THE DIGITALIZATION OF DEMOCRACY

HOW TECHNOLOGY IS CHANGING GOVERNMENT ACCOUNTABILITY

// KRZYSZTOF IZDEBSKI / TEONA TURASHVILI / HAYKUHI HARUTYUNYAN / ED. BETH KERLEY

NED NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

FORUM INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES

// REPORT / MARCH 2023

THE DIGITALIZATION OF DEMOCRACY

HOW TECHNOLOGY IS CHANGING GOVERNMENT ACCOUNTABILITY

CONTENTS

NED NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

FORUM INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES

EDITOR'S OVERVIEW

In a world where digital tools have come to mediate much of social and political life, navigating technological change will be key to sustaining democracy for the future. The business of governing is undergoing dramatic changes amid rapid advances in computing power, breakthroughs in fields such as artificial intelligence (AI), and the spread of digital products to new markets and settings. Public officials around the world rely on digital technologies to make governance faster, smarter, and more efficient. But what do these changes mean for citizens seeking to hold their governments accountable?

For government by the people to be a reality, **citizens must be able to monitor and assess those who govern**—whether this entails watching out for corruption, holding politicians to their promises, or working to ensure the impartiality of justice. As democratic states go digital, **these tasks increasingly involve both monitoring and leveraging innovative technologies such as AI.**

TECHNOLOGY IS TRANSFORMING GOVERNMENT ACCOUNTABILITY

The digitalization of democratic states involves more than just making analog information available in digital formats. Algorithmic tools, including complex, often difficult-to-explain AI systems, are becoming an ever more appealing option for officials looking to analyze trends, categorize people, and make decisions. Digital systems might be assigning judges to court cases; allocating social benefits; or identifying criminal suspects. Whether they rely on cutting edge machine-learning (AI/ML) models, or pre-set rules coded in by humans, digital tools are working at the core of governance.

These circumstances make it possible for watchdogs to take a **more systemic approach to monitoring for abuses.** Volumes of digital data on government officials, resources, and practices now exist. So, too, do new analytical tools for making sense of this information. Yet accountability institutions both within and outside of government also confront a new task: **how to ensure that not only public officials, but also the technologies on which they rely comply with transparency and human-rights norms.**

The following essays offer insights on the diverse ways the digital transformation of the public sector is changing government accountability. Drawing on their experiences advocating for open government in Poland, Georgia, and Armenia, our contributors outline a multifaceted transformation that will require **new capacities, concepts, and collaborations** to ensure that the accountability toolkit stays up-to-date. Their work highlights several key themes:

- **Responsible digitalization can be a path to enhanced accountability:** Where watchdog institutions must process great volumes of information with limited human resources, Haykuhi Harutyunyan notes, new digital platforms are a way to turn open government data from a "box-checking exercise" into a meaningful tool for accountability. AI/ML systems—increasingly popular for combatting illicit financial flows—hold particular promise for helping oversight institutions to stay "one step ahead of officials looking to conceal their conflicts of interest or ill-gotten gains." Officials looking to responsibly leverage these and other data-driven technologies must navigate trade-offs between the benefits of accessible information and various digital risks.
- **Developers should consider both technological and human risks:** Data-driven digital technologies introduce particular hazards to democracy: such tools can erode privacy in unprecedented ways or encode social inequalities in new algorithmic models. Yet other tech-associated risks ultimately stem from the persistent threat of human misconduct, for instance when officials hide behind digital systems to dodge responsibility for their actions. The abuse of "health code" apps in the People's Republic of China marks one particularly egregious instance of this practice—but democratic settings are not immune. As Krzysztof Izdebski observes, digital tools in the hands of corrupt or repressive officials are no guarantee of fair governance: "In the absence of trust in governing institutions, there can be no trust in the tools they deploy."
- **Government institutions are struggling to keep pace with digital change:** When researching technologies in government, accountability advocates have found that public officials themselves often have limited knowledge of the digital systems they use. As Teona Turashvili shows, this challenge is particularly acute in newer fields such as AI, where there is frequently a "void when it comes to defining working principles, ethical norms, and even basic concepts." Closing these conceptual gaps will be a significant step toward holding governments accountable for the ways in which they are deploying AI tools.
- **Collaboration across sectors is critical:** Collaboration among institutions in government, civil society, and the private sector will be crucial to closing knowledge gaps, building accountable systems, and upgrading oversight for the age of AI. While models for such engagement already exist, these kinds of practices will need to be brought to a greater scale to match the scope of the digital accountability challenge. Like governments, civil society organizations face the challenge of upgrading their capacities to engage in greater depth on fast-evolving and complex digital governance issues.

To be prepared for the digital advances that are likely in the coming years, democracies need strategies and mechanisms to begin addressing these challenges today. Cross-sectoral collaboration will be vital to explore how societies can fully leverage the prodemocratic potential of tools like AI, while also developing approaches to tech procurement, design, and deployment that will ensure democratic principles are baked into new digital products. By starting conversations across sectors about accountable government in the digital age, democracies can identify promising models for both ensuring accountability in the use of technology and leveraging technology in service of accountability.

THE DIGITAL BATTLEFIELD FOR DEMOCRATIC PRINCIPLES

// **KRZYSZTOF IZDEBSKI,** CO-LEAD OF THE OPEN SPENDING EU COALITION AND LEGAL AND POLICY OFFICER AT THE STEFAN BATORY FOUNDATION

EXECUTIVE SUMMARY

From law enforcement and the courts to voting systems and social services, new digital tools that collect and process data are changing how governments operate. The implementation of these technologies takes forms ranging from China's regular use of artificial intelligence (AI) tools to assess citizens' "fitness" for society to democracies' introduction of algorithmic systems that allocate social benefits, support school enrollment, assign judges to cases, or sustain dialogue with citizens.[1]

While many digital tools hold promise as instruments for open government, their adoption also presents new challenges to democratic principles of transparency, equality, and privacy. Moreover, public sector institutions are often woefully unprepared to address these issues due to knowledge gaps as well as a tendency to dismiss digital risks as a question solely for specialists. Over the coming years, digital risks in the public sector will have a growing impact on the work of civil society groups already struggling amid democratic backsliding and waning public trust. To defend democratic principles on the new digital battlefield, **civil society must take on a more active role in the governance of public-sector technologies themselves**—whether by educating policy makers and the public about foundational issues, advocating around specific human rights concerns, or helping to craft policy reforms to bolster transparency and accountability.

THOSE WHO RULE THE CODE, RULE THE PEOPLE

With AI–powered systems growing more accessible worldwide, AI together with a wider set of **automated decision-making (ADM) tools** are among the many technologies becoming an integral part of the citizen-government relationship. In a moment where the path from democracy to authoritarianism is proving very short,[2] developing the right mechanisms to govern the introduction and use of these systems will be vital to democratic health.

For democratic governance to be effective, the public must be able to hold state institutions accountable. Where trust in institutions is low and corruption widespread, watchdogs may view new digital tools meant to automate or supercharge governance processes as a promising solution (see forthcoming essay by Haykuhi Harutyunyan). Such systems might be designed to support officials in the delivery of public services, increase civic engagement, or strengthen public security. Monitoring and decision-making tools that harness digital data in new ways can help realize citizens' right to good governance.[3]

Where trust in institutions is low and corruption widespread, watchdogs may view new digital tools meant to automate or supercharge governance processes as a promising solution.

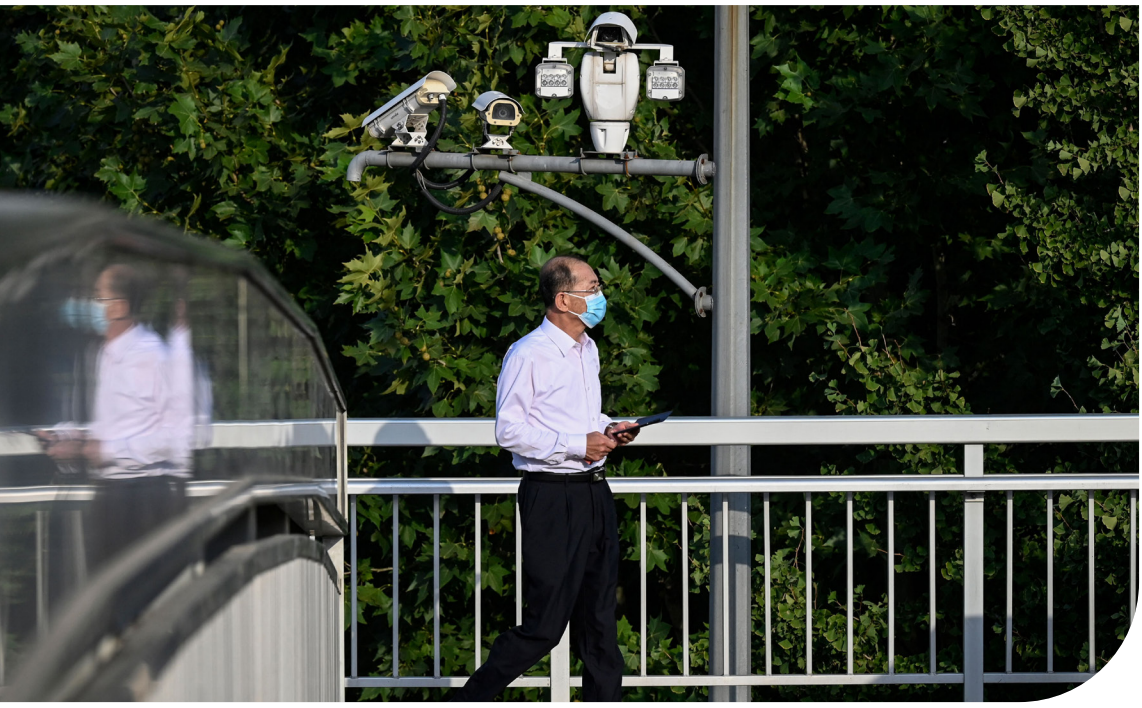
Yet like other imperfect products of human labor, digital tools in the public sector carry risks. These hazards may be present with any technology, no matter how simple, that directly or indirectly impacts democratic processes or citizens' rights and obligations. The uptake of AI and other ADMs, however, is expanding the scope of this challenge. Whether through opaque decision-making processes that blur lines of official responsibility, discriminatory impacts of algorithmic tools (as we have seen across a range of established democracies),[4] or abuses of new surveillance powers (as with NSO Group's Pegasus spyware),[5] **poorly overseen digitalization may further erode political accountability where it is already under threat.**

With publics across the globe concerned that "[the] use of technology will mostly weaken core aspects of democracy and democratic representation in the next decade,"[6] **addressing these risks is essential to maintaining trusted and trustworthy democracies.** This challenge is particularly urgent because, as research from a set of Central and East European countries shows, the adoption of new digital tools in backsliding democracies can create a veneer of objectivity that obscures real risks to democratic integrity.

THE CHALLENGE OF RESPONSIBLE DIGITALIZATION

Closed autocracies such as China, Russia, and Saudi Arabia offer ample illustrations of the many ways in which states can abuse digital tools—particularly surveillance technologies—to act on their repressive inclinations.[7] In such settings, many experts see governments themselves as the greatest source of "digital threats to civil society."[8] Conversely, citizens in democracies can, in theory, leverage accountability mechanisms—such as judicial review—to guard against government abuses of technology as well as unintentional digital harms. Yet numerous obstacles currently impede efforts to make this vision a reality. **In this context, citizens in democracies also have understandable concerns about how politicians may leverage new opportunities to automate governance processes, customize them, and expand their reach.**

Despite their wide-ranging impacts, new digital tools are still too often dismissed in many settings as something purely "technical" without considering the implications for democratic principles. Among the people and institutions responsible for ensuring good governance, education on the risks these tools pose and procedures for addressing them are frequently lacking (see forthcoming essay by Teona Turashvili). As technologies increasingly perform critical tasks on the state's behalf, **societies urgently need to understand how they can make sure the same standards of transparency and accountability that exist for traditional public authorities are also applied to digital systems.**[9] This principle was well articulated by a Polish court,[10] which held that an algorithm assigning judges to court cases should be treated as an "expression" of an official procedure (and therefore considered public information).



A man walking past closed circuit television (CCTV) surveillance cameras on an overpass in Beijing.

Digital technologies' impact on societies will depend on more than just the intentions of the officials who use them. As a 2021 United Nations Human Rights Council report explains, "technologies, not just their users, affect human rights because they influence policymaking and can restrict individual liberties."[11] Thus, even before agencies launch a new digital system, making the right design choices is critical. So, too, is having **adequate procurement and oversight procedures** in place. When agencies decide on deploying new Information Technology (IT) systems that affect the government-citizen relationship, they need to consider not only cost-effectiveness, but also compliance with rule-of-law principles.

This challenge is global, although local context (such as groups facing discrimination), legal context (for example, privacy protections or lack thereof), and political context (official corruption or other factors) shape the risk dynamics and response required in any given case. Meeting the moment will require deepening understanding of the risks digital governance tools may pose to democracy; shoring up what are still often flimsy procedures for assessing these risks; and facilitating participation by citizens as well as civil society organizations in creating and controlling new digital systems.

Decision-making tools introduced in the name of making governance more objective can enable authorities to obscure or deflect responsibility for their actions instead.

UNDERSTANDING THE RISKS

Monitoring the procurement and use of advanced digital tools in the public sector may seem like an arcane topic for technical specialists.[12] Nonetheless, these issues intersect with broader conversations about democratic accountability. While the list of challenges is long and constantly evolving, three critical concerns involve the ways in which technology can lend a veneer of ***false objectivity*** to flawed governance processes; actively introduce new governance failures through ***discriminatory impacts***; and undermine the conditions for free association and activism through both overt and surreptitious ***erosions of citizens' privacy***.

False Objectivity

Where mechanisms to ensure the transparency of digital systems are lacking, decision-making tools introduced in the name of making governance more objective can **enable authorities to obscure or deflect responsibility for their actions** instead.[13] A good example is the aforementioned case assignment system used for Polish judges.[14] In theory, the use of automatic, random tools to select judges should—as Polish authorities promised—help to ensure a fair trial. Yet this change must be considered in its political context: It was introduced in tandem with reforms that threatened judicial independence by ceding more control over the courts to politicians. Against this backdrop, it was particularly concerning that the algorithm to select judges, produced and maintained by the Ministry of Justice, was introduced without any consultation and kept secret.

Once the new system came into operation, work was assigned unevenly, with preference given to judges in positions filled directly or indirectly by the Minister of Justice.[15] Judges could not even see why the algorithm allocated more cases to them than to others. Though independent audits conducted in the courts revealed numerous issues, the Ministry still resisted disclosing the algorithm on the grounds that it was not public information. It was only as a result of a media attention to the problems with the system's functioning and legal action by a nongovernmental organization (NGO)—with which I was professionally involved at the time—that the Ministry took action to resolve the situation. After winning a freedom of information case, we managed to get access to the algorithm, while another NGO won a later case seeking access to the source code.[16] The latter has not yet been released; its analysis will show whether the system was indeed randomized.

In the absence of trust in governing institutions, there can be no trust in the tools they deploy.

Similar doubts have been raised about the Automated Court Case Management Information System operating since 2010 in North Macedonia.[17] A 2017 audit conducted after a number of scandals showed that state authorities had manipulated the system: In hundreds of cases important to the government, authorities hand-picked judges under the guise of a computer draw. Meanwhile in Czechia, auditors identified irregularities in an algorithm used in the 2013 presidential election to select a sample of endorsement signatures for verification. Ultimately, a court found that this issue did not affect the election results, but did create a risk of the unauthorized elimination of some candidates.[18]

These cases underscore that in the absence of trust in governing institutions, there can be no trust in the tools they deploy. **Where corruption is widespread or independent scrutiny of politicians' actions is weak, digitalization is not a silver bullet that will guarantee fair governance.** Instead, digital tools must themselves be embedded in robust transparency and accountability mechanisms in order to earn and warrant public trust. Whatever theoretical merits any digital system may possess, constant and independent scrutiny of its operation is crucial.

Discriminatory Impacts

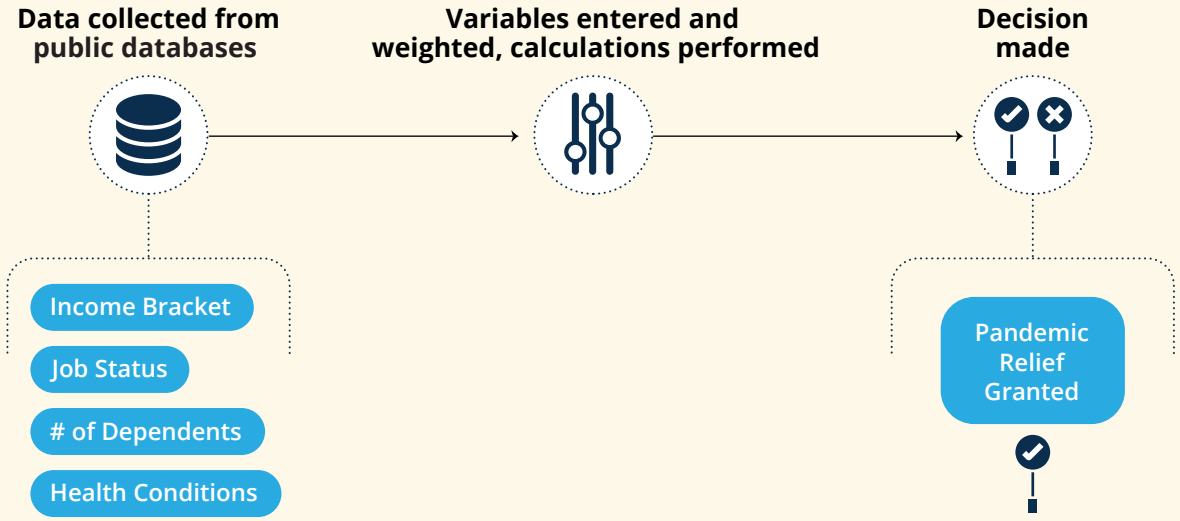
While the examples above involve digital tools serving as smokescreens for human malfeasance, accountability for harms caused by algorithmic systems themselves is also a major concern. When governments employ data-driven tools to automate decision making, discrimination against marginalized groups can occur. In order to make a decision on whether, for instance, to grant social benefits or check the accuracy of tax payments, these tools rely on data about an individual's wealth and finances, family situation, education level, or health conditions, among other variables.

In a nutshell, an algorithmic system takes these data points—whether collected specifically for this purpose, or taken from other public databases—assigns certain values to each attribute, and makes a decision based on these inputs.

FIGURE

Example of data-driven automated decision making tool

Automated decision making tools use data inputs from government databases and other sources, weighted and combined in a manner determined by their algorithm, to answer questions such as who is eligible for social benefits or how government resources should be allocated.



Tools that perform these calculations may be either complex machine learning (AI/ML) systems whose assessment criteria evolve as they identify patterns in datasets, or simpler algorithmic tools that operate according to fixed criteria. Reliance on such technologies creates opportunities for mistreatment of citizens on the basis of their personal information—even when officials do not consciously intend to discriminate.

The data held by public officials commonly reflects historical conditions or preexisting prejudices in a country. Many of the risks that result are predictable: If an algorithmic system were to describe the "ideal" student, it would most likely be a male from a privileged part of society, as this subset of the population has been eligible to study for longer than other groups. If the police have scrutinized ethnic, racial, or religious minorities disproportionately, algorithms will suggest that people in these categories are more likely to commit crimes. (For this reason, bans on predictive policing techniques have been proposed as part of the EU's draft AI Act.)[19] An algorithm used by the Austrian Public Employment Service to predict job-seekers' chances of finding employment assigned women lower scores than men, with all other characteristics held equal.[20] There are also less obvious examples of algorithmic discrimination, with place of residence being a particularly risky category of data profiling. Residents who might live in neighborhoods with high crime rates and low levels of tax payment might, for instance, face extra scrutiny when interacting with government agencies.[21]

Discrimination undermines one of the guiding principles of democracy: the equality of all citizens among one another and before the law. In many countries, equality is even a constitutional principle, and state authorities have an obligation to take action against discriminatory practices. By definition, **democracy requires "a kind of equality among the participants at an essential stage of the decision-making process."**[22] When collective decision-making is undertaken by a computer system that can amplify inequalities, democracy is compromised. Thus, democratic authorities have a duty to balance the potential benefits of new technologies with the risks of exclusion and discrimination that follow from their use.

When collective decision-making is undertaken by a computer system that can amplify inequalities, democracy is compromised.

Privacy Risks

Finally, the privacy impacts of new capacities for data collection and processing can degrade citizens' ability to hold their government accountable for their practices writ large. As Carissa Véliz from the University of Oxford has rightly noted, "the power that privacy grants us collectively as citizens is necessary for democracy—for us to vote according to our beliefs and without undue pressure, for us to protest anonymously without fear of repercussions, to have freedom to associate, speak our minds, read what we are curious about."[23] Anonymity and the ability to hide from the watchful eye of state security services used to be the protective shield of democratic movements. Without careful deliberation, **the shift toward digital governance tools could imperil this critical safeguard for civic engagement, skewing the balance of power in favor of state authorities**.

On this front, the most obvious threat comes from AI and other cutting-edge surveillance tools. These surveillance capabilities have been used in Belarus and Russia to quickly identify and repress peaceful protesters.[24] More broadly, new forms of surveillance can create an environment in which the authorities can easily determine where and with whom citizens are at any given time, even when they do nothing wrong. But the challenge is broader than just surveillance by public-security agencies. The collection of data for automated decision-making tools of the kind described in the previous section, for instance, may also undermine privacy protections in the absence of a thoughtful approach to data retention, access, and security.

Digital tools theoretically intended to empower the public may exacerbate privacy risks. For example, citizens may contribute to the government's centralized surveillance apparatus through crowdsourcing platforms that collect photos and videos of badly parked cars and traffic offenses, dangerous behavior, and so forth—and in so doing, construct a societal panopticon.[25] Furthermore, privacy risks associated with internet voting (i-voting) systems (used in local elections or for projects submitted in participatory budgeting) could lead citizens to abstain from voting or to vote in a way that does not reflect their true preferences.[26]

European Executive Vice-President Margrethe Vestager (L) and European Commissioner in charge of internal market Thierry Breton (R) hold a press conference on artificial intelligence following the weekly meeting of the EU Commission in Brussels on April 21, 2021.

A Regulatory Solution?

The European Union's AI Act—still under negotiation in the European Parliament as of this writing in March 2023—represents a significant attempt to grapple with many of the aforementioned democracy and human rights challenges. This legislation, which may set a global precedent, takes a comprehensive approach to addressing the risks that AI technologies present when used in certain contexts. It bans the deployment of certain technologies (such as real-time remote biometric identification systems in publicly accessible spaces) or classifies them as "high-risk." In other cases, it confers this "high-risk" designation on certain AI applications within the judicial system—for instance, when AI tools are used "to interpret the facts or the law and to apply the law to a concrete set of facts." The Act also requires that information on "high-risk" uses be included in a public database maintained by the EU and stipulates that control over these systems must be exercised by a person tasked with this responsibility.[27]

While this type of regulation should be supported, it will not on its own provide a sufficient answer to digital risks in the public sector. First, it should be noted that individual state governments will be primarily responsible for the Act's enforcement. Thus, rule of law, checks and balances, and capacity to address technology issues at the national level will still be of paramount importance. Moreover, **AI represents only one subset of the technologies that may impact citizens' rights and states' democratic processes when deployed by officials. Risks can also arise in connection with simpler ICT solutions that do not meet the technical definition of AI**—such as the Polish judicial assignment algorithm discussed above.

MISSING THE FULL PICTURE

To ensure accountable governance for the digital age, new processes and tools for performing public tasks should be assessed meticulously for their impact on citizens' rights as well as government effectiveness and efficiency.[28] As an essential component of the government-citizen relationship, these tools must meet open government standards that include upholding transparency, protecting privacy, guarding against discriminatory impacts, and establishing accountability mechanisms.

Public sector digital tools must meet open government standards that include ensuring transparency and privacy protections, guarding against discriminatory impacts, and establishing accountability mechanisms.

At present, however, few entities or officials reflect upon the risks that ADMs and other, new digital governance systems might pose. Alongside weak internal procedures, a dearth of relevant knowledge and experience among officials is major problem in this regard. In the United Kingdom, research has found that "too many senior government leaders are not equipped with the knowledge and know-how required to make good decisions and lead digital business change."[29] The problem is even greater in low- and middle-income countries.[30]

In the "algOVrithms: The State of Play" studies in 2019, 2021, and 2023, a group of NGO researchers identified **low levels of official knowledge about digital systems** as a challenge across eight Central and East European countries (representing a range of income levels).[31] An audit conducted by the Polish Supreme Chamber of Control on the system for allocating judges found that "the direct users of the tool were not well versed in how it works, as the training needs of the users of the system were not properly identified, and . . . much of the training was not carried out until a year and a half after the implementation of the system."[32] Our *algOVrithms 2.0* study highlighted similar concerns with regard to officials using ADMs in North Macedonia: "Delegated responsibility, with minimal knowledge of the subject—and resorting to establishing subcontractors (private companies) as a point of information, but also a potential point of responsibility, is a dangerous exercise in good governance."[33]

The implications of such knowledge gaps are evident when digital tools fail and officials do not have answers to questions from concerned citizens—or are themselves slow to see the problem. For instance, when errors were identified in a system designed to allocate nursery places in Wrocław, parents contacting local authorities were referred back to the company that had originally developed the system.[34]

As technology's role in governance expands, officials will need to receive ongoing education and training that go beyond specifics of individual tools and basic questions that may come from residents. **Public officials should know, for example, what data is being used, whether problems have previously been reported, and, if so, what these errors entailed.** Training courses should cover principles of open e-government, sensitizing officials to the impact of technology on the state-citizen relationship and to possible human rights risks.

TAMING TECHNOLOGY

Beyond improving officials' digital skillset, democracies should continuously reflect on how good governance practices might fruitfully be applied to digital tools that take on governance functions. For instance, it is good practice, and in many countries an obligation, to prepare a regulatory impact assessment before presenting a draft of new legislation. Among other functions, these assessments identify potentially affected groups or individuals, examine the regulation's budget implications, judge the feasibility of implementing alternative solutions (e.g., changing the practices of officials), outline how similar solutions work in other countries, and determine indicators to assess whether the regulation in question is serving its stated purpose.

Algorithmic or, more broadly, technology impact assessments, are a promising innovation that operate on the same principle.[35] These evaluations are already a required step in Canada[36] and New Zealand,[37] among other jurisdictions; officials elsewhere conduct them on a voluntary basis.[38] Through such mechanisms, it is possible to predict before a new digital system is implemented whether the risks presented by its use of outweigh the potential benefits. The practical implementation of algorithmic impact assessments in any given setting, of course, is what determines whether they will actually protect citizens, or simply lend a façade of legitimacy to official decisions.

Before even getting into technical details, agencies should also be sure to **ask whether new digital tools are necessary to achieve their desired policy goals.** If the goal of implementing a digital communications platform is to encourage public participation in civic deliberation, for instance, officials should consider whether such engagement was lacking due to technical obstacles, or instead because officials were too late in informing the public about such political discussions or ignored the voices of those who took part.

CIVIL SOCIETY'S ROLE

While robust government processes are necessary to create an environment of accountability around the use of digital tools, a thoughtful and meaningful response to digital risks ultimately depends on civil society engagement. Civil society organizations can **draw public attention to the dangers** that might stem from authorities' abuse of new technologies and the unintended consequences of design or deployment choices. They can also lobby public authorities to **create a legal environment that ensures maximal transparency** around digital governance tools, so that any interested citizen can gain an understanding of how the technology works. Finally, they should **work alongside governments in co-creating new digital tools**, as well as in assessing their impact on individuals and societies. Civil society's participation in these areas, among others, could be strengthened by the establishment of national digital-rights ombudsmen, which would simplify the task of finding the right interlocutors in government.

A thoughtful and meaningful response to digital risks ultimately depends on civil society engagement.

Procurement as Opportunity

Opacity, discriminatory impacts, and privacy risks are common challenges created by many digital applications, from social media to software used in hiring. When public-sector entities are the ones acquiring new digital systems, however, **public procurement processes present a unique opportunity for democratic institutions to address these risks.**[39] In this context, the contracting authority (such as a particular government department) has considerable leeway in defining the terms of the bid and the execution of the contract. Consequently, it can **oblige the provider to be more transparent**, for example, by making the technical details in the source code available to independent experts who can inspect its performance periodically. Contracting authorities can even make this information publicly available, enabling anyone who wishes to check the system's operation to do so. Wayne Lonstein from the Forbes Technology Council has gone so far as to argue that in the public sector, "[A]ny agreement with a technology vendor that contains anything but full transparency should be deemed illegal."[40] The contracting authority should also **specify what data can be used by the system**, taking into account the need to ensure representativeness, protect privacy, and clearly identify those responsible for the system's accuracy. In addition, public institutions can set a positive precedent by ensuring that the teams working on and later evaluating the tool **reflect broader, social diversity** in order to avoid having the prejudices of privileged groups built into the system.

A range of interesting precedents for this kind of engagement have already emerged. In Poland, for instance, a multi-stakeholder working group exists to discuss implementation of legislation regulating AI (including in the public sector).[41] The Code for All Network has pioneered fruitful approaches to collaboration with representatives of public institutions.[42] For many years, Code for Pakistan has successfully organized internship programs, with a focus on engaging women, through which activists help officials to implement human-centric digital transformation.[43] Finally, at the international level, the action coalitions of businesses, government representatives, and non-profits centered around the Tech for Democracy initiative are a noteworthy multistakeholder effort with potentially significant implications.[44]

To build on these initiatives and match the scope of the digital accountability challenge, a systematic approach to expanding civil society capacity is needed. The authors of the *algOVrithms 3.0* report, for instance, call for

"systemic activities for increasing the competence of representatives of NGOs, journalists and academics in identifying specific risks arising from the operation of automatic decision-making systems." For civil society organizations to defend digital rights effectively, they need to be adequately funded. It is worth noting, for example, the European Artificial Intelligence & Society Fund,[45] an initiative that allocates resources to build the digital competencies of organizations that until recently focused exclusively on "analogue" problems of discrimination or support for excluded groups. The Digital Freedom Fund,[46] on the other hand, seeks to support organizations in strategic litigation in the area of digital rights and to combine the competencies of technologists and human rights defenders.[47]

Amid flagging confidence in democratic systems, digital tools that serve as novel manifestations of the state require constant scrutiny. Setting technology outside the domain of public-sector oversight and accountability mechanisms will only weaken public trust and worsen democratic backsliding. If technologies have become part of democracy, democratic principles such as diversity, transparency, and participatory decision making must be reflected in their implementation and control.

Setting technology outside the domain of public-sector oversight and accountability mechanisms will only weaken public trust and worsen democratic backsliding.

ASSESSING THE ACCOUNTABILITY OF AI SYSTEMS IN GEORGIA

// **TEONA TURASHVILI,** HEAD OF LOCAL GOVERNMENT & INTERNET AND INNOVATIONS DIRECTIONS AT THE INSTITUTE FOR DEVELOPMENT OF FREEDOM OF INFORMATION (IDFI)

In younger democracies such as Georgia that still struggle to fortify the rule of law, the risks that artificial intelligence (AI) and other emerging technologies pose in the public sector are particularly acute. Where officials confront entrenched corruption and cumbersome systems of public administration, advanced digital tools hold out an appealing promise to improve service delivery, modernize the public sector, and make it easier to do business.

Yet these same applications can endanger democratic principles—especially if state accountability is already tenuous due to shortcomings in judicial independence, government transparency, or law-enforcement oversight mechanisms. **Free expression, non-discrimination, and the right to privacy are among the many democratic norms potentially at stake.**

In Georgia, much remains to be done in terms of establishing the institutional and informational structures needed for public agencies to guard against these risks. My organization, the Institute for Development of Freedom of Information (IDFI), has conducted research on **AI use in Georgia's public sector**. Our experience serves as a case study on the obstacles that exist across many settings to holding governments accountable in their deployment of AI tools.[1]

Our report identified only a few cases of AI usage within these agencies, possibly in part because officials either do not know or do not wish to share information about the systems they use. Nonetheless, such tools are rapidly growing more popular and

accessible. In this context, our research experience reveals some key gaps that Georgia and other developing democracies should address to **ensure political transparency, enable civil society engagement,** and **facilitate thoughtful, open, and inclusive deliberation around AI systems** as they are adopted—rather than waiting until unforeseen digital risks undercut citizens' rights.

USES OF AI IN THE GEORGIAN GOVERNMENT

Since Georgia's Rose Revolution in 2003, when peaceful protests led to post-Soviet president Eduard Shevardnadze's resignation and the election of a new government with an ambitious anticorruption agenda, the country has implemented numerous good governance reforms. E-government initiatives, in particular, became popular starting in 2009. These innovations modernized the public sector significantly, with notable improvements in public service delivery, public procurement, public finance, and the transparency and accountability of public institutions. Still, a number of serious challenges to the rule of law remain. It is against this backdrop that IDFI decided to examine **the extent to which public agencies were utilizing AI,** as well as **what measures the officials implementing these systems had taken to protect democratic principles** such as transparency and accountability.

Our study identified five government institutions that have been using AI-enabled digital systems.[2] In some cases, these were isolated applications—for instance, to analyze and visualize education-management data or to conduct an AI-powered analysis of social media posts by visitors to Georgia. The Ministry of Internal Affairs' systems, however, stood out for their relative complexity. Most important, this ministry used **facial recognition systems** for investigative purposes and to carry out criminal and administrative proceedings.[3] Recently, media outlets reported that the Ministry also employed other AI systems, including ballistics and fingerprint recognition programs of Russian and Belarusian origin.[4] The recent revelation that these systems were in use—something that was not not disclosed to IDFI during our research—underscores the possibility that other agencies may similarly be deploying AI systems of which we remain unaware.

Guarding against the abuse or misuse of AI tools is particularly critical in the public-security context, especially since Georgia's law enforcement agencies are criticized frequently for their opaque practices. As with other countries in the region, civilian oversight and control mechanisms for these agencies are weak, and Georgian politics in recent years has been shaken by reports of large-scale, politically motivated surveillance. Moreover, the Russian origin of certain applications raised concerns that they could make the country more vulnerable to Russian cyberattacks. (Following critical reporting on the two systems mentioned above as well as Russian facial recognition software, the Ministry of Internal Affairs claimed that some of these programs were actually developed in Turkey and that they are connected only to the Ministry's internal network.)[5]

Guarding against the abuse or misuse of AI tools is particularly critical in the public-security context.

OBSTACLES TO TRANSPARENCY

Our ability to assess whether AI systems were being used responsibly in Georgia's public sector was limited. While conducting our study, we found that **detailed information about this topic was difficult to retrieve**. The institutions that provided information on their AI use supplied only general details. In most cases, they did not share additional relevant documentation such as user instructions or technical manuals, legal or normative acts governing the use of the software, ethical standards, or personal data protection safeguards. The responses we received left us with the sense that Georgian public institutions **do not regularly conduct external audits** to vet the proper functioning of their AI tools.

Gaps in AI governance also make collecting reliable information more challenging. In Georgia, as in most other settings, there is no common registry with information about AI systems in use by public agencies. Although few examples of such registries currently exist globally,[6] their adoption will be critical for accountable governance as public institutions begin to rely on AI tools more heavily. To uphold democratic principles in the use of technologies that are transforming governance, **stakeholders need a clear understanding of which AI systems are being used by government institutions, and for what purposes.**

Another challenge is that Georgian official institutions seem to lack a clear definition of AI, including on the legislative level. Absent such guidance, it is difficult for officials to distinguish between AI and other types of software with high levels of automation. This situation has provided institutions with a ready pretext to avoid answering our request for public information about their use of AI tools. Defining AI more clearly is an important precondition for understanding what types of AI systems are in use and what level of scrutiny may be needed depending on their function, complexity, and potential impact on human rights.

Defining AI more clearly is an important precondition for understanding what types of AI systems are in use and what level of scrutiny may be needed.

These omissions are more than just a problem for researchers: They dampen the prospects for regulating AI and adequately monitoring AI systems to address privacy, human rights, and other risks. Our study found that **there is currently a void when it comes to defining working principles, ethical norms, and even basic concepts related to AI**. The National Bank of Georgia was the only exception we identified; it has adopted a decree setting out risk management principles and control mechanisms for statistical, AI, and machine learning systems. In May 2022, the decree was revised to include requirements to adopt ethical standards and certain transparency mechanisms for these systems.[7]

FILLING THE GAPS

Georgia's situation highlights several critical gaps that struggling democracies will need to close if they want to ensure that AI's integration into their public sectors strengthens, rather than weakens, state accountability. In order to begin tackling this challenge, digitalizing democracies should keep in mind the following principles:

- **Analyze Critical Risks.** When agencies embark on the process of developing AI tools, officials should analyze algorithmic risks as well as opportunities that technology offers, and establish relevant ethical, transparency, and accountability mechanisms at the outset. Moreover, **safeguards should be enacted in advance to mitigate human rights risks and ensure that officials do not have opportunities to abuse AI tools for personal, economic, or political ends.**[8] These measures are especially vital where public institutions have been criticized for their opacity, corruption, or lack of oversight.
- **Prioritize Tech Literacy.** Public institutions need to bolster their capacity to understand the workings and challenges of AI systems, emerging trends in this field, and how to address technical issues, among other considerations. To this end, **institutions should regularly provide opportunities for public servants to participate in experience-sharing and educational programs**. As our exchanges and meetings with civil servants during our research demonstrated, there is currently no common understanding about AI systems within Georgia's public institutions. The issue is viewed as a niche policy concern, often considered relevant only for technology specialists. New training and credentials for civil servants can help to address this knowledge gap and encourage more effective engagement on the human rights impacts of AI technologies.

Officials should analyze algorithmic risks as well as opportunities that technology offers, and establish relevant ethical, transparency, and accountability mechanisms at the outset.

FIGURE

Key Principles for the Democratic Integration of AI in Government

To ensure that public agencies' use of AI tools is in line with democratic values, officials should keep the following guidelines in mind.

Analyze Critical Risks | **Prioritize Tech Literacy** | **Share Information with the Public** | **Develop Crucial Normative Frameworks**

- **Share Information with the Public.** To build public trust in AI systems and ensure that people see actions taken with the help of these tools as legitimate, **adequate information about their functions and capacities must be made publicly available.** In addition, complaint mechanisms should be made available for those affected by system failures or other technical errors.
- **Develop Crucial Normative Frameworks.** Countries must develop adequate **overarching regulatory frameworks and standards** for AI systems across sectors and articulate a **common vision when it comes to the benefits expected** from these systems. These frameworks should provide a **clear definition of AI** as a starting point for broader conversations.

In various international fora, it has become popular to speak about the need for multistakeholder AI governance. In practice, however, **civil society organizations seeking to engage on these issues face major roadblocks when public institutions are opaque or even ill-informed about their own use of AI tools.** Establishing clearer norms, concepts, and procedures for AI governance will be a crucial step toward ensuring that civil society can carry out its critical role overseeing public institutions in the digital age.

Civil society organizations seeking to engage on these issues face major roadblocks when public institutions are opaque or even ill-informed about their own use of AI tools.

LEVERAGING AI TO COUNTER CORRUPTION IN ARMENIA

// **HAYKUHI HARUTYUNYAN,** CHAIR OF THE CORRUPTION PREVENTION COMMISSION OF THE REPUBLIC OF ARMENIA

In March 2020, Armenia's Corruption Prevention Commission (CPC) started a digital project aimed at making it easier to hold public officials accountable. Specifically, the Commission decided it would develop **a new digital platform to collect, store, and analyze the asset declarations of public officials**, in order to help watchdogs, journalists, and the public sift through data for signs of officials' malfeasance. As part of this project, the CPC plans to incorporate an algorithmic tool with artificial intelligence/machine learning (AI/ML) capabilities to sift through thousands of e-declarations and find red flags.

This initiative is an **example of the potential that new digital systems for collecting and processing data hold for bolstering government accountability.** Although many such tools are designed to give governments a more granular picture of social trends and patterns, projects like the CPC's platform can instead **enable greater scrutiny of government officials**. At the same time, the CPC faced challenges when it comes to thinking through how democratic principles should be applied to the **procurement, design, and use of the digital platform itself**. Through measures such as advance consultations with key stakeholders and adherence to international data protection norms, the CPC is striving to demonstrate accountability in its approach to these processes as well.

CORRUPTION AS A MAJOR CHALLENGE

Corruption has been a major challenge for Armenia since the country gained independence from the Soviet Union in 1991.[1] Over the following decades political power was organized around leader-centric oligarchic networks, underpinned by backroom dealings and patronage relationships. These networks subverted and superseded the workings of formal social, political, legal, and economic institutions. Although there has been pressure from civil society and international institutions to act against corruption, this challenge has persisted.

The **April 2018 "Velvet Revolution"** of nationwide protests was a major turning point, peacefully bringing down Armenia's highly corrupt, semi-authoritarian regime.[2] In late November 2019, the new government launched the **independent CPC**, reflecting a commitment to make resilience against corruption a priority in the country's democratic transition.

To aid in this struggle, the CPC began looking for a way to monitor officials' assets and activities more effectively. At this point, Armenia already had an **electronic platform for asset declarations** that was first developed in 2012 in response to OECD recommendations.[3] State officials holding certain positions (about 3,500 people as of 2017) are required to submit these declarations periodically as a measure to **prevent conflicts of interest, illicit self-enrichment, and other forms of malfeasance**. In theory, the declarations provide the public with a reasonably exhaustive picture officials' income, expenditures, and activities.

In practice, however, the electronic platform was more a box-checking exercise—aimed at meeting the formal demands of the national anticorruption strategy—than an effective tool for holding officials accountable. It lacked automated functions for submission and verification, analysis, or cross-checking of data within the system and across other government databases. Even if applicants chose to fill in their declarations electronically, the resulting information was stored in PDFs rather than in a machine-readable format.

These shortcomings forced anyone wishing to analyze data to first retrieve it and then compare it to other sources manually. With limited human resources available to process a staggering volume of information, government watchdogs succeeded in analyzing only a tiny fraction of the available declarations. Similarly, although the declarations were public, civil society organizations and the media found it challenging to work with data in this format.

With limited human resources available to process a staggering volume of information, government watchdogs succeeded in analyzing only a tiny fraction of the available declarations.

DATA FOR DEMOCRACY

As part of the reform agenda, the asset declarations have been expanded to include additional information and now cover roughly seven thousand public officials, as well as those who reside with them (all together, approximately 35,000 declarations are submitted annually). **The CPC wanted to make this information more accessible and useful for accountability institutions as well as the general public.**[4] To this end, the Commission decided to develop an electronic platform that would store the data in a structured way, enabling users to search, analyze, and compare information on public officials more readily. For the CPC's internal purposes, we would take the use of digital tools one step further by employing **algorithmic decision making and AI/ML** both to flag potential indicators of malfeasance by officials automatically and to assist the CPC with data analysis.

The Commission decided to develop an electronic platform that would store the data in a structured way, enabling users to search, analyze, and compare information on public officials more readily.

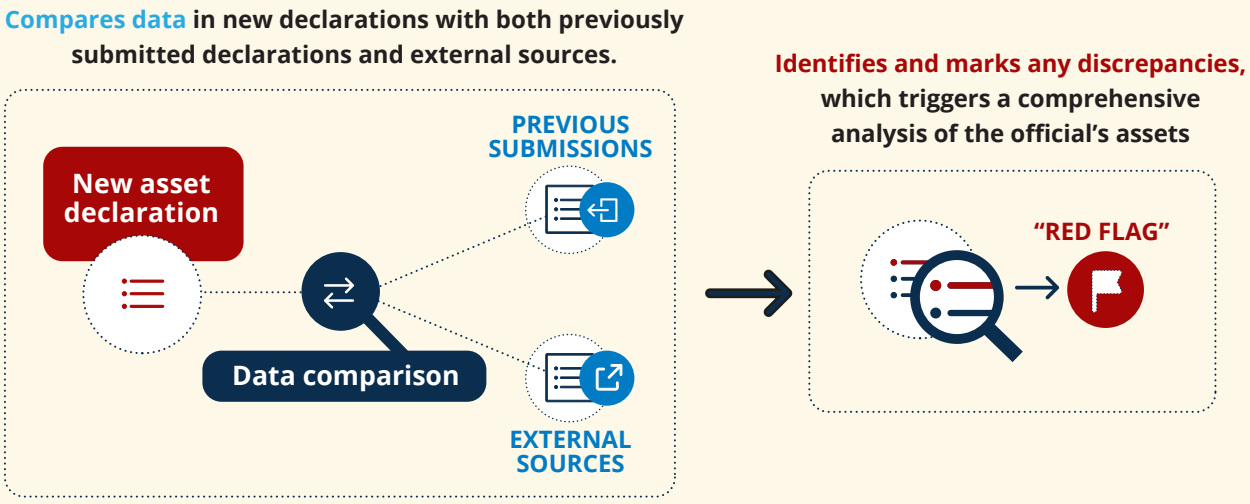
The first module of our platform is now complete. This system streamlines data entry and collection in a number of ways. It **automatically integrates data from other state agencies** and employs various automated functions to make use of the platform simpler for declarants as well as those looking for information. Since data will be disclosed publicly, this latter group potentially includes civil society, media outlets, and the wider public. The system tracks actions by both users and the system's managers (the CPC) to ensure accountability.

One of the innovations in the new platform is an automated verification function that compares data in new declarations with both previously submitted

FIGURE

Automated Verification of New Asset Declarations

The CPC's new digital platform will give corruption investigators a head-start on identifying official misconduct.



declarations and external sources (other state databases). Whenever this process identifies any discrepancies, the system will mark these concerns as a "red flag," which will trigger a comprehensive analysis of the official's assets. That procedure begins with an automated analysis of prior declarations and available external data, after which the CPC initiates a legal inquiry. The system's analytical process can be tailored to meet the needs of individual agencies, and a **public application programming interface (API)** enables reporters, activists, and ordinary citizens to use their own software tools to sift through declaration data on the public website.

After the initial round of applications is submitted through the new platform, work on the second module will begin. This next stage of our project will employ more advanced analytical tools to **flag corruption risks automatically**. Initially, its algorithm will be based on fixed indicators developed for the CPC's own corruption risk assessment tool. After a trial period, however, we intend to activate an **AI/ML component that will enable the system to "learn" from the data it processes**, helping us to identify new types corrupt and deceptive practices. In this way, we can stay one step ahead of officials looking to conceal their conflicts of interest or ill-gotten gains.

Defining our objective was was not simply a task for a single vendor; rather, it required effective communication with public institutions, as well as media outlets and civil society.

ENGAGING PARTNERS AND STAKEHOLDERS

The process of developing the new electronic platform has been challenging in all phases, from identifying a developer to meeting the safeguards required of a public institution that collects, stores, and analyzes potentially sensitive data.

The first and most essential step was to define the objective: What key features would need to be included? Answering this question was not simply a task for a single vendor; rather, it required **effective communication with public institutions, as well as media outlets and civil society**. The CPC conducted numerous consultations—with USAID support and engagement by relevant experts—before it developed terms of reference for the project and issued a call for bids.[5] After researching existing systems similar to the one we wished to create, as well as the companies that had developed them, we approached firms outside Armenia in hopes of **drawing on international experience**. Our discussions with international companies helped us to deepen our understanding of the data collection scheme and analytics we would require. The consultation process as a whole made clearer to us the importance of **first having structured data available in order to carry out an effective analysis**, among other matters.

To develop the system, the CPC looked for partners among both local and international private information technology (IT) companies. However, distrust

toward the government proved to be an obstacle: Given past precedents of cronyism and corruption, **local companies doubted that a public institution would assess their applications fairly**. As a result, none were received by the stated deadline. To encourage more local participation, the CPC has organized meetings and discussions with local IT companies. For example, we launched a campaign on "Innovative (Digital) Technologies to Prevent Corruption: Opportunities and Needs for Cooperation." Ultimately, three international and two local vendors applied; we selected one of the latter.

Since the CPC's mandate encompasses corruption risks in both the private sector and public institutions, we also used these and other meetings to communicate an important message for developers: Private IT companies are expected to adhere to codes of conduct, follow ethical rules-based design and management practices, and take measures to ensure equal opportunity and prevent conflicts of interest. To further drive this message home, the CPC plans to pilot the **corruption risk assessment methodology** it has been developing in five semi-public institutions,[6] including EKENG—an e-governance infrastructure implementation agency. In this way, **public-sector digitalization can reinforce good governance norms in the wider society**.

GRAPPLING WITH PRIVACY

In designing this system—especially the features that allow for public engagement—the CPC faced the challenge of balancing privacy and personal security with the public's interest in transparency and accountability. In this regard, we have relied on principles defined by the European Court of Human Rights, which established that **general publics have a legitimate interest in transparency around the conduct of public officials**. Online access to asset declarations serves this interest, since the public needs an easy way to view these declarations if they are to be an effective tool for making citizens more informed. However, we ultimately came to the conclusion that while the declarations themselves would be public, the algorithmic tool we are developing to flag corruption risks will need to be kept private in order to ensure compliance with the EU's General Data Protection Regulation (GDPR).

The CPC faced the challenge of balancing privacy and personal security with the public's interest in transparency and accountability.

In general, **the CPC has followed the standards established by the GDPR, as well as additional requirements enumerated in Armenia's own legislation**. These efforts will not only make the platform privacy compliant, but also ensure adequate functionality and protect the rights of all users. Once the platform is ready for use, the CPC also plans to ensure its compliance with international standards for information security.

DIGITAL ACCOUNTABILITY

The CPC's experience underscores that **data-driven technologies can be a force for accountable governance**. At the same time, it is important for institutions that are deploying these tools to build relationships of trust with stakeholders across government, civil society, and the public sector; engage these stakeholders in setting the parameters for new systems; and familiarize themselves with norms for responsible digital design and deployment. Taking these steps will help to ensure that as watchdog institutions leverage new digital tools, they can continue to hold themselves and other sections of government accountable to the citizens they serve.

ENDNOTES

The Digital Battlefield for Democratic Principles

1 For more information, please consult the Bertelsmann Stiftung's "China's Social Credit System" graphic: www.bertelsmann-stiftung.de/fileadmin/files/aam/Asia-Book_A_03_China_Social_Credit_System.pdf.

2 *The Global State of Democracy 2021: Building Resilience in the Pandemic Era*, International IDEA, November 2021, https://idea.int/gsod-2021/sites/default/files/2021-11/global-state-of-democracy-2021.pdf.

3 Raquel Benbunan-Fich, Kevin C. Desouza, and Kim Normann Andersen, "IT-Enabled Innovation in the Public Sector," *European Journal of Information Systems*, 29 (October 2020): 323-328, www.tandfonline.com/doi/full/10.1080/0960085X.2020.1814989?scroll=top&needAccess=true&role=tab.

4 Jeff Larson et al., "How We Analyzed the COMPAS Recidivism Algorithm," ProPublica, 23 May 2016, www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm; Koen Vervloesem "How Dutch activists got an invasive fraud detection algorithm banned," AlgoritmWatch, 2020, https://algorithmwatch.org/en/syri-netherlands-algorithm/; and Will Bedingfield, "Everything that Went Wrong with the Botched A-Levels Algorithm," *Wired,* 19 August 2020, www.wired.co.uk/article/alevel-exam-algorithm.

5 For more information, please visit *the Guardian's* "the Pegasus Project" webpage: www.theguardian.com/news/series/pegasus-project.

6 Janna Anderson and Lee Rainie, "Many Tech Experts Say Digital Disruption Will Hurt Democracy," Pew Research Center, 21 February 2020, www.pewresearch.org/internet/2020/02/21/many-tech-experts-say-digital-disruption-will-hurt-democracy/.

7 Adrian Shahbaz, Allie Funk, and Kian Vesteinsson, *Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet,* Freedom House, 2022, https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet.

8 Lincoln Ajoku, "How Civil Society Can Work to Improve our Technological Future," Open Global Rights, 13 March 2019, www.openglobalrights.org/how-civil-society-can-work-to-improve-our-technological-future/.

9 Katya Abazajian et al., "Artificial Intelligence in the City: Building Civic Engagement and Public Trust," eds. Ana Brandusescu and Jess Reia, Centre for Interdisciplinary Research on Montreal (McGill University), 2022, https://libraopen.lib.virginia.edu/downloads/6w924c005.

10 "Algorithm of the System of Random Allocation of Cases finally disclosed!" Moje Państwo Foundation, 22 September 2021, https://mojepanstwo.pl/aktualnosci/773.

11 Buhm-Suk Baek et al., "New and Emerging Digital Technologies and Human Rights," United Nations Human Rights Council, 2021, www.ohchr.org/en/hr-bodies/hrc/advisory-committee/digital-technologiesand-hr.

12 For more information about the challenge of engaging traditional human rights groups in digital rights discussions, please see: Eduardo Ferreyra, "Bridging the Gap between the Digital and Human Rights Communities," *Power 3.0* (blog), 25 October 2022, www.power3point0.org/2022/10/25/bridging-the-gap-between-the-digital-and-human-rights-communities/.

13 Wilson Wong and Eric W. Welch, "Does E-Government Promote Accountability? A Comparative Analysis of Website Openness and Government Accountability," *Governance,* 17 (April 2004): 275-297, www.researchgate.net/publication/227629713_Does_E-Government_Promote_Accountability_A_Comparative_Analysis_of_Website_Openness_and_Government_Accountability.

14 For information, please see this grant information page on the Digital Freedom Fund's website: https://digitalfreedomfund.org/access-to-government-algorithms-in-poland/.

15 For more information, please consult: Piotr Mgłosiek "SLPS, czyli Swoim Lepszy Przydział Spraw" [SLPS, or a Better Allocation of Cases for Ourselves], *Dziennik Gazeta Prawna,* 28 November 2018, https://prawo.gazetaprawna.pl/artykuly/1368536,mglosiek-o-losowym-przydziale-spraw.html; Piotr Mgłosiek "Mgłosiek o losowaniu spraw: SLPS, czyli mało miejsca na przypadek" [Mgłosiek on case allocation: SLPS, or little room for chance], *Dziennik Gazeta Prawna,* 7 March 2019, https://prawo.gazetaprawna.pl/artykuly/1401758,mglosiek-losowanie-spraw-sadowych.html; and Małgorzata Kryszkiewicz, "Jak w praktyce (nie) działa losowy przydział spraw" [How random case allocation (doesn't) work in practice], *Dziennik Gazeta Prawna,* 21 November 2018, https://prawo.gazetaprawna.pl/artykuly/1357772,losowy-poczal-spraw-nie-dziala.html.

16 For more information, please see this Polish Supreme Administrative Court ruling from May 26, 2022: https://orzeczenia.nsa.gov.pl/doc/E6F1F9BFB1. (Original source material in Polish.)

17 Nenad Georgievski "ACMIS served as a decoration only: The Criminal and the Supreme Court were allocating cases manually," Meta.mk, 7 December 2017, https://meta.mk/en/acmis-served-as-a-decoration-only-the-criminal-and-the-supreme-court-were-allocating-cases-manually/.

18 Michal Škop et al., *alGOVrithms 2.0: The State of Play*, eds. Art Alishani and Krzysztof Izdebski, Open Data Kosovo (ODK), March 2021, https://opendatakosovo.org/wp-content/uploads/2021/03/ODK_alGOVrithms-2-0_report-2021_1.pdf.

19 For more information, please see the Council of the European Union's "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts" (November 11, 2022): https://artificialintelligenceact.eu/wp-content/uploads/2022/11/AIA-CZ-Draft-General-Approach-11-Nov-22.pdf.

20 Paola Lopez, "Reinforcing Intersectional Inequality via the AMS Algorithm in Austria" Critical Issues in Science, Technology and Society Studies (Graz: Verlag der Technischen Universität), 1–19, 2019, https://paolalopez.eu/wp-content/uploads/2019/11/LOPEZ_Preprint.pdf.

21 Frederik Zuiderveen Borgesius, *Discrimination, Artificial Intelligence, and Algorithmic Decision-Making,* Council of Europe, 2018, https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73; and Jessica Wulf, "Automated Decision-Making Systems and Discrimination: Understanding causes, recognizing cases, supporting those affected (A guidebook for anti-discrimination counselling)," AlgorithmWatch, June 2022, https://algorithmwatch.org/en/wp-content/uploads/2022/06/AutoCheck-Guidebook_ADM_Discrimination_EN-AlgorithmWatch_June_2022.pdf.

22 Tom Christiano and Sameer Bajaj, "Democracy" in *The Stanford Encyclopedia of Philosophy (Spring 2022 Edition),* ed. Edward N. Zalta, 3 March 2022, https://plato.stanford.edu/archives/spr2022/entries/democracy/.

23 Carissa Véliz, "Why Democracy Needs Privacy," *Boston Review,* 6 April 2021, www.bostonreview.net/articles/why-democracy-needs-privacy/.

24 For more information, please see: "Media, Chats, Narratives: The Role of the Internet and Other New Technologies During Protests in Belarus," ed. Krzysztof Izdebski, Fundacja ePaństwo, 2020, https://drive.google.com/file/d/1OT1YTXjQug_fG8Lkw1DA7SIcAUL5U7XO/view; Anastasiia Kruope, "Moscow's Use of Facial Recognition Technology Challenged," Human Rights Watch, 8 July 2020, www.hrw.org/news/2020/07/08/moscows-use-facial-recognition-technology-challenged; and "Facial Recognition," Privacy International, 2022, https://privacyinternational.org/learn/facial-recognition.

25 Gerard Ritsema van Eck, "Privacy and Participation in Public: Data protection issues of crowdsourced surveillance," University of Groningen, 2021, https://doi.org/10.33612/diss.171025411.

26 "Technology, data and elections: A 'checklist' on the election cycle," Privacy International, June 2019, https://privacyinternational.org/sites/default/files/2019-07/Technology%2C%20data%2C%20and%20elections_0.pdf.

27 For more information, please visit the EU's AI Act website: https://artificialintelligenceact.eu/.

28 For more information, please consult: "Democracy and technology," the Council of Europe, 2022, www.coe.int/en/web/good-governance/democracy-and-technology.

29 "Challenges in implementing digital change," House of Commons Committee of Public Accounts, 10 December 2021, https://committees.parliament.uk/publications/8146/documents/83439/default/.

30 Cem Dener et al., *GovTech Maturity Index: The Stage of Public Sector Digital Transformation,* (Washington, D.C.: World Bank Group: 2021), https://openknowledge.worldbank.org/entities/publication/5b2c81db-9bd3-5a41-b05d-14f878abe03d.

31 Michal Škop et al., *alGOVrithms: State of Play*, ed. Krzysztof Izdebski, Center for Research, Transparency and Accountability (CRTA), 21 May 2019, https://crta.rs/en/algovrithms-state-of-play/; and Michal Škop et al., *alGOVrithms 3.0: The State of Play—How Automated Are Our Public Procedures: Czechia, Hungary, Kosovo, and Poland*, eds. Ariana Gjuli and Krzysztof Izdebski, to be published 13 April 2023, (formal publication forthcoming).

32 "Information on the results of the audit. Implementation of IT Projects Aimed at Improving Administration Of Justice," Polish Supreme Audit Office, 22 September 2020, www.nik.gov.pl/plik/id,23378.pdf.

33 *alGOVrithms 2.0: The State of Play.*

34 *alGOVrithms: State of Play.*

35 For more information, please see: "Algorithmic impact assessment: AIA template," Ada Lovelace Institute, 8 February 2022, www.adalovelaceinstitute.org/resource/aia-template/.

36 "Algorithmic Impact Assessment Tool," Government of Canada, 19 January 2023, www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html.

37 "Algorithmic Assessment Report," Government of New Zealand, 21 March 2021, https://data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-assessment-report/.

38 Paula Perez and Paul Braithwaite, "Algorithms and Human Rights: Understanding Their Impacts," Open Government Partnership (blog), 28 June 2022, www.opengovpartnership.org/stories/algorithms-and-human-rights-understanding-their-impacts/.

39 Sabine Gerdon et al., *AI Procurement in a Box: AI Government Procurement Guidelines,* World Economic Forum, June 2020, www3.weforum.org/docs/WEF_AI_Procurement_in_a_Box_AI_Government_Procurement_Guidelines_2020.pdf.

40 Wayne Lonstein, "Technology without Transparency Lacks Trust," *Forbes,* 30 June 2021, www.forbes.com/sites/forbestechcouncil/2021/06/30/technology-without-transparency-lacks-trust/?sh=792d629a3cf0.

41 For more information, please consult: "Grupa Robocza ds. Sztucznej Inteligencji (GRAI)" [Working Party on Artificial Intelligence (GRAI)], Government of Poland, 2021, www.gov.pl/web/cyfryzacja/grupa-robocza-ds-sztucznej-inteligencji-grai. (Original source material in Polish.)

42 Krzyzstof Izdebski, "Civic Tech and Governments: Successful Models of Collaboration," *Medium,* 12 November 2018, https://medium.com/dsi4eu/civic-tech-and-governments-successful-models-of-collaboration-9d1787b35aaf; and more for more information, please see: https://codeforall.org/.

43 For more information, please consult: https://codeforpakistan.medium.com/the-kp-women-civic-internship-program-2021-4fc8bd345a89.

44 For more information, please consult: https://techfordemocracy.dk/coalitions/.

45 For more information, please consult: https://europeanaifund.org/.

46 For more information, please consult: https://digitalfreedomfund.org/.

47 Jonathan McCully "Strategising together: embedding tech expertise in digital rights litigation," Digital Freedom Fund, 17 August 2022, https://digitalfreedomfund.org/author/jonathan/page/2/.

Assessing the Accountability of AI Systems in Georgia

1 Much of the information in this essay has been drawn from IDFI's study on AI usage in the public sector (with a focus on Georgia). For more information, please consult: *Artificial Intelligence: International Tendencies and Georgia – Legislation and Practice*, Institute for Development of Freedom of Information, 19 February 2021, https://idfi.ge/en/artificial%20intelligence_international_tendencies_and_georgia.

2 These government institutions were: the Ministry of Internal Affairs of Georgia and its Public Safety Command Center 112, the General Prosecutor's Office of Georgia, the Georgian National Tourism Administration, Education Management Information System for the Ministry of Education and Science, and the National Center for Educational Quality Enhancement.

3 For instance, POLYFACE application is a system that can be used identify persons of interest using subjective portraits (photorobots)—For more information, please see: https://papillonsystems.com/products/programs/polyface/; and *Artificial Intelligence: International Tendencies and Georgia – Legislation and Practice*.

4 "დანაშაულის გამოსაძიებლად საქართველო რუსულ ხელოვნურ ინტელექტს იყენებს," [Georgia Uses Russian Artificial Intelligence to Investigate Crimes], NextOn, 24 January 2023, https://tinyurl.com/2p8b5u78; and Nastasia Arabuli, "როგორ იყენებს ქართული პოლიცია რუსულ პროგრამებს და საექსპერტიზო ტექნიკას" [How the Georgian Police Uses Russian Programs and Expert Techniques], Radio Free Europe/Radio Liberty, 31 January 2023, http://bit.ly/3DHwsAZ. (Original source material for both citations in Georgian.)

5 "Statement of the Strategic Communications Department of the Ministry of Internal Affairs," Department of Strategic Communications of the Ministry of Internal Affairs, 26 January 2023, www.facebook.com/photo?fbid=495601639418277&set=a.233701852274925.

6 Initiatives along these lines can be found in Amsterdam, Helsinki, and New York City. For more information, please see: Khari Johnson, "Amsterdam and Helsinki Launch Algorithm Registries to Bring Transparency to Public Deployments of AI," Venture Beat, 28 September 2020, https://venturebeat.com/ai/amsterdam-and-helsinki-launch-algorithm-registries-to-bring-transparency-to-public-deployments-of-ai/.

7 "მონაცემებზე დაფუძნებული სტატისტიკური, ხელოვნური ინტელექტის და მანქანური სწავლების მოდელების რისკების მართვის დებულების დამტკიცების თაობაზე" [Approving the Provision for Risk Management of Data-Driven Statistical, Artificial Intelligence and Machine Learning Models], Office of the President of the National Bank of Georgia, 17 August 2020, https://matsne.gov.ge/en/document/view/4964423?publication=0. (Original source material in Georgian.)

8 Procedures to address these risks have been implemented in other settings. Please see, for instance, the following examples: The Canadian government's Algorithmic Impact Assessment Tool, www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html; and the U.K.'s Algorithmic Transparency Standard, www.gov.uk/government/collections/algorithmic-transparency-reports.

Leveraging AI to Counter Corruption in Armenia

1 Mathias Bak, "U4 Helpdesk Answer," Transparency International, 18 April 2022, https://knowledgehub.transparency.org/assets/uploads/kproducts/Overview-of-corruption-and-anti-corruption-in-Armenia_2022-final.pdf.

2 Miriam Lanskoy and Elspeth Suthers, "Armenia's Velvet Revolution," *Journal of Democracy*, 30, 2 (April 2019), 85-99, www.journalofdemocracy.org/articles/armenias-velvet-revolution/.

3 "Anti-Corruption Reforms in Armenia: Round 3 Monitoring of the Istanbul Anti-Corruption Action Plan," OECD, 2014, www.oecd.org/daf/anti-bribery/Armenia-Round-3-Monitoring-Report-ENG.pdf.

4 Such information included data on officials' expenditures, rented properties, liquid financial assets, external activities, employment, investment portfolios, as well as information on the assets of their family members and other persons residing with them.

5 For more information, please consult this information page from the CPC's website: http://cpcarmenia.am/files/legislation/365.pdf.

6 For more information about the methodology of this initiative, please see: "A Two-Day Convention on the Assessment of Corruption Risks was Summarized," CPC, 14 October 2022, http://cpcarmenia.am/hy/news/item/2022/10/14/2022-10-14/. (Original source material in Armenian.)

ABOUT THE CONTRIBUTORS

ABOUT THE AUTHORS

Krzysztof Izdebski is co-lead of the Open Spending EU Coalition and legal and policy officer at the Stefan Batory Foundation. He is a member of the Osiatyński Archive Advisory Board, the Marshall Memorial, Marcin Król, and and an alumnus of the Recharging Advocacy Rights in Europe program. Izdebski is a lawyer specializing in Freedom of Information cases, as well as legal questions pertaining to the re-use of public sector information and technology's impact on democracy. He also has broad expertise in the relationship between public-facing institutions and citizens. Finally, he has authored publications on freedom of information, technology, public administration, corruption, and public participation. Follow him on Twitter: @K_Izdebski.

Teona Turashvili is head of local government as well as internet and innovations directions at the Institute for Development of Freedom of Information (IDFI) based in Tbilisi, Georgia. She leads and coordinates IDFI's activities and projects on new technologies, digital rights, internet, e-governance, and open data issues. She has also authored dozens of analytical papers and research projects. Turashvili earned her Master's degree from the Institute of Political Science at the University of Warsaw. She is also a graduate student of the Masters of Sciences program in Transformation in the South Caucasus at the Center for Social Sciences, at Tbilisi State University. Follow her on Twitter: @teoturashvili.

Haykuhi Harutyunyan is a human rights defender and lawyer, currently serving as chair of the Corruption Prevention Commission (CPC) of the Republic of Armenia. She previously led Protection of Rights Without Borders, an influential human rights organization in Armenia, and has over fifteen years of experience working with local and international civil society organizations on rule of law, judiciary, and human rights issues, including as a member of the Steering Committee of the Eastern Partnership Civil Society Forum from 2016 to 2019. Harutyunyan was a 2018 Draper Hills Summer Fellow at Stanford University's Center for Democracy, Development, and the Rule of Law, a 2011-2012 Hubert Humphrey Fellow at the University of Minnesota Law School's Human Rights Center, and a 2020-2021 Reagan-Fascell fellow at NED.

ABOUT THE EDITOR

Beth Kerley is a program officer with the research and conferences section of the National Endowment for Democracy's International Forum for Democratic Studies. She manages the Forum's emerging technologies portfolio, which covers the challenges and opportunities for democracy as technological advances in areas such as machine learning, the Internet of Things, and big-data analytics supply new tools of politics and governance. She was previously associate editor of the Journal of Democracy, and holds a PhD in History from Harvard University and a Bachelor of Science in Foreign Service from Georgetown University.

ACKNOWLEDGMENTS

The authors appreciate the contributions of the International Forum's staff and leadership, including Christopher Walker, John Glenn, Kevin Sheives, John Engelken, Lily Sabol, and Joslyn Brodfuehrer, all of whom played important roles in the editing and publication of this report. The authors and editors of this report also wish to acknowledge its anonymous peer reviewer whose comments sharpened and further refined the analysis and text. Particular acknowledgment goes to Beth Kerley, whose support and vision for this project were vital to its completion.

In addition, Haykuhi Harutyunyan would like to express special thanks and gratitude to Matthew Murray who was the team leader for the USAID project in Armenia. He has helped and guided the team to develop the technical requirements aligned with the corruption prevention. As a vital partner and team member, she would like to acknowledge Aren Zomoradian and Tawheed Makhdoomi for their professional and personal support.

Finally, the Forum wishes to thank Factor3 Digital for their efforts and invaluable support in designing this report for publication.

PHOTO CREDITS

Cover image: Photo by GIGISTOCK/Shutterstock

Page 4: Photo by Kheng Guan Toh/Shutterstock

Page 6: Photo by Jade Gao/AFP via Getty Images

Page 11: Photo by Olivier Hoslet/POOL/AFP via Getty Images

Page 16: Photo by PopTika/Shutterstock

Page 21: Photo by GagoDesign/Shutterstock

FORUM | INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES

The International Forum for Democratic Studies at the National Endowment for Democracy (NED) is a leading center for analysis and discussion of the theory and practice of democracy around the world. The Forum complements NED's core mission—assisting civil society groups abroad in their efforts to foster and strengthen democracy—by linking the academic community with activists from across the globe. Through its multifaceted activities, the Forum responds to challenges facing countries around the world by analyzing opportunities for democratic transition, reform, and consolidation. The Forum pursues its goals through several interrelated initiatives: publishing the *Journal of Democracy*, the world's leading publication on the theory and practice of democracy; hosting fellowship programs for international democracy activists, journalists, and scholars; coordinating a global network of think tanks; and undertaking a diverse range of analytical initiatives to explore critical themes relating to democratic development.

NED | NATIONAL ENDOWMENT FOR DEMOCRACY

SUPPORTING FREEDOM AROUND THE WORLD

The National Endowment for Democracy (NED) is a private, nonprofit foundation dedicated to the growth and strengthening of democratic institutions around the world. Each year, NED makes more than 1,700 grants to support the projects of nongovernmental groups abroad who are working for democratic goals in more than 90 countries. Since its founding in 1983, the Endowment has remained on the leading edge of democratic struggles everywhere, while evolving into a multifaceted institution that is a hub of activity, resources, and intellectual exchange for activists, practitioners, and scholars of democracy the world over.

1201 Pennsylvania Avenue, NW
Suite 1100
Washington, DC 20004
(202) 378-9700
ned.org

@thinkdemocracy

ThinkDemocracy