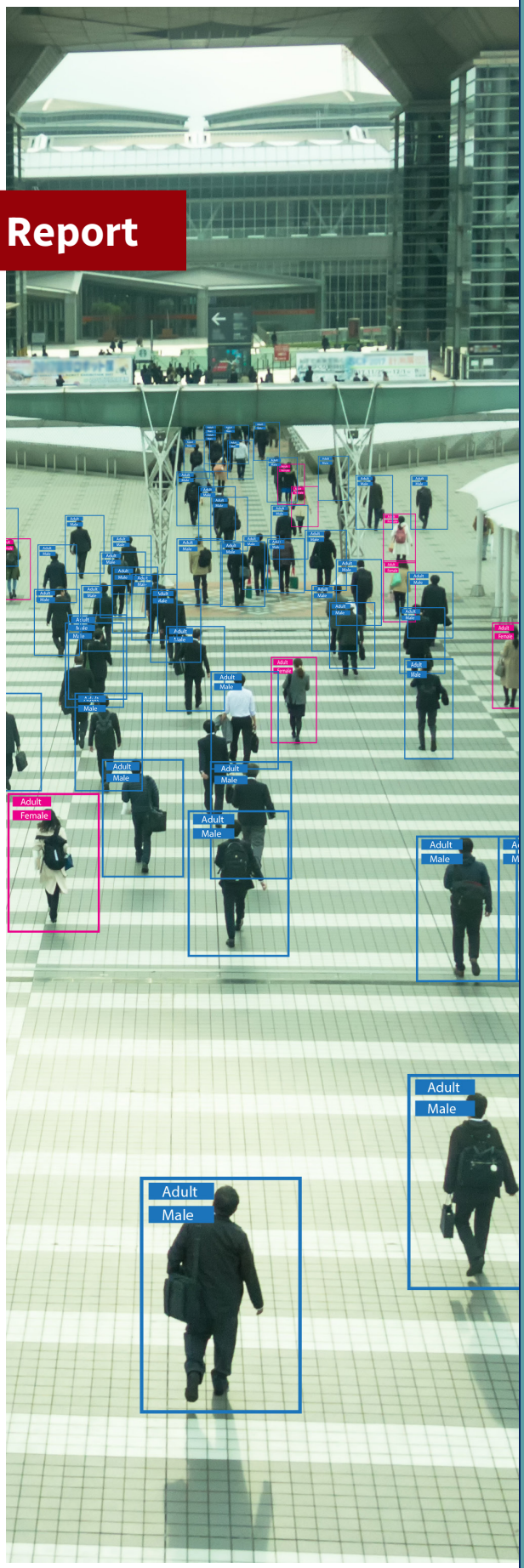

Report

G | M | F

IDEAS LEADERSHIP HOPE

AI Policy in EU Illiberal Democracies

The Experience in Hungary and Poland

Filip Konopczyński

ReThink.CEE Fellowship

January 2024

Table of Contents

Summary **4**
Introduction **5**
The Rise of AI Governance **6**
AI Regulation in the EU **7**
AI Policies in Hungary and Poland **10**
Hungary 11
Poland 14
Implications of the EU's AI Regulatory Model **19**
AI Systems in Security and Law Enforcement 20
AI in Migration Control 21
Automation of Public Administration 21
AI and Democracy 22
AI R&D and Economic Policies 23
Conclusion **24**
Endnotes **25**

Summary

This paper examines the emergence of AI policies in Hungary and Poland under illiberal governments, and highlights their potential social and political consequences, particularly for democratic values and civil and fundamental rights. It focuses on the adoption of AI in the public sector, encompassing research and development, public administration, law enforcement, migration, and economic policy. In their AI policies, both countries' governments have prioritized industry demands and subordination to the expectations of large foreign corporations (which is inconsistent with their digital sovereignty rhetoric). Meanwhile, they have neglected societal consultations and the needs of the scientific community.

The AI policies implemented in Hungary and Poland by the Fidesz and Law and Justice (PiS) parties have been characterized, respectively, by centralization and fragmentation, with varying outcomes. The AI systems deployed do not safeguard citizens' rights as the political takeover of the justice system and partisan control of law enforcement have undermined redress mechanisms and limited legal protection from AI-related violations. The increasing use of AI in election campaigns, coupled with the lack of democratic oversight, increases the risk of mass disinformation campaigns and electoral manipulation in both countries.

The cases of Hungary and Poland highlight some key implications for democracy and human rights in the EU where illiberal actors control AI policies and governance and disregard these values. The new EU AI Act may offer some protection for the rule of law and individual rights, but its potential loopholes could allow the unlawful deployment of AI systems in vital areas. AI policies in both countries have reflected their governments' illiberal tendencies, expanding their control over citizens and curtailing democratic processes. The centralized governance raises concerns about the potential for mass surveillance and censorship, while the lack of transparency and inclusivity in AI policymaking could further marginalize minority groups and vulnerable populations. However, there are key steps that the EU can take to address these issues.

First, the EU should significantly increase funding for EU AI companies and provide the new AI Office with a mandate to be involved in distributing funds for promising AI projects. This will help companies compete with global leaders and develop AI solutions aligned with human rights and democratic values. Second, the EU and its member states should provide sufficient resources to the European Commission (including a new AI Office) to effectively enforce the AI Act. This includes allocating funding for algorithm audits, legal compliance, and training for public-sector institutions. Third, they should provide funding and resources to civil society organizations (CSOs), consumer-protection agencies, and other relevant societal stakeholders to develop the legal expertise and networking capabilities necessary to exercise their rights and hold government institutions accountable. Fourth, since the AI Act does not cover defense and national security, and makes exceptions for public security and migration control, efforts are needed to establish parallel national measures aligned with EU fundamental values to address potential abuses in these areas. Fifth, the EU must work to make the AI regulatory system more inclusive and transparent. It can do so by developing new methods of multi-stakeholder consultations involving CSOs, consumers, patients, workers, and vulnerable communities for future AI legislation and governance discussions. At the member-state level, public institutions could also be asked to voluntarily register AI systems that could pose potential threats and publish information about the potential risks.

Introduction

The ethics, regulations, and governance of artificial intelligence (AI) are increasingly the focus of policymakers, administrators, and politicians. The latest phase of AI innovation, marked by the launch of ChatGPT in 2022, has further fuelled the discussion over the need for a coherent, enforceable, and future-proof AI regulatory framework.

While many of the policy discussions on AI focus on the economy and international affairs, the rise of autonomous and semi-autonomous algorithms will profoundly impact a variety of legal, societal, cultural, and political issues. Meanwhile, the rediscovery of the state as an active regulator in charge of facilitating and supervising the rise of frontier, emerging technologies has different connotations depending on the type of political regime in a country. In the European Union, this is particularly relevant in the case of Hungary and Poland. After the right-wing parties Fidesz in Hungary and Law and Justice (PiS) in Poland came to power in 2010 and 2015 respectively, both countries have been described as illiberal or "backsliding" democracies. In Budapest and Warsaw (in the latter at least up to the end of 2023), AI policy has presented particular risks of further undermining democratic values and institution, the rule of law, judiciary independence, and access to fundamental rights. A better understanding of the role of the state as regulator and as a market and political actor in the context of the AI transformation, and of the use of AI by illiberal governments in polarized societies under such regimes, gives insights into the complex nature of the new technology's impacts on democracy and suggests measures to mitigate risks.

Even with the European Commission and European Parliament reaching an agreement on the EU's long-debated AI Act in December 2023, the challenges posed by the technology are far from settled. Notably, under the act, AI systems used in law enforcement will effectively remain under the control and supervision of national public institutions and courts. Even though in certain cases the act introduces bans or strict rules, the European Commission would likely not be able to effectively stop AI practices amplifying measures that the Fidesz and PiS governments have already employed against migrants, political opposition, independent media, or private companies. As the agreed version of the act excepts law-enforcement and migration authorities from certain prohibitions, rules and transparency obligations, and leaves national security out of its scope completely, it leaves much space for the member states to arm themselves with advanced AI with a wide array of potentially invasive functionalities.

This paper examines the emergence of AI policies in Hungary and Poland under illiberal governments, and their potential social and political consequences, particularly for democratic values and civil and fundamental rights. Its main focus is on the adoption of AI in the public sector, including in research and development (R&D), administration, law enforcement, migration, and economic policy. The analysis is based on researching policies, legislation, and economic and technological data as well as interviews with scholars, activists, lawyers, and members of parliament from the two countries who have been involved in AI policymaking, including working on national and EU legislation, crafting AI strategies, and delivering policies.

The Rise of AI Governance

There is no consensus on a universal definition of artificial intelligence. The Organisation for Economic Co-operation and Development (OECD) characterizes the technology as "a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments".[1] In this paper, the term refers to a wide category of algorithmic tools (models, systems, products, end devices) designed to function with a certain level of autonomy and to execute tasks assigned to them and that surpass the simple automation of processes.

What eventually came to be known as AI policy for decades constituted only a small part of programs and agendas in academia, industry, and—particularly in the case of global powers like the United States—the defense and intelligence sectors. The scope of early AI policies was thus relatively limited, and in many cases developed by scientists and engineers rather than officials and politicians. This applied also to Hungary and Poland, whose R&D sectors from the early 1990s, and particularly after joining NATO in 1999 and the EU in 2004, were on the path of modernization and convergence with the Western innovation ecosystem.

The European Commission has proposed a legislative agenda that could significantly empower the EU and its member states to regulate and control the digital sectors, including AI.

The process of politicization of AI took off when the governments in the United States in 2016 and 2019[2] and in China in 2017[3] laid out ambitious national plans and provided substantial government funding for the development and implementation of AI at the national level. In response, the EU in 2018 published the Coordinated Plan on Artificial Intelligence, its first blueprint for an AI policy framework.[4] By enacting the General Data Protection Regulation (GDPR) in 2018, the Digital Services Act (DSA) in 2022, and the Digital Markets Act (DMA) in 2024, and by beginning in 2021 the legislative process for an Artificial Intelligence Act and an AI Liability Directive, the EU has tried to position itself on the global stage as an actor that is simultaneously pro-innovation and a standard-bearer for fundamental rights in the digital era. Through this approach, the European Commission has proposed a legislative agenda that could significantly empower the EU and its member states to regulate and control the digital sectors, including AI.

Today, AI policy and governance is a vast, complex, and growing field, as the monitoring of countries' regulatory frameworks by the OECD[5] and others shows. The modern governmental AI policy landscape usually consists of three pillars (see Table 1). The first relates to general R&D policies and includes agenda setting and financial resources allocated for that purpose. The second defines the scope and modes of introduction of AI-powered solutions within the public sector, which includes educational, administrative, policing, intelligence, defense, and security applications. The third relates to regulations and includes laws, international treaties, and technical norms and standards accepted within the industry. To be coherent and effective, government policies as well as research

Table 1. Governmental AI Policy

AI R&D Agenda	AI Implementation in the Public Sector	AI Regulations
Total spending on R&D	AI in public services and administration	International, supranational, agreements, acts, treaties etc.
Grants for higher education	AI in law enforcement and the judicial system	Fundamental (human, civic, constitutional, etc.) rights protections, prohibitions, etc.
	Rules for AI in the public sector	
	AI skills in primary, secondary, and vocational education	National laws, delegated acts for markets
Grants for businesses (industrial policy)	AI in the defense and intelligence sectors	Technical norms, codes, standards
Establishment of AI-dedicated agencies, institutes, labs, etc.		Non-binding ethical guidelines, self-regulatory frameworks, codes of conducts and practices, etc.
Official bodies responsible for regulating, overseeing, supervising, auditing, etc. the AI sector or aspects of it		

and public-sector programs need to be aligned with international treaties, national laws, and policies, which for Poland and Hungary require harmonization at the EU level.

AI Regulation in the EU

In the case of the EU, the new digital agenda includes several layers of regulations. At the international level, two agreements are under development: the EU-US Trade and Technology Council Joint Roadmap for Trustworthy AI and Risk Management and the Council of Europe's AI Convention. Apart from the AI Act, the EU's regulatory framework will also be shaped by the implementation of recently enacted DSA and DMA, both of which apply to the growing application of AI by online platforms. In the near future, the new regime will be supplemented by

the AI Liability Directive and revisions of the Product Liability Directive. The EU's emerging AI legal framework will also consist of a wide range of EU and national regulations. The list includes the GDPR and other personal-data regulations that already play a prominent role as well as other acts, directives, standards, and codes of conduct and practices (for example, the Hiroshima Process International Code of Conduct for Advanced AI System or the EU AI Code of Conduct) developed in dialogue with the industry.

These policy developments have been met with general approval and moderate optimism in expert circles. This sentiment is understandable given the scale and gravity of risks posed by digital technologies, especially in the context of the economic (inequality, inflation), military (Russia's invasion of Ukraine, tension over Taiwan), and environmental (climate crisis, increasing rivalry over resources and rare-earth minerals) threats Europe and the West face. The push for stronger digital policies also comes at a moment many call critical for the future of liberal democracy. However, pursuing a new, ambitious AI agenda in the current era of economic and international insecurity comes at a political cost. The pressure of economic and global competition may encourage governments to trade off fundamental rights and democratic values for incentivizing innovation and for public and national security. Yet, in considerations of the overall impact of AI, the state of democracy, the rule of law, the system of checks and balances, the record of civil and human rights violations, and administrative efficacy are as important as industrial capacity or openness to innovation. For these reasons, the regulation of AI-powered products, services, or business models should be designed, executed, and evaluated on the basis of the complex set of technological, societal, and political factors.

Without effective rule-of-law safeguards—particularly if the recent EU regulations fail to deliver on their promises—it would be entirely up to those in power in individual member states to decide upon the scale, goals, and methods of utilizing new, disruptive AI tools.

The debate on the threats posed by AI tends to focus on distant existential threats (the "AI Apocalypse"), economic insecurities (technounemployment), or the consequences of the AI arms race for international security. From the human rights perspective, the perils of a mass adoption of AI tools are usually linked to cases of algorithm-mediated discrimination, particularly related to gender and sexual orientation, race and ethnicity, culture and religion, or mental and physical disabilities. In the case of Hungary and Poland, which have experienced long periods under governments with a record of violating democratic standards, the widespread adoption of AI by government agencies and state-owned companies pose additional serious risks to citizens' rights. Their citizens have good reasons to fear the dangers of AI as the state can employ the technology to restrict fair access to public-administration institutions and courts; to profile voters based on their political views, beliefs, gender or sexual orientation; to create and spread propaganda and disinformation; or to surveil political opponents or voters.

Without effective rule-of-law safeguards—particularly if the recent EU regulations fail to deliver on their promises—it would be entirely up to those in power in individual member states to decide upon the scale, goals, and methods of utilizing new, disruptive AI tools such as generative AI large language models (similar or based on

ChatGPT, Stable Diffusion, or Bard, Gemini, etc.), particularly in sensitive areas of public administration, criminal and justice systems, and public and national security.

It is to address such issues that the European Commission in 2021 presented the first draft of the AI Act, which was designed to become the cornerstone of the EU's emerging AI regulatory ecosystem. At the time, Commissioner for Internal Market Thierry Breton and Executive Vice President of the European Commission for A Europe Fit for the Digital Age Margrethe Vestager focused on two main issues: competitiveness and trustworthiness. Describing the philosophy of the act, she said that "rules will intervene where strictly needed: when the safety and fundamental rights of EU citizens are at stake".[6] In this narrative, the European Commission put forward the AI Act with the ambition of balancing the interests of innovative, already-or-soon-to-become global European companies and the societal and political rights of European citizens and EU values. To achieve this, the AI Act lays down:

- Rules for placing various AI systems on the single market
- Prohibitions of certain AI practices, such as social credit scoring or most use cases of real life remote biometric identification (RBI)
- Transparency rules for interactive AI systems (chatbots etc.)
- Standards for AI systems used to generate or manipulate image, audio, or video content
- Rules on market monitoring and surveillance[7]

During the negotiations on the AI Act, civil society organizations (CSOs) pointed out its shortcomings in protecting individual and democratic rights.[8] The most heated debates centered around:

- The general scope of regulation (the biggest controversies concerned the use of AI by the state for national security).
- The list of areas in which the use of AI would be prohibited or restricted (real-time RBI), as well as the exceptions from rules and obligations for law-enforcement and border-control agencies.
- The areas defined as high-risk, including the procedures for the qualification of systems as such and for compliance and enforcement mechanisms related to fundamental rights
- The category and obligations for general-purpose AI or foundation models such as GPT, Bard, Anthropic, etc.
- The role of the European Commission including the AI Office as a new body responsible for coordinating the enforcement of the act and supervised by the member states.

Even though the AI Act does not cover the areas of science, defense, and national security, it sets out specific requirements for AI programs classified as high-risk that are applied in other domains. Once enacted, it will introduce a legal differentiation between "regular" digital tools and those that employ AI techniques. This will have a significant practical impact since any developers, providers, and deployers of the latter will have to abide the Act in order to put their products on the EU's single digital market. The security, health, and rights—among other

things—of people affected by such systems will be affected by how effectively these rules will be enforced by the European Commission and relevant national authorities.

The Pegasus hacking scandal, which revealed that the governments in Hungary and Poland (among others) used the spyware system to unlawfully surveil opposition politicians, activists, and the media is one example of how the abuse of new, powerful digital tools can undermine democratic standards, the rule of law, and the fundamental rights of individuals. Crucially, under current EU law such cases fall outside the purview of the European Commission. Law-enforcement agencies are allowed to gather extensive personal data[9] and the EU lacks political tools to stop governments from such practices or to provide people affected by them with means of legal redress.

In societies where democracy is backsliding, leaving the government with more powers over the emerging private and public AI ecosystem raises legitimate concerns. Apart from undermining fundamental rights of citizens and democratic values, the prospect of illiberal member-state governments exploiting AI-driven security mechanisms to increase or retain their power poses significant repercussions for the whole of the European Union. Should these actions go unchecked—as in the Pegasus spyware case—by EU law and institutions, it could be interpreted as a tacit endorsement of such practices throughout the union and further reduce Europeans' trust in democratic institutions and the rule of law.

AI Policies in Hungary and Poland

Despite differences in certain aspects of their development and implementation of AI governance and programs, the context for AI policies in Hungary and Poland is relatively similar. At least since 2018, the EU has been calling on member states to take action on AI governance and been a stable source of R&D funding. Yet at the same time it has failed to provide a solid framework within which governments could do so. That put the Fidesz and PiS governments in a comfortable position, allowing them to design, finance, and execute their AI policies without much oversight from Brussels.

Hungary and Poland have not made investments in science and innovation a priority, becoming instead late adopters of emerging digital technologies. Although expenditures on information and communications technologies constitutes a large part of their total spending (around 8% of GDP),[10] overall GDP per capita funding for R&D in both countries between 1989 and 2021 was low. Even though it increased in Hungary from 1% to 1.5% and in Poland from 0.79% to 1.38% over the period, both still lag far behind the 2021 OECD average of 2.67%.[11] Although the precise methodology of assessing AI investments is a matter of debate,[12] these indicators suffice to put Poland and Hungary's ambitious and aspirational—declarations, plans, and strategies into proper perspective.

In Hungary and Poland, apart from large multinational companies, the public sector plays the leading role in funding fundamental and applied research projects. While the share of private-sector investments in total R&D expenditures has steadily grown over the last decade, it still is mainly the government and the publicly funded

(often by the EU) higher-education institutions that have the financial means to shape the development of innovative products and services.

Hungary and Poland are also equally profoundly influenced by the EU context. Their AI programs are to a large extent financed by EU funds, which have increased the levels of private-sector innovations in Central and Eastern Europe.[13] On the regulatory side, the digital policies and agenda in both countries are shaped by the EU institutions, as was the case with privacy and data-protection legislation. Consequently, their national AI strategies were designed in an effort to meet the EU's expectations.

The transformation of higher education into an industry-oriented, grant-based system promoted by the EU made it easier for the governments of Hungary and Poland to capture and weaponize EU funds. These are only partially allocated via the ministries responsible for science and education, with the majority allocated by ministries and agencies responsible for the economy and industry. The wages of academics and researchers in Hungary and Poland lag behind the EU average,[14] which, combined with overall low investment in innovation and education, makes it hard to attract and retain talent. Instead of cost- and time-consuming comprehensive reforms, Hungary and Poland used EU funds to establish AI research systems built on handpicked, better-funded research institutions under the auspices of the government, rather than tertiary education institutions. As their startups and small and mid-size AI companies rely heavily on government support for their R&D projects, the consequences of this shift similarly apply to the private AI sector, allowing the governments to tie the funding of companies to political factors. Although the EU has acknowledged the issue of corruption in its approach to Hungary's use of EU funds,[15] similar instances widely publicized in Poland have not yet attracted similar scrutiny.[16]

The approach of Hungary and Poland to AI policy has been in stark contradiction to their governments' political narrative of strategic technological autonomy and digital sovereignty. In both countries it is the large international tech companies that play lead the digital innovations ecosystem. Given the size of both countries' economies, foreign companies are crucial sources of much needed foreign investment and high-quality jobs, which leads to policy and legislative compromises. In the case of AI such close public-private relationships can come at the expense of citizens' rights. In their quest for significant investments and close partnerships with providers of state-of-the-art technologies, Hungary and Poland have been able to provide not only tax relief or direct financial aid, but also indirect support to large businesses by adopting industry arguments in national legislation and promoting them in EU regulation negotiations. While this can beneficial to the countries' economic and technological development, this rarely addresses the interests of vulnerable communities or serves democracy.

Hungary

Hungarian scientists played an important role in the early days of AI research, with names such as the US-emigrant John von Neumann and László Kalmár among the "fathers" of the discipline. The legacy of brilliant mathematicians continued into the modern era through the John von Neumann Computer Society (NJSZT) and other computer science associations. In the late 1980s, Hungary exported a series of software products (PROLOG) to over 25 countries.[17] Due to a lack of substantial funding and to the economic and political instability the country experienced after the fall of communism, it failed to establish itself a leading or regional AI hub. The European

Commission estimated that, in 2020, Hungary spent €84 million on AI, the least among member states except for Bulgaria.[18] In 2023, it ranked 45th in the AI Government Readiness Index.[19] The country's leading AI scientific institution is the Budapest University of Technology and Economics, whose researchers published over 350 AI-related papers in 2022.[20] Hungary has a growing number of AI startups, many of which are focused on innovations in healthcare, transportation, and manufacturing. The increase in recent years in private capital funding of ICT projects has been largely due to foreign investments.[21] As a result of demographic trends, the lack of skilled AI talent is and will remain one of the major challenges of Hungary's AI ecosystem, particularly in the public sector.

AI Strategy

In May 2020, the government presented the Artificial Intelligence Strategy.[22] During the event, Minister of Technology and Industry László Palkovics focused on the potential benefits of AI for industry, while also expressing the intent to introduce "data wallets" as a foundation for a data-driven economy granting citizens more agency and privacy. The ministry coordinated the consultation on the strategy in a process that involved over 250 member organizations of Hungary's AI Coalition and over a thousand experts, most of which represented the interests of international and Hungarian technology companies. The strategy defines sector-specific focus areas, most of which are industry-oriented: manufacturing and autonomous systems, data-driven healthcare, digital agriculture, energy, logistics, and transport. Its first chapters present analyses of the global and regional AI landscape, while the main parts of the document define the roles and responsibilities of different stakeholders (government agencies, research institutions and universities, private companies, CSOs, and international partners). The strategy also lists the main challenges Hungary may encounter in executing its AI action plan, enumerating a mix of technological and societal issues: complexity, ethical dilemmas, social resistance, legal uncertainty, disruptive innovations, national security threats, and international competition. A distinctive feature of the strategy is its approach to national and cultural and linguistic aspects of the AI transformation. The document highlights the lack of high-quality Hungarian-language processing models as a major strategic vulnerability. To address this, it sets research efforts in this area as a priority necessary for the "survival of our language in a digital era".

The AI Coalition, apart from its advisory role in designing and implementing the strategy, is also tasked with raising awareness of AI-related issues and promoting the responsible development and use of the technology. According to some people involved in its workings, several problems undermine its overall legitimacy. First, the voice of nongovernmental organizations was intentionally not adequately represented in the drafting of the strategy, leaving the process in hands of government officials and industry. Second, the lack of funding for Hungarian CSOs and watchdogs—not surprising given the government's general stance against civil society—makes it very difficult for them to monitor the field of digital policies. Third, since engagement in the AI Coalition was not supported with sufficient government funding, over time the number of experts involved in the initiative dwindled. Consequently, the strategy does not address crucial societal and political issues, altogether neglecting human and civil rights perspectives, and focusing instead on issues close to the interests of industry (whether big international companies or local startups).

AI Policies and Public Implementation

Prime Minister Viktor Orbán's control over the political system has resulted in a relatively stable legislative and administrative digital ecosystem in Hungary. Designing and implementing AI-related policies is carried out by several government institutions, with the Ministry of Innovation and Technology responsible for development and execution of the AI strategy as well as for coordinating the activities of other major stakeholders. Funds are directly distributed by the ministry based on the type of projects, with smaller ones at the disposal of the Ministry of Human Resources, which oversees higher education and science sectors.

The implementation of specific policies is delegated to specialized institutions. The National Artificial Intelligence Research and Development Office (NAIIRO) is in charge of coordinating and supporting AI research and development, of providing funding for AI research projects, and of training and education for AI researchers and developers. The National Data Assets Agency (NAVÜ) supervises the collection and management of data assets utilized mainly by businesses and researchers. The National Authority for Data Protection and Freedom of Information (NAIH) handles issues related to data protection. It has begun tackling AI-related cases; for example, it issued fines over the abuse of automated analysis of voice recordings of consumers of a commercial bank in 2022.[23] In 2023, Hungary met the deadline for assigning a body (the National Media and Infocommunications Authority, NMHH) to act as the national Digital Services Coordinator as required by the DSA.

Although implementation of the AI strategy is stifled by bureaucratic and political obstacles, significant R&D policies have been enacted. In the process of consolidation of AI research institutions, two new state-controlled institutions were created. One is MILAB, a consortium of ten research centers, universities, and governmental bodies, coordinated by the Institute for Computer Science and Control (SZTAKI). The other is the National Laboratory for Autonomous Systems (ARNL), a consortium led by the Institute for Computer Science and Control, and including the Budapest University of Technology and the Economics and Széchenyi University of Győr. Both institutions design research agendas, provide funding for scientists, carry out projects, and collaborate with private AI companies. The ARNL, which focuses on driverless cars and drones research, also collaborates with international partners. It is also actively seeking funding and investment from the Chinese tech industry.

Although implementation of the AI strategy is stifled by bureaucratic and political obstacles, significant R&D policies have been enacted.

To accelerate the digital transformation of the economy, the Ministry of Innovation in 2019 established a Digital Welfare Program, which was designed to support financially private, mostly large and medium-sized companies. The Ministry of Economic Development also facilitated the establishment of two AI hubs, one in Zalaegerszeg (ZalaZone) and one in Debrecen. Thanks to public backing, the latter purchased a 100Gbps Komondor supercomputer, which will be used by researchers and startups collaborating with the centers.

Attracting foreign investors, like Genesys for its new R&D Center in Budapest,[24] and acquiring funding for public-private partnership innovation is a priority. In healthcare, the e-stroke platform developed by the British company Brainomix in 2022 was awarded a tender to be installed in state-run hospitals across the country. The diagnostic system automatically monitors and analyzes patient's brain scans, assisting doctors with analysis and treatment recommendations, and allowing them to consult other professionals via a mobile app. Other prominent new AI-related projects include the plans to develop monitoring apps for other health conditions and an automated ambulance service software.[25]

In 2023, the government invested in AI tools designed to bolster its administrative capabilities, purchasing and deploying the automatic reporting and data-processing KNIME system.[26] The Swiss company that developed the system claims that it can facilitate instant data collection and analysis on a large scale, making top-down policy monitoring possible in real time. Public administration has also already faced the risks related to AI's impact on fundamental rights. In 2021, the town of Siófok intended to install a CCTV facial-recognition AI system to monitor public spaces in light of the issue of petty crime. A year later, following a complaint by a privacy advocate who argued that the use of AI facial recognition violates the law, the NAIH ruled that the use of public biometric surveillance was unlawful.[27] This decision is in line with the approach toward biometric AI reflected in the AI Act. However, the ruling does not apply to all use cases of such technologies, with significant exemptions for law-enforcement, intelligence, and border-control agencies.

Hungary's approach to the international dimension of AI development reflects its overall ambiguous orientation in international relations. While remaining on the sidelines throughout the AI Act negotiations, in the end Fidesz members supported the European Parliament version of the act in the plenary vote in June 2023. At the same time Budapest continues to actively purse investments and close scientific collaboration with Chinese and US companies and universities alike.

Poland

In Stanford University's AI 2022 index and AI Vibrancy tool, Poland was 19th among 29 developed countries in terms of the strength of its AI ecosystem.[28] This position was based mainly on the number of publications by and citations of Polish AI researchers. At the same time, Polish private companies lag behind their global competitors in a variety of dimensions ranging from spending to patents and to the number of newly funded companies. According to the State of Polish AI report by Fundacja Digital Poland in 2022, businesses heavily rely on foreign funding and know-how, with nearly 40% deriving a significant portion of their revenue from abroad (mainly the EU and US markets), and with over 60% cooperating with foreign partners.[29] The situation is different in the case of scientific efforts: out of almost 14,000 papers in this field published by Polish authors between 2010 and 2021, 27% were the result of an international collaboration.[30] Only 1.2% of all science, technology, engineering, and mathematics publications by Polish scientists in this period were AI-related, significantly less than is the case not only for the United States (11%) and China (24%), but also Germany (2.9%) and France (2%). In terms of the number of papers, Poland is the fifth-largest source of AI academic output in the EU, largely due to work conducted by its technical universities. These indicators paint the picture of an underdeveloped and

underperforming science-and-research-oriented AI ecosystem that relies heavily on state or EU funding with a dominant presence by international, usually US, private companies.

AI Strategy

The process of designing an AI strategy was launched in 2019, when the Ministry of Digital Affairs presented the first draft of the AI Development Policy in Poland for 2019–2027. The document was then subjected to consultations with experts and interest groups organized by the ministry and the Office of the Prime Minister, before it was adopted by the cabinet and published in September 2020.[31]

The strategy outlines the vision, goals, and actions of the government to foster the growth and innovation of AI in various sectors of the economy and society. It is ostensibly aligned with the Strategy for Responsible Development as well as with the European Commission's Coordinated Plan of AI, and the OECD's AI Principles. The first chapters introduce the concept of AI as well as its potential benefits, challenges, and impact. The vision and objectives set out are to make Poland one of the largest beneficiaries of the data-based economy, to support its AI enterprises and scientific community, to educate and empower citizens with digital skills, to cooperate with international partners on ethical and legal standards, and to use AI to improve public services and administration. The document then describes the current state of AI development in Poland. It also outlines six areas of intervention: AI and—respectively—society, innovative companies, science, education, international cooperation, and the public sector. The fifth chapter specifies the requirements and conditions for the use of AI in Poland, covering all phases from design to deployment, which include ethical principles, the legal framework, technical standards, quality assurance, risk management, transparency, accountability, human oversight, data protection, cybersecurity, and social dialogue. The final chapters describe the roles of various actors involved in AI development and propose a governance model for coordinating and monitoring the implementation of the policy for AI development.

The PiS government also did not fulfill the promise of an open, transparent, and inclusive approach to public consultations on AI-related legislation and polices.

According to the strategy, the Ministry of Digital Affairs is responsible for coordinating the process, and it is also tasked with establishing an intergovernmental team for AI development and regulation, which it has not done fully in practice given the lack of transparency. The ministry was also supposed to set up an advisory council for AI development with representatives from different stakeholders, to organize regular consultations with social partners and experts on AI issues, and to report on the progress and outcomes of the strategy. By the time it left office at the end of 2023, the PiS government had not established such a national-level expert body responsible for coordinating and advising on its AI policies.

The PiS government also did not fulfill the promise of an open, transparent, and inclusive approach to public consultations on AI-related legislation and polices. In an attempt to better engage with the stakeholders

representing the business, academic, and nongovernmental sectors of the emerging AI ecosystem the Ministry of Digital Affairs in 2018 launched a Working Group on AI (Grupa Robocza ds. AI, GRAI). The role of the group was to advise, to provide recommendations, and to suggest new policies to the government by inviting experts from various AI-related fields and professions. Membership is open, yet not transparent—the list of experts and entities involved was not available to the public. This left a lot of room for officials to shape the structure and membership of the GRAI according to arbitrary decisions. Even though some of its members were invited for last-minute consultations on the final draft, their feedback did not significantly impact the official document.

AI Policies and Public Implementation

Poland's approach to AI policies results from the interplay between three main forces: political and international aspirations, pressure from market-oriented interest groups, and the EU's digital agenda. In 2023, Poland ranked 36th in the AI Government Readiness Index.[32] Despite Czechia, Estonia, and Lithuania performing better, Poland is considered an emerging regional AI hub due to the size of its market. A major pillar of the index combines governments' technological capacity and of regulatory, policy, and governance frameworks.

The digitization of public services was a key element in the strategies of successive Polish governments. As part of this policy, the Ministry of Digital Affairs has developed regulations and principles for building digital public services. More crucially, it also provided funding for dependent agencies to develop and execute projects associated with the electronic servicing of citizens.

At the same time, issues related to the digital policies have been widely considered by the public to be primarily of a technical rather than political nature. Consequently, the role of the parliament in making policies has for many years been marginalized, particularly after PiS came to power in 2015. However, due to the silo mentality and political struggles within the governing majority this did not lead to strong, centralized AI governance. In this period, despite AI policies being formally under the auspices of the Ministry of Digital Affairs, the majority of R&D spending was through agencies controlled by other ministries: the Ministry of Science and Higher Education, which is in charge of scientific funding and policy, and the Ministry of Economic Development and Technology, which controls the distribution of the R&D spending through applied research programs, and the Ministry of Development Funds and Regional Policy, which distributes EU cohesion policy funds. To complicate matters further, internal power dynamics within the PiS-led coalition government resulted in frequent changes at the helm of ministries, institutions, and agencies tasked with setting the agenda and R&D funding for AI, leading to a state of permanent political and administrative uncertainty.

According to independent experts and state officials interviewed, the government did not approach the enactment of the strategy seriously. Two and half years after the official launch of the ambitious AI agenda, the government had not started working on legislation or rules for addressing potential threats posed by the use of modern AI systems. The Ministry of Digital Affairs does not keep a registry of all AI or automated systems used in the public sector even though several government agencies have already experimented with introducing such applications.[33] This lack of oversight could be attributed not only to an overall disregard by PiS for transparency, but also to general inefficacy and fragmentation of the executive branch.

After a period of prolonged inactivity, the GRAI was reactivated in 2021 in an effort to engage with and address the needs of the AI sector. Since then, the list of its accomplishments includes launching two websites,[34] organizing a conference in the autumn of 2022, and sporadically publishes on selected AI-related topics. The latter include documents with recommendations for the public sector in areas such as banking and finance or energy. In the summer of 2023, the GRAI launched a portal dedicated to linking AI businesses with potential contractors, but its success is yet to be determined given the insignificant number of companies in the initial database. In August 2023, the GRAI also published a report on legal issues related to the implementation of the AI Act.[35] The document, which clearly states that it does not represent the position of the government, focuses on areas such as law enforcement, the financial sector, and the intersection between AI and medical-products regulations. However, the authors relied on the European Commission's 2021 proposal and, hence, the report does not address many of the most pressing issues that emerged during the legislative process. Topics covered in the publication center around the challenges posed by AI to fundamental rights, such as in the use of the technology by law-enforcement, border-control, and intelligence agencies. As the Ministry of Digital Affairs, which supervises the GRAI, did not involve high-level representatives from other ministries responsible for public and national security or the justice system, the importance of the report and the workings of the GRAI in these areas are questionable.

Academics, lawyers, and representatives of the nongovernmental sector who at some point joined or engaged with various subgroups have criticized the way that the GRAI operated. Their work was not compensated, which over time led to a drop in membership and to overrepresentation of government officials and private-sector professionals. In October 2023, the GRAI was reactivated by the Ministry of Digital Affairs yet again; however, with the change in government at the end of 2023, this reactivation was eventually dropped.

When it comes to the milestones set in the AI strategy, the results have also so far been disappointing.

When it comes to the milestones set in the AI strategy, the results have also so far been disappointing. Despite having successfully established eleven regional Digital Innovation Hubs (with half of the funding coming from the EU), many of the most ambitious goals such as the development of data trusts or AI codes of conducts have not been achieved. For instance, the Virtual Research Institute, designed to become one of the sources of funding for advanced projects, has failed to produce AI programs. The government has also missed the EU deadlines for an assigning an agency to be the regulator of the AI market as required by the DSA. Meanwhile, institutions independent from the Ministry of Digital Affairs have been given resources to carry out their own AI policies, with the National Centre for Research and Development (NCBR) being the most prominent one. This center, which is tasked with providing resources to and setting the agenda for Polish innovators has funded its own AI body, IDEAS NCBR, with a mission to focus on applied research and to scout for top-tier foreign AI students and experts. So far IDEAS NCBR has managed to attract top AI talents and to carry out projects in collaboration with public and private institutions. However, as it is supervised and funded by Ministry of Development Funds and Regional Policy, it is independent from the AI policies executed by the Ministry of Digital Affairs and the Ministry of Education and Science.

Poland's AI ambitions have also suffered from political and legal instability and from illiberal state-capture. An audit by the Supreme Audit Office audit of the NCBR's effectiveness in providing funding for Polish companies paints a bleak picture of the country's innovation ecosystem.[36] After analyzing over 400 projects, of which almost 120 were selected for funding of over €200 million in total, its authors raised the alarm about a high probability of fraud and corruption as well as of illegality in decision-making.

Poland's AI ambitions have also suffered from political and legal instability and from illiberal state-capture.

Poland's shortcomings in A governance cannot be fully explained by the lack of technical and financial capabilities. While it has not been able to utilize the benefits of recent progress in AI, the country has a successful track record of automation and digitalization of essential public services based on less advanced ICT solutions. The latter include the creation of the ePUAP e-administration platform (which gathers citizen's administrative data) and the mobile app mObywatel (a digital depository equivalent to physical documents). Another example is the Central Tax Authority (KAS), which, as early as 2018, introduced automatic-decision-making tools that allowed the government to significantly increase overall tax revenues.

Simultaneously, there are few successful governmental projects that require development and implementation of advanced AI techniques. For example, the KAS's 2021–2024 strategy only mentions its plans to introduce powerful AI models designed to fight tax avoidance in the future.[37] Even the launch of large language models (LLMs or foundation models like GPT3) and the global AI hype that this unleashed did not significantly impact Poland's AI strategy or policies. It took over half a year after the launch of ChatGPT for the government to even address the issue. The response was far from impressive. The Ministry of Justice to announced it would start to design and introduce new AI-powered tools in the justice system that would allow judges to use AI assistants (not unexpectedly, given that judges have been assigned cases by a computer-mediated system since 2018),[38] while the Ministry of Education published short guidelines for teachers explaining the potential and risks of utilizing ChatGPT for teachers and students.[39] Statements published on government websites clarified that AI is to be utilized mainly for preliminary legal analysis systems so as to reduce courts being overburdened with cases, which is a long-standing problem. According to unofficial sources, by mid-2023 the Ministry of Justice was also investigating potential legal and technical means to obtain AI tools for use in the administration of the judicial system as well as other related purposes.

Supposedly the biggest success in the field of innovative, powerful AI models came from a consortium of NASK Research Institute and the Centre for Networking and Supercomputing at the Wrocław Technical University. In November 2023, it announced the launch of PLLuM, the first LLM model trained on datasets built upon sources in Polish.[40] As it turned out, the model is not at the stage of technological maturity, which suggests that the announcement had more to do with public relations than with scientific and engineering breakthroughs, not to mention the lack of a detailed plan for future implementation within the public sector.

Besides PLuMM, the urge to utilize AI tools in the public sector has in the last years been limited to the introduction by a few ministries of AI-powered virtual assistants instead of call-center services and automated

fraud-detection software. Among the state-funded research projects implementing AI solutions for public security the most prominent ones include systems capable of detecting child sexual abuse materials[41] and models used by the police for predictive assessing of probability of future crimes.[42] Again, it is impossible to assess these projects given they are in the early stages of development.

Poland did not significantly contribute to the AI Act negotiations. Its position on major issues was not communicated to the public. In informal discussions, high-ranking officials involved in the process expressed contradictory opinions on the matter. While government representatives working on the issue expressed general support for the act,[43] in July 2023 the minister of digital affairs criticized the very idea of passing the act as it would in his opinion stifle European innovators and hinder international competition.[44] This lack of a cohesive approach also manifested itself when PiS members voted in favor of the version of the act that is more oriented to fundamental rights in the European Parliament in June 2023 while at the same time the government supported the less strict and more government-friendly version proposed by the European Council. According to unofficial sources, in the European Council meetings Poland supported the national security exemption that would allow intelligence services and other law-enforcement agencies involved in national security to be excluded from the scope of the act.

Implications of the EU's AI Regulatory Model

The EU's new regulatory model and agenda will have a fundamental impact on AI governance, particularly for the governments in Central and Eastern Europe with little experience in digital markets regulation, including Hungary and Poland. As in the cases of the Digital Services Act and the Digital Markets Act, the AI Act will operate on the principle of a single, overarching EU regulatory framework. Once it comes into full force, the European Commission, within which the new AI Office will sit, will have a broad mandate to oversee providers and deployers of (particularly powerful and available internationally) AI systems. The European Commission will also set up norms and guidelines for national authorities to follow, as well as having a final say in deciding upon complicated administrative cases.

The AI Act will establish a system that divides the oversight over the sector between the EU and national authorities, the latter overseeing smaller AI systems. Given how transnational business models dominate in the digital innovations ecosystem, this will leave the member states with only limited control over the actual market. A similar framework was put in place by the DSA, which, among other issues, regulates the use of AI recommendation algorithms on online platforms. The much needed centralization of regulatory oversight of the single digital market has so far has been stifled by some member states, including Poland, that have not managed to meet the deadlines for the establishment of competent national authorities and Digital Services Coordinators. The same could be expected in the case of the AI Act, especially given that the European Commission will be in charge simultaneously of developing detailed guidelines, templates, and instructions. These will be essential not only for the AI companies but also for the member states in preparing institutional settings for the implementation of the act.

Apart from the AI Act and the DSA, leading AI market actors will have to also conform to other EU regulations. Providers and deployers of models trained on or accessing personal data will continue to be supervised by data-protection agencies. From the perspective of democratic principles the EU's body of privacy legislation (the GDPR, the e-privacy directive, the law-enforcement privacy directive) will be the most impactful, and the GDPR and the AI Act will function together as a primary regulatory regime for the public- and private-sector providers and deployers of systems that affect people's privacy. Additionally, online platforms using AI products will have to follow the DSA, and large online companies will fall under the rules set by the DMA. Moreover, many products with an AI component will also fall under specific sectoral regulations, such as those for the automotive, energy, and health sectors.

AI Systems in Security and Law Enforcement

During the legislative process for the AI Act, the use of AI systems and models by intelligence, law-enforcement, and migration agencies were core issues of debate. Even though the AI Act will play a crucial role in the EU's digital regulatory framework, it will not affect all areas of AI development and implementation equally, which has led some experts to characterize it as "deregulation in disguise".[45] CSOs repeatedly warned about the act lacking strong rule-of-law safeguards, particularly in the context of public security and migration control.[46] On top of that, leaving national security out of the scope of the act will allow the likes of intelligence agencies, the police, and prosecutors not to follow the AI Act in its entirety whenever a government considers a use case to be of high importance to the state's security. This exemption will leave any related abuse of AI by member-state governments subject to regular human rights litigation, which has proven to be ineffective.

The situation for fundamental rights protections in public security and migration control (see also below) will be more nuanced. The member states will have a central role, but the AI Office will technically have the power to curtail certain practices. However, this will depend on a complicated system of legal and administrative measures, so it is likely that in practice marginalized groups and vulnerable individuals (such as migrants, the political opposition, and ethnic or cultural minorities) will struggle to benefit from the safeguards formally granted to them by the AI Act.

In the cases of Hungary and Poland, the lack of functioning democratic oversight of the police, migration services, and intelligence agencies will enable governments to utilize new AI tools without effective legal measures to mitigate or limit their impact on human, civic, and democratic rights. According to official records, the number of people under police surveillance in Hungary[47] and Poland[48] has so far been relatively limited. At the same time, in the vast majority of cases the courts comply with requests by law-enforcement bodies to authorize surveillance, making judicial control a question of formal rather than actual oversight and legal protection.

The relatively low number of cases could be attributed to the lack of technical and human resources at the disposal of the law-enforcement bodies. However, this will change with the rapid growth and availability of AI platforms such Palantir Gotham and Clearview AI, which will allow the authorities to test the limits to the scope of automated surveillance operations. In Central and Eastern Europe, this process has already begun. In 2022, Czechia's police covertly introduced an AI biometric system connected to the personal data of citizens and other Central and

Eastern European countries are likely to follow suit.[49] The case of the use of the Pegasus spyware to target opposition figures and activists is a warning sign of the perils of an emerging, AI-powered state security apparatus.

In a context of assaults on the rule of law and the independence of the judiciary, as in the case of the Fidesz and PiS governments, citizens targeted by the state's security apparatus for political reasons could not expect access to fair trials. Moreover, in light of the European Commission's push for mandatory, real-time monitoring of child sexual abuse materials shared via online platforms and messaging apps (the anti-child abuse regulation), governments are likely to try to extend the range and depth of automated surveillance to other types of crimes or otherwise suspect activities. This problem is exacerbated by the fact that the EU directive for the control of exports, brokering, technical assistance, transit, and transfer of dual-use items does not cover exports between member states.

AI in Migration Control

Currently developed AI systems can also provide governments with more effective tools for migration policy. Fidesz and PiS used the influx of refugees and migrants to Hungary and Poland in recent years as an opportunity to build their electoral platforms in stark opposition to immigration as well as the EU's alleged soft approach to migration policies. The EU institutions are already funding the development of such systems, which are expected to be used primarily by the agencies responsible for monitoring the external EU borders by he European Border and Coast Guard Agency (Frontex).[50] The authorization of AI in migration control as well as a general EU's acceptance of this policy direction, reflected in the European Commission R&D funding agenda, could further incentivize states to embrace and weaponize such methods, allowing Fidesz in Hungary and, possibly to a lesser extent, the new government in Poland to use AI on a wide scale to control the borders and surveil foreign residents.

Technically, the AI Act provides EU and non-EU citizens with equal protection of their fundamental rights. However, the EU institutions and the member states will be allowed for security purposes to use high-risk AI systems designed to identify people based on biometric characteristics or to recognize emotions, additionally granting law enforcement authorities exemptions from certain transparency obligations. Due to the complexity of the Act and the financial, logistical, linguistic, and legal obstacles migrants and refugees from outside the EU face, in practice they are not likely to have equal access to the legal remedies granted to them by the AI Act unless governments do not provide them with dedicated programs and assistance.

Automation of Public Administration

The rise in interest in AI products and services, as well as the passing of the AI Act, will soon lead to a wider adoption of the technology in public administration. Such tools allow institutions to reduce costs and time of processes, sometimes drastically. AI tools are becoming increasingly adept at recognizing patterns, faces, objects, and situations; at acquiring and processing information; at estimating risk; and at managing decision-making processes. This gives the state the opportunity to take actions that were previously either impossible or required too much human and financial investment—notably in the security and law-enforcement sectors. Due to their efficacy, AI systems can be utilized to implement policies—such as in the fiscal, judiciary, and

administrative spheres—on a scale that would until recently have been considered controversial, invasive, or outright authoritarian.

In the case of Hungary and Poland, this will take place in a context in which government databases containing information about citizens are already almost entirely digitized. These can be utilized to enhance the administrative powers of the state as input data for AI models. Experts interviewed pointed out that there is wide, bipartisan public support for automation of procedures in public administration in Hungary and Poland. Apart from the benefits, this process generates new legal, technological, and societal risks. For instance, mass implementation of AI in the public services can lead to the digital exclusion of senior citizens (the fastest-growing demographic cohort in Central and Eastern Europe) struggling to adapt to new forms of citizen-government interactions (such as chatbots or AI interfaces). Furthermore, the Fidesz and PiS governments repeatedly showed that even basic state functions can be weaponized against political, societal, or market actors they regarded as opponents. The potential use of official government databases for political purposes constitutes an even bigger threat. Some cases of illegal weaponization of such information have already been reported. For example, in August 2023, Poland's health minister was sacked when it became clear that he or his subordinates had violated patient-doctor confidentiality by unlawfully accessing and leaking sensitive, personal information from the national digital medical database of a doctor who had publicly criticized the ministry. With an increasing number of public services digitized and accessible online, the risk of sensitive data being used against citizens will be ever present; thus, adequate policies addressing the issue could include not just legal (consequences for public officials unlawfully using personal information), but also technical (interconnected ICT systems precisely monitoring access to databases) solutions.

AI and Democracy

The wide adoption of AI systems in the public sector increases the risk of personal data being intentionally utilized for political purposes. In illiberal systems this can threaten the freedom and fairness of elections irrespective of whether such tactics are deployed illegally or within the parameters of existing regulatory framework. PiS followed Fidesz's example in reshaping the Polish media by taking over public and private media institutions.[51] By doing so, besides limiting media pluralism and independent journalism, both gained access to extensive digital databases of consumers of information, which allowed them to use their media ecosystem to push mass-scale political propaganda through digital channels. Given that modern political campaigns operate largely via large online platforms such as Facebook, X, Instagram, and Tik Tok, and given their control over public-sector institutions and their marketing budgets, this has provided them with a huge advantage over their political opponents.

The 2023 parliamentary elections campaign in Poland should be regarded as a test case of such practices. For the first time, PiS focused its outreach on the digital media, particularly Youtube ads and sponsored videos. During the last phase of the campaign, the platform was flooded with PiS videos and content, which at one point reached over 120 million views via online social media platforms in a single week.[52] The unlawful use of the personal data of citizens for political purposes was claimed during the campaign by the former commissioner for human rights and democratic opposition candidate Adam Bodnar (who became the minister of justice after the elections),[53] but this has not been substantiated so far.

Even more disturbing is the potential for state-controlled institutions to use government-held personal data of citizens in wide-ranging ways as input data for AI systems (particularly powerful general-purpose models like GPT) in the future. With access to large amounts of data, such systems can help to categorize, profile, and target voters based on their—for example—health, financial, criminal record, biometric traits, or psychological vulnerabilities. Combined with the state's control over the national media landscape and the growing role of recommendation algorithms on social media, illiberal governments will have access to tools for electoral campaigning that are unprecedented in terms of scale, precision, and efficacy.[54] Some aspects of the problem could be mitigated through the EU's new political advertising regulation, which lays down rules for transparency and accountability of paid political ads. The European Commission and the European Parliament reached a provisional agreement on this regulation in December 2023.[55] However, it remains to be seen how effective the new rules will prove to be.

AI R&D and Economic Policies

Apart from introducing new obligations for developers of certain AI models and systems, the AI Act will have no direct impact on the EU's scientific agenda or industry policies. The European Commission will continue to set general developmental goals for the development of AI in Europe, but the limits in EU funding mean that most of the policies designed to incentivize and scale up AI companies will be decided by national governments.

For Hungary, the most plausible scenario is a continuation of the direction presented in its AI strategy with its heavy focus on the industry, close collaboration with Chinese investors, as well as efforts to protect the Hungarian language and heritage from the perils of AI-fuelled globalization. The main uncertainty concerns the outcome of the EU's legal measures with regard to accusations of corruption in the allocation and use of EU funds by the government. In the worst-case scenario, the EU's application of conditionality resulting in the freezing of cohesion funds could deprive Hungarian AI companies of an important source of investment.

Poland's AI ecosystem will undergo significant transformation and the oversight of the public sector will be divided among ministries headed by members of one of the four parties in the new coalition government. As a result, the government's AI policy will be executed in parallel by various political forces and their subordinate institutions. The Ministry of Digital Affairs will play a significant role in coordinating these actions, and its importance will be strengthened by the fact that the new minister is also a deputy prime minister. The Ministry of Science and Higher Education, which is also important for AI policy, is now led by a politician from the same party in the coalition government, which increases the chances of executing more coordinated policies. The change in government may also result in more openness to introducing regulations protecting citizens' rights, which will be facilitated by the fact that the Ministry of Justice and the Ministry of Interior, which oversee, among others, the police, the border guard, and the intelligence agencies are led by politicians from the same party. Neverthelesss, the nature of the four-party coalition government poses a serious risk associated with the fragmentation of public institution actions. The potential lack of a coherent strategy in the public sector may negatively affect Polish companies and scientists as they apply for funding distributed by many institutions in parallel.

Conclusion

In recent years, Hungary and Poland have embarked on AI policies that bear striking similarities. In both countries, the government has primarily addressed the challenges and demands of the industry, relegating societal consultations to mere public-relations exercises. The legislative efforts at the national and European levels lacked transparency and inclusivity, failing to adequately represent groups advocating for the common good or marginalized communities. Poland and Hungary have been navigating EU and national law, combining the rhetoric of digital sovereignty and the subordination of public policies to the expectations of large foreign corporations. In government, Fidesz and PiS have also largely disregarded the scientific community's needs, opting instead to establish and to reinforce a parallel institutional system largely subservient to their interests. This approach has hurt the functioning of research funding institutions, leading to an increase in corruption, nepotism, and misuse of EU funds in both countries. There is also scant evidence that Russia's invasion of Ukraine has prompted a shift in thinking about the military applications of new technologies.

Despite these parallels, there are also notable differences between Hungary and Poland. These are evident, for instance, in their respective relations with China. Under US pressure, Poland is gradually moving away from allowing Chinese companies to participate in strategic programs and to influence legislation. In contrast, Hungary's government continues to foster closer ties with Beijing despite explicit warnings from NATO. Acting against the policy of technological "decoupling" (in AI but also in, for example, microchips and cloud technologies) from China adopted by NATO[56] and the United States, the Fidesz government allows Chinese agencies and companies to play a pivotal role as scientific partners and investors in private companies and public institutions alike. In the context of Russia's war against Ukraine this further undermines Hungary's credibility as a member of NATO, and it can potentially weaken the alliance's cybersecurity resilience architecture.

The outcomes of the enacted policies in Hungary and Poland have also varied, and the centralization of control over public-sector AI institutions yielded different results. While Budapest has managed to establish a relatively cohesive and stable governance system, Poland has seen further fragmentation and a deepening of administrative chaos. The field of AI in Poland has been subjected to various government agendas at the same time, which has led to a lack of coordination in investments and regulatory oversight. Consequently, despite it having significantly greater financial resources than Hungary, the country's top scientists and engineers working on AI systems do so for companies like Google or OpenAI, rather than contributing to the public sector or start-ups with prospects for global expansion.

From the perspective of democratic values and human rights, the systems in Hungary and Poland fail to guarantee sufficient legal protection for citizens. The political takeover of the justice system and the partisan control of law-enforcement institutions, coupled with attacks on civil society, have resulted in individuals whose rights have been violated as a result of actions involving computer and information systems being unable to get swift, efficient, and fair hearing from state institutions. Worse still, the growing use of AI in election campaigns, in the absence of democratic oversight, means that the risk of mass disinformation campaigns and electoral manipulation is greater than ever.

As a result of the recent change of government in Poland, the two countries are now facing different AI development scenarios. While in Hungary one can expect a continuation of the strategy that has been pursued in the past years, Poland now has the opportunity to carry out major structural reforms to the AI sector governance model. The high political rank of the minister of digitization, who is also a deputy prime minister, makes it possible to undertake actions for the coordination of state policy in investment and regulation.

The EU'S AI Act may have positive effects for the rule of law and the protection of individual rights. Unfortunately, the many potential loopholes in its agreed version will make it easy for governments to deploy AI systems in sensitive areas such as public and national security, migration control, and the judiciary. The AI Act will thus not be a silver bullet against the risks associated with an unlawful deployment of advanced autonomous systems at the expense of society and democracy. At the same time, the fight for aligning AI with liberal values and human-centered ethics will continue in other areas such as national law, other EU regulations, and international treaties.

Recommendations

Adequate Funding and Consolidation of AI Agendas

Compared to its US and Chinese counterparts, the EU's AI sector suffers from insufficient public and private funding. The systemic problem of fragmentation of R&D investments among member states, combined with post-Covid-19 economic woes, makes it difficult for EU innovators to successfully compete with the global leaders. In the case of Hungary and Poland, their AI ecosystems have also been stifled by the state capture by illiberal parties. The political takeover of agencies responsible for R&D funding in both countries resulted in a drift toward structural corruption and nepotism, which disincentivized law-abiding (particularly, reluctant to bribe) private-sector actors from accessing the EU funding via state agencies has made the problem even worse.

These challenges could be combatted by a policy mix that involves the supply side and regulatory oversight. Most obviously, there is the need for a radical increase in funding available to European AI companies. The €1 billion assigned for that purpose anually until 2030 in the EU budget is not ambitious enough considering the needs and potential of the EU information and communications technology sector. However, money alone will not solve other pressing issues related to the fragmentation of the European AI ecosystem. The problem could be tackled by giving the AI Office, in addition to its executive and advisory role within the European Commission, the mandate to participate in the distribution of funding for the most promising AI projects developed by EU companies. Sharing funding responsibilities with existing EU's R&D programs (such as Horizon Europe) and utilizing the data and resources it acquires as the regulator of the AI ecosystem could be crucial in selecting and helping EU companies to expand their market base on a European and global scale while also following the new legal and ethical principles and norms that constitute the "human-centered" approach to AI that the EU claims to have taken.

This additional role for the AI Office could also guarantee high levels of legal and ethical diligence on the part of companies joining its programs, linking access to significant funds with them following the AI Act's fundamental rights and democracy-protection mechanisms as well the technical standards, codes of conduct, and other norms of the EU's emerging AI regulatory framework. However, this would also require the EU institutions to critically reassess their own funding and research agendas. The case of the controversial R&D agenda pursued by Frontex, which according to its critics[57] has not followed the legal and ethical principles of the EU's official approach[58] to the use of AI in migration policy is an example of the possible legal and political inconsistencies in that regard. Apart from being in line with the core EU values, the shift in policies suggested above could also set a good example for non-EU competitors. By proving that commercial success can be achieved without legitimizing large-scale infringements of the rights of individuals and of democratic values, the EU could convincingly position itself as a global leader in the safe, lawful, reliable, and democratically aligned development and application of AI-based technologies.

Resources for Enforcing the AI Act

The successful enforcement of the AI Act will depend on providing the European Commission and the AI Office with resources adequate to the task. Given the skepticism toward the act expressed in the European Council's general approach as well as the budgetary constraints of the EU institutions, the EU's AI regulators will likely have to work with little time and limited funding, which will not allow them to handle a large number of administrative cases at a time. According to the 2024 EU budget,[59] the bodies tasked with supervising the digital markets will have to take on new responsibilities with an annual budget increase of less than 5%. As this barely matches the inflation rate in the eurozone, they can be expected to struggle to handle the enforcement of DSA and DMA, not to mention the preparatory-phase obligations that the European Commission will have to fulfill before the AI Act comes into force.

In Hungary and Poland the new regulatory regime will require not only the implementation of the AI Act into the national legal systems but also, more importantly, establishing a new institutional setting. Public-sector institutions will have to adapt to the new technological and legal challenges in little over a year's time. As the entire AI sector will be subject to oversight by several international and public institutions, small and medium-sized enterprises (SMEs) might face difficulties in trying to fulfill their new obligations. And these institutions will not be able to build up the technical and administrative capacity required to supervise and control the market without the EU or the state allocating adequate funds for AI compliance.

From the point of view of private-sector actors, this could lead to a high level of uncertainty and disincentivize investors from supporting more ambitious projects. Moreover, the new EU rules will lead to an additional financial burden for SMEs. Without dedicating new funds and programs to cover the expenditure for algorithm audits and legal compliance some, particularly small start-ups, will struggle even more to keep up with their non-EU competitors.

Empowering CSOs and Institutionalizing the Voice of Societal Stakeholders

Addressing the growing asymmetry between the state and large online platforms on one side and society on the other requires a systemic approach. Thanks to the media hype that followed the launch of ChatGPT, the safety,

legal, economic, and ethical concerns over the impact of AI on society have entered the public debate. After successful advocacy campaigns carried out by a coalition of several European CSOs (including the European Consumer Organisation, the Digital Rights Network, Access Now, the European Center for Not-for-Profit Law, and Amnesty International) that called for the introduction of certain fundamental rights provisions in the AI Act (such as an individual and collective right to redress against AI-mediated decisions), all EU citizens and consumers will have legal avenues with regard to the actions of private- and public-sector deployers of AI systems.

In Hungary and Poland this would be particularly valuable for marginalized groups and political opposition actors. However, after years of being subjected to administrative, financial, and political attacks by the government, CSOs in Hungary and, to a lesser extent, Poland are not prepared to face the new threats to fundamental and human rights posed by a possible rushed and uncoordinated large-scale adoption of AI. In both countries, as in the rest of Central and Eastern Europe, the number of independent watchdogs and activists for human rights in digital spaces is low, and the established CSOs lack programs and staff specialized in that field; therefore, civil society will struggle to effectively utilize the new administrative and judicial measures.

To make the new regulatory system work, the EU and member-state governments should provide CSOs, consumer-protection agencies, trade unions, and other relevant societal stakeholders with funding and resources to develop the legal know-how and networking capabilities necessary for exercising the rights to redress and to access to due process in the future cases before the AI Office and national AI authorities. The EU could also make efforts to institutionalize the voice of people affected by AI systems. The representatives of vital societal stakeholders—including children, people with disabilities, migrants, and other vulnerable communities—in the advisory forum to a new European Artificial Intelligence Board will be selected by the board itself, which will consist of member-state representatives. This will leave the European Commission with little direct impact on the ultimate role of CSOs in the EU's AI regulatory model. In order to address the issues of democratic rights and inclusiveness, it should therefore not only implement fundamental rights-oriented policies but also engage with human and civil rights and AI experts during the process of establishing and later overseeing the work of the AI Office.

Addressing the National and Public Security and Migration Loopholes

Even though the agreed version of the AI Act addresses the challenges of AI better than the original draft, it nonetheless leaves member-state governments with legal maneuvering room to weaponize AI systems against people. The Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence issued by President Joe Biden in the United States in October 2023 introduces administrative and judicial oversight of how autonomous systems and software are deployed by the military and intelligence community.[60] Conversely, the AI Act does not cover areas of strategic importance such as science, research, defense, and national security, leaving considerable leeway for the state, and it makes exceptions for public security and migration control.

It will be difficult to tackle the challenges that come with these loopholes. To preempt the negative societal and political impacts, the European Parliament or the European Commission could launch additional policy measures to address potential civic and human rights violations in public security or migration related to automated digital systems, for instance by not providing research funding for projects that pose risks to democratic values. The EU

institutions can also build on already existing mechanisms and frameworks, such as EUROPOL's Accountability Principles for AI,[61] or the Fundamental Rights Agency's reports on AI and fundamental rights.[62]

Ultimately, it will be up to the member states whether to conform to the new EU rules or to game them by intentional negligence or by adopting inefficient, cumbersome, and nontransparent or otherwise exclusionary ways of deploying prohibited and high risk AI systems in public security and migration. To prevent further divergence of member-state policies affecting fundamental rights related to the use of AI systems in these two areas, the European Commission could provide—either via the AI Office or in a collaboration with the European Union Agency for Fundamental Rights, or the European Data Protection Supervisor—CSOs with materials, know how, and funding for national-level policy and legislation advocacy as well as for public awareness campaigns.

The EU institutions could also assist national authorities and civil society in designing and funding parallel national measures (regulation, guidelines, training etc.) for regulating the use of AI in defense and national security, aligned with standards set by the AI Act. Such assistance could facilitate some synchronization of policies within the EU without undermining the prerogatives of member states. In Poland CSOs have already started to develop tools and methods addressing these issues,[63] but these efforts were met with a lack of interest on the part of the PiS government. Alternatively, the EU could support efforts undertaken by the United Nations; however, the differences between the EU and UN legal regimes and the lack of adequate enforcement mechanisms on part of the latter make it a distant possibility.

A More Inclusive and Transparent Regulatory System

In Hungary and Poland the initiatives involving various stakeholders in AI governance have not been transparent or accessible for the media, CSOs, or other representatives of citizens or consumers. New methods of multi-stakeholder consultations should be developed with regard to digitalization and the introduction of advanced algorithms in public administration. In both countries the AI stakeholders engaged in the process, besides representatives of industry and academia, should also include representatives of CSOs, consumers, patients, workers, and vulnerable communities.

New standards of transparency and accountability obligations for public institutions (and the entities acting on their behalf) that deploy AI with the potential to affect the rights of people should also be introduced. Even when not directly obliged by the AI Act (for instance, software that uses sensitive personal data, but does not technically qualify as a high risk system), public institutional deployers of AI systems that could pose potential threats to people and society could be required to register them in publicly available databases alongside information necessary to evaluate potential risks (personal data and fundamental risk impact assessments and other relevant technical documentation). In line with the precautionary principle, new rules, guidelines, and standards for the use of high-risk AI models and programs by law-enforcement, migration, asylum, and intelligence agencies should be developed and enacted prior to their deployment. This should be done in dialogue with experts and CSOs, and enacted via national legislation even if the AI Act does not make it mandatory under EU law.

Endnotes

1 Organisation for Economic Co-operation and Development (OECD), AI Principles, 2023.

2 Kate Saslow, Understanding US Federal AI Policy: recommitting to a transatlantic coalition on AI, Stiftung Neue Verantwortung, 2020.

3 State Council of the People's Republic of China, New Generation Artificial Intelligence Development Plan, 2017.

4 European Commission, Coordinated Plan on Artificial Intelligence, 2018.

5 OECD.AI Policy Observatory, Policies, data and analysis for trustworthy artificial intelligence, 2021.

6 European Commission, Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence, April 21, 2021.

7 European Commission, Proposal for a Regulation laying down harmonised rules on artificial intelligence, April 21, 2021.

8 An EU Artificial Intelligence Act for Fundamental—A Civil Society Statement, November 30, 2021.

9 Regulation (EU) 2018/1806 of the European Parliament and of the Council of 14 November 2018 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement (codification).

10 Tatjana Evas et al, AI Watch: Estimating AI investments in the European Union, European Commission, 2022.

11 OECD data portal, Gross domestic spending on R&D, 2023.

12 Marta Daroń and Monika Górska, "Enterprises development in context of artificial intelligence usage in main processes", Procedia Computer Science, vol. 225, 2023.

13 James Foreman-Peck and Peng Zhou, "R&D subsidies and productivity in eastern European countries", Economic Systems, vol. 46, issue 2, 2022.

14 European Commission, National Education Systems, 2023.

15 Nicholas Watson, "Hungary tops list of investigations into misuse of EU funds in 2022", Balkan Insight, June 6, 2023.

16 Zosia Wanat, "How a corruption scandal has left dozens of Polish startups facing bankruptcy", Sifted, April 18, 2023.

17 Edit Sántáné-Tóth, Artificial Intelligence in Hungary—the first 20 years, Eötvös Loránd University, 2006.

18 European Commission Joint Research Centre, AI Watch: Estimating AI Investments in the European Union, May 23, 2022.

19 Oxford Insights, 2023 Government AI Readiness Index, 2023.

20 Ibid.

21 EY Hungary, Venture Capital and Private Equity Update 2022, 2022.

22 Ministry of Innovation and Technology, Hungary, Hungary's Artificial Intelligence Strategy, 2020.

23 CMS Law-Now, "Hungary data authority issues heavy fine for the use of AI voice recording analysis", April 7, 2022.

24 Veronica Silva Cusi, Genesys Opens New R&D Centre in Budapest, Further Strengthening its Investment in Hungary, ContactCenterWorld, November 14, 2023.

25 Monika Kiss and Balázs Széchy, Hungary's National Recovery and Resilience Plan, European Parliament Next Generation EU Monitoring Service, April 2023.

26 KNIME, How the Hungarian Government automated reporting processes, 2021.

27 Data Guidance, Hungary: NAIH declares public biometric surveillance unlawful, fines Techno-Tel HUF 500,0000, March 21, 2022.

28 Stanford University, Artificial Intelligence Index Report 2022, 2022.

29 Fundacja Digital Poland, State of Polish AI, 2022.

30 Sztuczna inteligencja: osiągnięcia publikacyjne z zakresu nauk ścisłych i technicznych w latach 2010–2021 [Artificial Intelligence: STEM publications 2010-2021], National Information Processing Institute, 2023.

31 Council of Ministers of the Republic of Poland, Policy for the Development of Artificial Intelligence in Poland, 2020.

32 Oxford Insights, 2023 Government AI Readiness Index, 2023.

33 Katarzyna Wójcik, "AI pomaga rozwiązywać sprawy w urzędach", [AI can help with administrative matters], Rzeczpospolita, May 18, 2023.
34 Council of Ministers of the Republic of Poland, AI Portal.
35 Council of Ministers of the Republic of Poland, Analysis of the relationship of the Act on art intelligence with selected and proposed regulations legislation, 2023.
36 Supreme Audit Office, NCBR – miliardy rozdane, innowacyjności brak [NCBR: funding programs did not result in innovation], October 13, 2023.
37 Central Tax Authority (KAS), Kierunki działania i rozwoju KAS na lata 2021-2024 [Policy and development goals of KAS, 2021-2024], 2020.
38 Ministry of Justice, Poland, Sztuczna inteligencja w służbie wymiaru sprawiedliwości – konferencja Ministerstwa Sprawiedliwości [Artificial Intelligence in the criminal justice system - Ministry of Justice's conference], April 17, 2023.
39 Ministry of Education and Science, Poland, Chat GPT w szkole. Szanse i zagrożenia [Chat GPT in school. Potentials and risks], July 31, 2023.
40 NASK, Powstanie pierwszy polski duży model językowy PLLuM [PLLuM: the first Polish large language model to be created], 2023
41 NASK, Projekt Apakt, 2023.
42 MIM Solutions, Predictive policing system for forecasting crimes created for the Polish Police, 2023.
43 Sejm, Parliament's session (21-07-2021) transcript, 2021.
44 Anna Wittenberg, "Zaczyna się wyścig o AI."[The AI race begins], DGP July 1, 2023.
45 Aida Ponce Del Castillo, The AI Act: deregulation in disguise, Social Europe, December 11, 2023.
46 Open letter: The AI Act Must Protect the Rule of Law, 2023.
47 XpatLoop, "2,645 People Under Surveillance by Secret Services in Hungary Since 2010", June 14, 2023.
48 Rzeczpospolita, "Policja rzadziej podsłuchuje" [Less police surveilance], July 13, 2023.
49 IuRe, "Czech police use facial recognition system, IuRe finds out details", EDRi, September 27, 2023.
50 European Commission, Intelligent Portable Border Control System, 2021.
51 Filip Konopczyński, "Digital Empire in the Making", Visegrad Insight, January 12, 2021.
52 Krzysztof Izdebski et al, Obraz kampanii w mediach społecznościowych Raport IV [Electoral campaign in social media: The Report vol. 4], Fundacja Batorego, 2023.
53 Agnieszka Jędrzejczyk, "Czy wybory są jeszcze tajne, skoro trzeba publicznie odmówić udziału w referendum?," [Is the ballot still secret, if one has to publicly refuse to vote in the referendum?] OKO.press, August 16, 2023.
54 Filip Konopczyński, "Czy sztuczna inteligencja może wpłynąć na wynik jesiennych wyborów" [How AI can affect the elections in the fall], Onet, August 26, 2023.
55 European Council, Transparency and targeting of political advertising: EU co-legislators strike deal on new regulation, November 7, 2023.
56 NATO Parliamentary Assembly, The rise of China: implications for global and Euro-Atlantic security, 2020.
57 Lucie Audibert, "Ban racist and lethal AI from Europe's borders", AL Jazeera, April 20 2023.
58 European Parliamentary Research Service, Artificial intelligence at EU borders Overview of applications and key issues, 2021.
59 European Commission, Statement of estimates of the European Commission: Preparation of the 2024 draft budget, 2023.
60 The US White House, Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, 2023.
61 Europol, Accountability Principles for Artificial Intelligence (AP4AI) in the Internal Security Domain, 2022.
62 European Union Agency for Fundamental Rights, Getting the future right: Artificial Intelligence and fundamental rights, 2020.
63 Fundacja Moje Państwo, Algorithmic Impact Assessment Artificial Intelligence Systems and Automatic Decision-Making Systems – Proposal for the public sector, 2023.

Disclaimer

The views expressed in GMF publications and commentary are the views of the author(s) alone.

As a non-partisan and independent research institution, The German Marshall Fund of the United States is committed to research integrity and transparency.

About the Author(s)

Filip Konopczyński is a lawyer and analyst focusing on regulation for artificial intelligence and emerging tech. In Poland, he has worked for several research institutes (NASK, IDEAS NCBR), human rights agencies, and civil society organizations (the Polish Commissioner for Human Rights, Fundacja Panoptykon) as well as think tanks and watchdogs (Fundacja Kaleckiego, OKO.press). He is an author and commentator, including for Verfassungblog, Visegrad Insight, Onet, Gazeta Wyborcza, Rzeczpospolita, DGP, TVN24, and Polsat.

About the ReThink.CEE Fellowship

As Central and Eastern Europe faces mounting challenges to its democracy, security, and prosperity, fresh intellectual and practical impulses are urgently needed in the region and in the West broadly. For this reason, GMF established the ReThink.CEE Fellowship that supports next-generation policy analysts and civic activists from this critical part of Europe. Through conducting and presenting an original piece of policy research, fellows contribute to better understanding of regional dynamics and to effective policy responses by the transatlantic community.

Cover photo credit: MONOPOLY919 | Shutterstock

About GMF

The German Marshall Fund of the United States (GMF) is a non-partisan policy organization committed to the idea that the United States and Europe are stronger together. GMF champions the principles of democracy, human rights, and international cooperation, which have served as the bedrock of peace and prosperity since the end of the Second World War, but are under increasing strain. GMF works on issues critical to transatlantic interests in the 21st century, including the future of democracy, security and defense, geopolitics and the rise of China, and technology and innovation. By drawing on and fostering a community of people with diverse life experiences and political perspectives, GMF pursues its mission by driving the policy debate through cutting-edge analysis and convening, fortifying civil society, and cultivating the next generation of leaders on both sides of the Atlantic. Founded in 1972 through a gift from Germany as a tribute to the Marshall Plan, GMF is headquartered in Washington, DC, with offices in Berlin, Brussels, Ankara, Belgrade, Bucharest, Paris, and Warsaw.

Ankara • Belgrade • Berlin • Brussels • Bucharest

Paris • Warsaw • Washington, DC

gmfus.org