# 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.

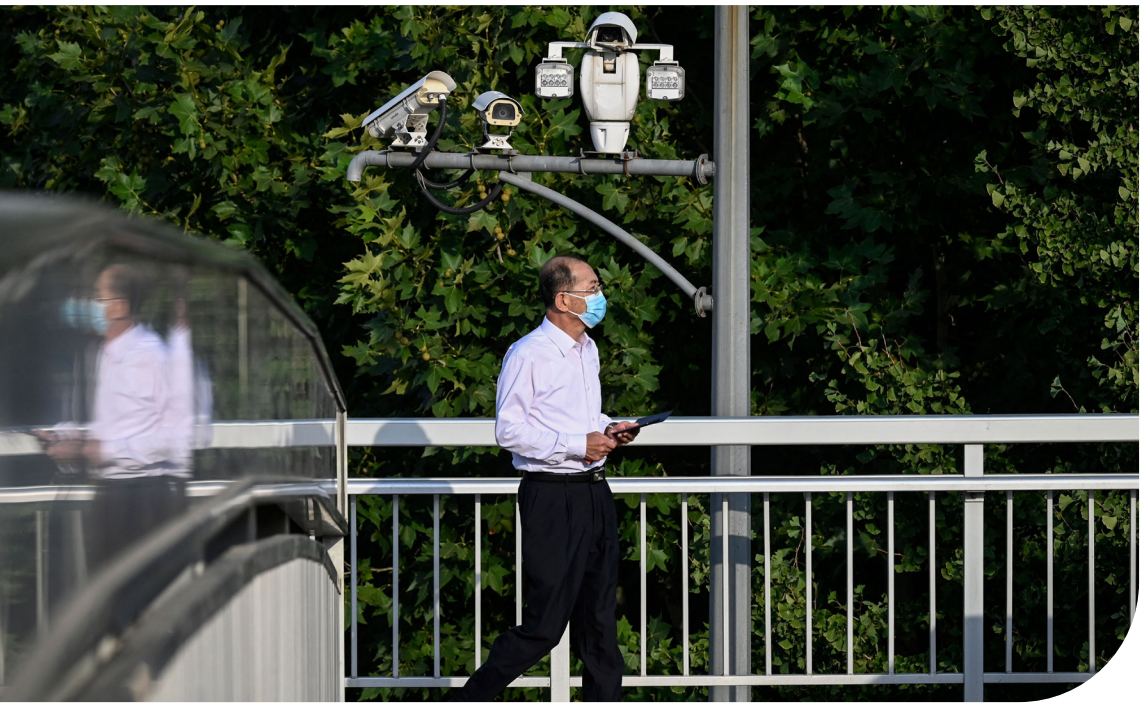
Yet like other imperfect products of human labor, digital tools in the public sector carry risks. These hazards may be present with any technology, no matter how simple, that directly or indirectly impacts democratic processes or citizens' rights and obligations. The uptake of AI and other ADMs, however, 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

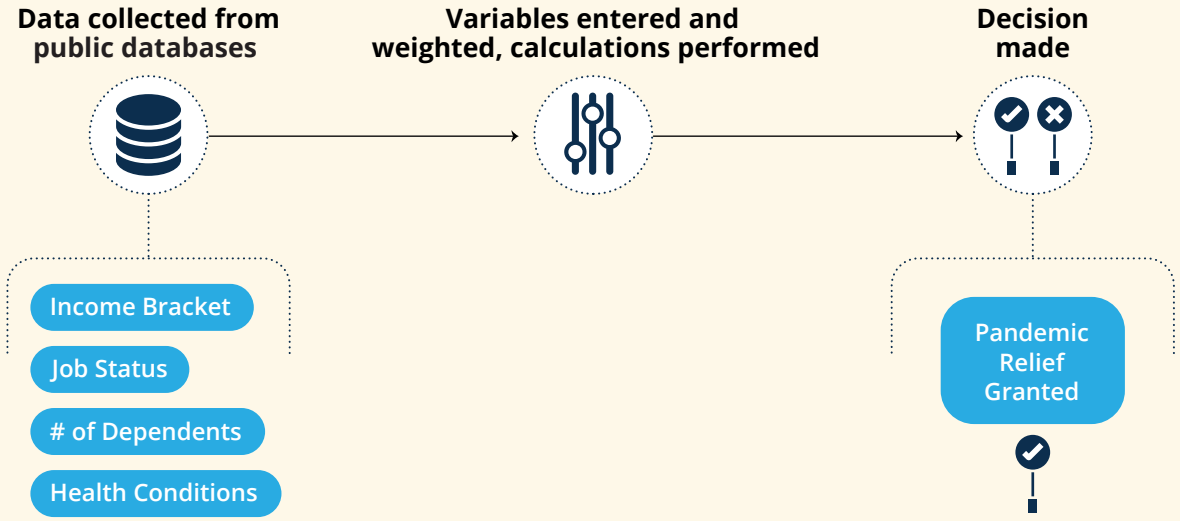
While the examples above involve digital tools serving as smokescreens for human malfeasance, accountability for harms caused by algorithmic systems themselves is also a major concern. When governments employ data-driven tools to automate decision making, discrimination against marginalized groups can 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.

# ENDNOTES

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/.

# ABOUT THE CONTRIBUTORS

## ABOUT THE AUTHORS

**Krzysztof Izdebski** is the co-lead of the Open Spending EU Coalition and the 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.

## 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 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

## PHOTO CREDITS

Page 1: Photo by Kheng Guan Toh/Shutterstock

Page 3: Photo by Jade Gao/AFP via Getty Images

Page 8: Photo by Olivier Hoslet/POOL/AFP via Getty Images

**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.

**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