; and rights of participation in civil society and politics, such as freedom of association, the right to assemble, the right to petition, the right of self-defence, and the right to vote. Civil and political rights form the original and main part of international human rights of the 1948 Universal Declaration of Human Rights and the 1966 International Covenant on Civil and Political Rights. Sources: (Wikipedia, 2022[130]) and (Sieghart, 1985[129]).

[2] https://e-estonia.com/solutions/e-governance/e-democracy/

[3] https://rk2019.valimised.ee/en/voting-result/voting-result-main.html

[4] A cyber threat is a threat actor, using the internet, who takes advantage of a known vulnerability in a product for the purposes of exploiting a network and the information the network carries.

[5] Malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of malware include computer viruses, worms, Trojans, spyware, and adware.

[6] https://cyber.gc.ca/en/guidance/cyber-threats-elections#defn-malware

[7] Democracy theory often refers to the key concept of "loyal opposition" as a foundation for liberal democracy based on the principles of political competition and of reasonable disagreement in democratic settings. It refers to the behaviour of the political opposition and minority parties whose opposition to the party in power is constructive, responsible, and bounded by loyalty to fundamental interests and principles of democracy enshrined in the constitution (Waldron, 2016[131]).

[8] https://v-dem.net/data_analysis/VariableGraph/

[9] Similarly, nearly all participants in a British programme for aspiring women leaders noted that they had witnessed sexist abuse of female politicians online. UNGA, 2018, https://www.un.org/en/ga/search/view_doc.asp?symbol=A/73/301

[10] https://petition.parliament.uk/

[11] See, for instance, https://participa.gov.pt/base/home and https://participa.pt/. Portugal also developed Consulta LEX, a platform for public consultations on legislation and the formulation of suggestions (https://www.consultalex.gov.pt/).

[12] On public interest technology, see the special issue of the Stanford Social Innovation Review on *Putting the Public Interest in Front of Technology* available here: https://ssir.org/putting_the_public_interest_in_front_of_technology and (McGuinness and Schank, 2021[128]).

[13] https://bogota.gov.co/yo-participo

[14] https://decidim.org/es/usedby/

[15] https://www.coe.int/en/web/education/competences-for-democratic-culture

[16] https://scvo.scot/p/36175/2020/03/19/no-one-left-behind-digital-scotland-covid-19

[17] https://digitalparticipation.scot/charter

[18] https://www.cncs.gov.pt/pt/cursos-e-learning/

[19] https://www.integritywatch.eu/

[20] These include for instance the Open Government Partnership, the Open Contracting Initiative, the Infrastructure Transparency Initiative, the International Budget Partnership, the Global Initiative on Fiscal Transparency or the Extractive Industries Transparency Initiative.

[21] https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation/about

[22] Scandals such as those related to the benefits fraud algorithms in the Netherlands and the exam grading algorithms in the United Kingdom, have heightened public interest about the use of algorithms in public decision-making and the importance of increasing transparency and accountability in government algorithms. In the Netherlands, the *System Risk Indication*, a risk-profiling system designed by the Ministry of Social Affairs to process large amounts of data collected by various public authorities to identify those most likely to commit benefits fraud, was declared illegal by the District Court of the Hague in 2020. The Court argued that that right to privacy prevails over fight against alleged benefits fraud.

[23] www.ai.gov

[24] https://data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/

[25] https://www.gov.uk/service-manual

[26] In other sphere related to the digital transition, different approaches are being taken. For example, in Europe, privacy legislation is enforced by public authorities, while in the United States enforcement falls mainly to the private sector and self-regulation.

[27] 15 out of 38 OECD countries have a converged communication and broadcasting regulator.

[28] OECD survey carried out in 2021 by the WPCISP. Percentages refer to OECD countries, Brazil and Singapore as reported in the forthcoming report “Communication Regulators of the Future” (OECD, forthcoming[115]).

[29] Formed in 2020, the DRFC comprises the Competition and Markets Authority (CMA), the Information Commissioner's Office (ICO), the communications regulator (Ofcom) and the Financial Conduct Authority (FCA).

[30] The Dutch Digital Regulation Co-operation Platform was formed in 2021, comprises the Netherlands Authority for Consumers and Markets (ACM), the Dutch Data Protection Authority (AP), the Dutch Authority for Financial Markets (AFM) and the Dutch Media Authority (CvdM).

[31] The Italian Telecommunications Authority, the Competition Authority and the Data Protection Authority published 'Guidelines and policy recommendations for Big Data' (see https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9123073).

[32] https://www.auditingalgorithms.net/

[33] https://www.gao.gov/products/gao-21-519sp

[34] https://www.rekenkamer.nl/onderwerpen/algoritmes/algoritmes-toetsingskader/

[35] See https://rm.coe.int/fin-the-report-of-the-non-discrimination-ombudsman-to-the-parliament/16808b7cd2 and https://www.yvtltk.fi/material/attachments/ytaltk/tapausselosteet/45LI2c6dD/YVTltk-tapausseloste-_21.3.2018-luotto-moniperusteinen_syrjinta-S-en_2.pdf

[36] See for instance: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

[37] https://www.state.gov/summit-for-democracy/

[38] On "digital authoritarianism," see for example https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

[39] https://techfordemocracy.dk/watch-now/

[40] https://www.gpai.ai/

[41] https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/joint-statement-by-the-ministry-for-europe-and-foreign-affairs-and-the-state

[42] https://oecd.ai/en/ai-principles and an in-depth case study in https://oecd-opsi.org/wp-content/uploads/2019/11/AI-Report-Online.pdf

[43] https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1

[44] https://en.unesco.org/artificial-intelligence/ethics#drafttext