Cupać, Jelena; Sienknecht, Mitja

Article — Published Version

Regulate against the machine: how the EU mitigates AI harm to democracy

Democratization

Provided in Cooperation with:
WZB Berlin Social Science Center

Suggested Citation: Cupać, Jelena; Sienknecht, Mitja (2024) : Regulate against the machine: how the EU mitigates AI harm to democracy, Democratization, ISSN 1743-890X, Taylor & Francis, London, Vol. 31, Iss. 5, pp. 1067-1090, https://doi.org/10.1080/13510347.2024.2353706

This Version is available at:
https://hdl.handle.net/10419/308004

DEMOCRATIZATION
2024, VOL. 31, NO. 5, 1067–1090
https://doi.org/10.1080/13510347.2024.2353706

Routledge
Taylor & Francis Group

RESEARCH ARTICLE

OPEN ACCESS Check for updates

Regulate against the machine: how the EU mitigates AI harm to democracy

Jelena Cupać [a] and Mitja Sienknecht [b]

[a]WZB Berlin Social Science Center, Berlin, Germany; [b]European University Viadrina Frankfurt, Frankfurt, Germany

ABSTRACT

Democracies are under attack from various sides. In recent years AI-powered techniques such as profiling, targeting, election manipulation, and massive disinformation campaigns via social bots and troll farms challenge the very foundations of democratic systems. Against this background, demands for regulating AI have gotten louder. In this paper, we focus on the European Union (EU) as the actor that has gone the furthest in terms of regulating AI. We therefore ask: What kind of instruments does the EU envision in their binding and non-binding documents to prevent AI harm to democracy? And what critique can be formulated regarding these instruments? To address these questions, the article makes two contributions. First, by building on a systematic understanding of deliberative democracy, we introduce the distinction between two types of harm that can arise from the widespread use of AI: rights-based harm and systemic harm. Second, by analysing a number of EU documents, including the GDPR, the AI Act, the TTAP, and the DSA, we argue that the EU envisions four primary instruments for safeguarding democracy from the harmful use of AI: prohibition, transparency, risk management, and digital education. While these instruments provide a relatively high level of protection for rights-based AI harm, there is still ample space for these technologies to produce systemic harm to democracy.

ARTICLE HISTORY Received 31 October 2022; Accepted 7 May 2024

KEYWORDS Artificial Intelligence (AI); democracy; harm; European Union (EU); AI Act

Introduction

Concerns about artificial intelligence (AI) negatively impacting democracy are not new. The Cambridge Analytica scandal has already revealed how practices such as psychographic profiling and targeted political advertising could be used for election manipulation. However, recent advancements in AI, notably the emergence of Large Language Models (LLMs) such as ChatGPT, along with models capable of generating images, audio, and video content, have escalated these concerns to a new level. As these technologies continue to spread and capture public attention, we are heading toward

CONTACT Jelena Cupać jelena.cupac@wzb.eu

the first wave of elections in which they will be widely deployed. It is expected that quite a few politicians will use synthetic content in their campaigns, whether to launch attacks against their opponents through manipulated videos and imagery or to reduce campaign costs. Against this backdrop, we focus on the European Union (EU) and ask what measures it envisions to mitigate the harm AI poses to democratic process.

The EU's relationship with democracy is not perfect. Since its founding, it has been accused of structural democratic deficit and, more recently, it has had to grapple with a populist wave causing democratic backsliding in several of its member states. Still, there is no denying that the EU is inextricably linked to democracy. Along with human dignity, freedom, equality, the rule of law, and human rights, the Lisbon Treaty lists democracy as one of the EU's core values. An important implication of this value orientation is that when the EU ventures into a new regulatory territory, it is expected to show concern for democracy and devise mechanisms for its protection, especially if there is ample evidence that a given domain might suffer significant democratic erosion.

As the global race towards AI intensifies, we are witnessing a parallel race towards AI regulation, with the EU emerging as a clear frontrunner.[1] Although lagging behind the United States and China in AI development, the EU is actively striving to establish itself as a global standard-setter in digital technologies. It has already achieved this goal through its flagship General Data Protection Regulation (GDPR), with various countries outside Europe adopting similar data protection rules. The EU now seeks to replicate this impact with the Digital Services Act (DSA), aimed at bolstering online safety by tackling harmful content, and more significantly, with the Artificial Intelligence Act (AIA), a comprehensive regulatory framework for AI grounded in a risk-based approach.[2]

Despite these documents' obligation to address harm to democracy, a systematic overview of the measures they establish for this purpose is still missing. As a result, we have a limited understanding of the set of actions the EU and its member states have at their disposal to uphold democratic processes in the AI age. The rapid progress of AI technologies underscores the importance of such understanding, not least to identify which areas of democracy are adequately protected and which require further safeguarding.

To address this gap, we start by identifying the types of harm a widespread use of AI can cause to democracy. Based on a systematic understanding of deliberative democracy, we distinguish between *rights-based harm* and *systemic harm*. The former pertains to using technology to limit people's participation in the democratic process, while the latter refers to broader societal and political factors that impede democratic deliberation, such as fragmentation, polarization, distrust, and political apathy. In making this distinction, we join a growing number of scholars who call for a broader approach to AI harm, one that goes beyond individual and human rights concerns and pays attention to the wider societal impact.[3]

Based on this framework, we have selected four legally binding EU documents for our analysis: the GDPR, DSA, AIA, and the Proposal for a Regulation on the Transparency and Targeting of Political Advertising (TTPA), alongside a range of non-binding documents (see Appendix, Table 1). Through close examination of these documents, we have identified four key instruments the EU proposes to protect democracy from AI harm: prohibition, transparency, risk management, and digital

education. Prohibition entails the outright banning of specific data and AI practices; transparency mandates the disclosure of information concerning the development and deployment of AI systems; risk management involves assessing the risk of an AI system before deployment and monitoring the risk after the system is in use; and digital education aims to raise public awareness of AI risks and empower individuals to use digital technologies responsibly. Although these instruments afford a relatively robust level of protection against rights-based harm, our core observation is that the widespread use of AI still has significant potential to inflict systemic harm to democracy in the EU.

Before proceeding, it is important to note this study's limitations. Our primary goal was to categorize AI harm to democracy and take a bird's eye view of the EU's regulatory and policy responses. Ideally, we would have matched each type of harm with specific protective measures and provided a detailed evaluation. However, the intertwined nature of rights-based and systemic harm, which is also mirrored in regulatory and policy instruments, makes such an approach challenging. Thus, we have opted for a broader approach, which can serve as a guide for future in-depth analysis.

The article proceeds in three steps. First, we define democracy and AI, and discuss rights-based and systemic harm in more detail. Second, we outline our analytical steps: selecting EU documents and identifying instruments to shield against AI harm. Third, we present and critically assess these instruments. In conclusion, apart from summarizing our findings, we delve into the challenges and possibilities of regulating against AI harm, thereby underscoring a significant avenue for future research.

Artificial intelligence and democracy: definitions

To explore the potential negative impact of AI on democracy, we must first define both concepts. However, defining AI and democracy is notoriously difficult. AI can refer to a broad range of constantly evolving technologies and applications that mimic human cognition, such as learning, problem-solving, and decision-making. Likewise, democracy remains elusive given the diverse ways democratic principles manifest across various societies and cultures. Recognizing these challenges, we have opted for a pragmatic approach, seeking definitions that neither impede thorough analysis nor restrict broader insights into the EU's AI regulation for democracy protection.

Defining artificial intelligence and its application in politics

AI can be defined as "Systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals."[4] AI systems can make autonomous decisions in various fields of human activity and generate original content such as text, pictures, and videos. Unlike conventional digital technologies based on fixed algorithmic patterns, AI systems rely on neural networks – machine learning algorithms modelled after the human brain's structure and function – to learn, adapt, and evolve through exposure to large amounts of data. In this way, AI systems can analyse complex patterns, make informed decisions, and create content that exceeds the limits of their initial programming.

Currently, numerous AI technologies and their applications are seen as potential threats to democracies. Some are entirely AI-based, while others rely on traditional digital methods. Yet, when augmented by AI, these conventional methods can be significantly enhanced, heightening their potential risk. Broadly speaking, these technologies can be split into two categories along their intended function: those centred on surveillance, such as data collection and profiling, and those geared towards manipulation, encompassing targeting, social bots, and deep fakes.[5]

Profiling consists of collecting and analysing data about people in order to classify them based on specific characteristics.[6] In the electoral process, demographic profiling can be used to categorize voters by attributes like age and education, whereas psychometric profiling probes deeper into personality traits, such as being argumentative or compliant. Yet, profiling is not solely informational; it typically supports *targeting*, a technique intended to influence people's attitudes and political stances.[7] While micro-targeting relies on this data to identify a specific audience segment, hyper-targeting takes it a step further by relying on even more detailed information such as location tracking and social media activity.

Social bots are automated programmes that emulate human actions on social media.[8] Augmented by AI models such as GPT and Midjourney, they could generate and spread vast amounts of text, images, videos, and links. With the ability to amplify particular narratives, sway discussions, and serve as a vehicle for spreading disinformation, social bots pose a significant threat to the integrity of online information. The same applies to *deep fakes*, multimedia counterfeits that swap one person's image or video likeness for another using advanced algorithms that analyse their facial cues.[9] The result is a fake yet highly realistic piece of media.

It is crucial to highlight that we are also entering an era of rapid development in AI-powered neurotechnology, biometrics, and subliminal messaging, all expected to further exacerbate issues related to profiling and manipulation.[10] Technologies ranging from real-time biometric identification systems to subliminal messaging such as AI-driven "dark patterns" are all poised to amplify the accuracy and subtlety of profiling and manipulation, generating a host of new and often unforeseeable challenges.[11] Lastly, although not yet a reality, there is significant discussion about the development of general-purpose AI – systems capable of learning and executing a broad spectrum of tasks instead of being confined to specific roles or areas. How such AI will be integrated into political systems is difficult to predict, but its impact on disrupting traditional democratic processes and citizen engagement will be profound, so a careful consideration of its implications for governance, democracy, ethics, and society at large will be paramount in shaping its role and impact on political processes.

Definition of democracy: a systemic deliberative approach

To define democracy, we take a cue from the work of Spencer McKay and Chris Tenove, who settled on the concept of systemic deliberative democracy in their analysis of how disinformation affects the democratic process.[12] The advantage of this approach to democracy is that rather than focusing on the intricacies of multiple democratic arenas and processes, it emphasizes deliberative functions that unite these arenas and processes into a systemic whole. As a result, a key feature of this approach to democracy is identifying normative goods and functions that sustain

meaningful deliberation across the system and which, if jeopardized, can threaten democracy in its entirety.

Different authors emphasize different normative goods and functions essential for genuine democratic deliberation.[13] In this study, we draw on the work of Jane Mansbridge and her colleagues, whose approach seems particularly pertinent to the information age. They identify three functions of deliberative democracy: democratic, epistemic, and ethical.[14] The democratic function focuses on the equal participation of citizens, stressing the active inclusion of diverse perspectives and the prevention of unjust exclusion. The epistemic function pertains to the quality of the information environment in which deliberation takes place, especially the quality of the information and logics influencing preferences and opinions. Finally, the ethical function emphasizes mutual respect in political discussions, with the emphasis on participants recognizing each other's viewpoints as valid and deserving of consideration.

These three functions suggest that the bedrock of a thriving democracy lies in upholding participation rights, whether for individuals or groups, and in the systemic conditions guaranteeing this participation. The systemic conditions derive from the integrity of the information ecosystem and the quality of interactions among citizens. Against this background, we assume that AI can undermine democracy at its core both by curtailing citizens' participation rights and by introducing disruptions at the systemic level. In other words, we differentiate between two types of AI induced harm to democracy: *rights-based harm* and *systemic harm*. In so doing, we align with the burgeoning literature seeking to map, systematize, and taxonomize AI harm across various domains.[15]

At the same time, we align ourselves with a growing number of sociologists, legal scholars, and policy experts who, drawing on foundational insights from Zemiology and Science and Technology Studies, argue that social harm, whether stemming from AI or other sources, should not be viewed in predominantly individualized and human rights terms.[16] Instead, special attention should also be paid to societal harm, including harm to systems and structures upholding societies.[17] We contribute to this strand of literature by distinguishing between rights-based and systemic harm within the specific context of democracy, instead of addressing it through the lens of a society as a whole.[18] This is an analytical move that we hope provides a framework from which AI harm to democracy can be studied in a broad yet more focused manner.

AI harm to democracy: two types

Rights-based harm to democracy

In the context of this article, rights-based harm to democracy refers to using AI technologies to violate individual, collective, and group rights essential to ensuring the meaningful participation of diverse voices and perspectives in a democratic society.[19] Individual rights and freedoms, such as privacy, freedom from discrimination, and freedom of thought and expression, are widely recognized as essential for democratic participation. Collective rights belong to groups based on shared identity, such as language or culture, and are vital for protecting minority rights and ensuring their representation. Finally, group rights apply to any group of individuals and encompass such rights as forming associations and organizations and engaging in collective bargaining and advocacy.

Based on the extant literature and real-world cases, we can discern several scenarios of digital technologies powered by AI causing significant harm to these rights. One such instance is the potential harm to privacy resulting from AI systems collecting large volumes of personal data through monitoring online behaviour and social media activity without consent.[20] This data can then be used to profile and target individuals, modifying their information environment without their awareness and influencing how and whether they engage in the democratic process. Furthermore, combining generative AI with AI-powered social bots could enable malicious actors to flood social media with an endless stream of messages that disparage and reinforce stereotypes about particular minority groups, corroding the moral respect they need to be recognized as equal democratic interlocutors.[21] Such information operations can spill over into the real world, contributing to these groups being further marginalized and even excluded from politics.

Similar things can happen to groups that organize around political interests rather than strictly their identities, such as political parties and social movements. In addition to large quantities of disparaging information, their political participation can also be jeopardized by the compromising fabrications created by deep fakes. Political adversaries could use deep fakes to depict each other engaging in disreputable behaviour, making controversial statements, or participating in criminal activities while portraying themselves in a favourable light. Finally, groups and collectives may find their voices drowned out not because of the nature of AI-generated content but its massive quantity on social media and other online platforms.[22]

Systemic harm to democracy

The systemic harm that the widespread use of AI technologies can inflict on democracies refers to the impairment of general societal, informational, and political conditions in which democratic participation and deliberation unfold. Such harm can come in the form of societal and political polarization, fragmentation, pervasive distrust, and widespread political apathy and indifference. These distortions need not be produced by AI. They can arise due to a variety of political, cultural, societal, and economic reasons and, as we know, from digital technologies that are not augmented by AI. However, AI-based technologies, and especially generative AI, threaten to exacerbate them to historically unprecedented levels.

As already indicated, rights-based harm and systemic harm to democracy are not strictly separable. The reason for this lies in the fact that the infringement of individual, collective, and group rights constitutes one means by which AI can inflict systemic harm on democracy. To illustrate, consider the case of pervasive AI propaganda campaigns targeting a minority group on social media platforms. Such campaigns can simultaneously erode the group's collective rights and foster a climate of intensified societal radicalization and polarization, thus developing from group rights-harm to systemic harm.

However, the distinction is nonetheless useful, considering that AI can undermine democracy at a systemic level even in the absence of explicit violations of individual, group, and collective rights. Strategies for achieving this can include spreading a plethora of conspiracy theories or amplifying extremist views. Such campaigns can lead to the formation of isolated, like-minded groups that are increasingly disconnected from the broader society, resulting in societal fragmentation. At the same time, the proliferation of conspiracy theories can deepen the divide between those who subscribe to them and those who reject them, thereby intensifying polarization. This widening rift

can make it more challenging for individuals and groups to engage in constructive dialogue and find common ground, ultimately undermining the democratic process.

Multiple scenarios can also be imagined in which the widespread use of AI can lead to distrust and political apathy. For instance, they may inadvertently prioritize content that triggers strong emotional reactions, such as outrage, fear, or disgust, leading to a more negative and cynical perception of politics and politicians. Using AI in mass surveillance may result in perceived or actual privacy loss, making people more cautious about expressing their opinions and engaging in political activities. Lastly, AI-produced disinformation and misinformation can erode trust in traditional knowledge sources, such as universities, leading citizens to regard all truth claims with scepticism, perceiving them as politically motivated.

Before we proceed, it should be emphasized that the literature recognizes the challenges of addressing and regulating systemic harm. A primary concern is the issue of temporality. On the one hand, there are systemic harms that remain unanticipated and thus elude regulation. On the other hand, the systemic harm we are familiar with does not arise from a singular use of AI but evolves over time from multiple deployments by various actors and in combination with other social factors. Consequently, this type of harm is accumulative, making it challenging to identify a direct cause or determine the responsible party.[23]

The EU's response to AI harm to democracy: a critical survey

Methodology

How does the only supranational organization of its kind comprising 27 democracies, the EU, respond to the outlined dangers posed by AI technologies to democracy? What measures is the EU taking to meet the challenge of regulating a constantly evolving technology? In this section, we survey the EU's policies and regulations aimed at mitigating rights-based and systemic harm the widespread use of AI may cause to democracy. Since the mid-1990s, the EU has regularly introduced policies, action plans, codes of conduct, and regulations to support member states' digital transition. To select documents relevant to our analysis, we first compiled a detailed list of the EU's digital regulations and policies by using the EU's website and EUR-Lex search function (see Appendix, Table 1). The resulting list is not exhaustive. When it comes to non-legal instruments, it only features documents with a direct or indirect connection to AI, rather than covering digitalization more broadly.

To select relevant documents for our analysis, in line with our definition of democracy, we identified documents concerned with rights to political participation and those addressing the integrity of the information environment. From the shortlisted documents we then selected for our analysis those addressing AI technologies and applications, specifically data collection, processing, profiling, targeting, social bots, deep-fakes, and disinformation campaigns, as well as other technologies that could broadly be defined as AI.

This selection process yielded four legally binding documents: The General Data Protection Regulation (GDPR), the Digital Services Act (DSA), the Artificial Intelligence Act (AIA), and the Proposal for a Regulation on the Transparency and Targeting of Political Advertising (TTPA). The GDPR is a privacy law that protects EU residents' data by restricting its unconsented collection and processing, including for automated

decision-making. The DSA is a legislative framework for digital services, aiming to enhance online safety by combating disinformation and harmful content. The EU AI Act is the first legislation aimed at directly regulating the development and deployment of AI systems within the common market. Finally, the TTPA is a proposed law designed to harmonize political campaigning across the continent, including the use of AI technologies such as profiling and targeting.

The European Media Freedom Act (EMFA) and the Digital Markets Act (DMA) are examples of the documents we excluded from our analysis, although they may appear relevant at first glance. While the EMFA emphasizes democratic participation, it does not directly address AI. Conversely, the DMA mentions AI but does not focus on democracy as we define it here in this article. As for non-binding legal and non-legal documents, we considered documents in our analysis that fulfilled the same criteria. Thus, we included declarations, communications, white papers, policies, and codes of practices that deal with threats to democracies and the influence of AI. For a detailed list, see the bolded text in the table located in the Appendix.

To identify the specific EU regulatory and policy measures intended to protect the continent's democracy from AI risks, we started by inductively analysing the four legally binding documents. By grouping the articles according to their similarity, we can show that the measures the EU is currently taking to protect democracy from AI-related harm fall into four broad categories: (1) prohibition, (2) transparency (subcategories: transparency to individuals, operational transparency, reporting transparency); (3) risk management; and (4) education (see Appendix, Table 2). In the course of the analysis, two more categories were considered: socio-technical design of AI systems and the governance of the digital sphere. However, we decided to omit them, considering them as already contained within our four primary categories. While specific articles in the AIA, like Article 15, explicitly require developers to adhere to certain design principles, we contend that the bulk of the articles within the prohibition, transparency, and risk management categories also guide the design of AI systems. These articles, by dictating what AI systems should or should not do to avoid causing harm, or asking developers to disclose features of design, essentially serve as directives for how these systems should be made. For this reason, we have opted not to treat socio-technical design as a separate category, although we acknowledge that some articles might be more explicit about it. Similarly, given that governance plays a crucial role in enforcing any EU regulation, we see it as unnecessary to treat it as a distinct category within the context of digital sphere governance. In the next section, we discuss each measure, along with their strengths and weaknesses in reducing rights-based and systemic AI harms to democracy. In doing so, we leverage insights from recent research in prohibition, transparency, risk, and education within the digitalization field.

EU instruments against AI harm to democracy

Prohibition

The EU's most far-reaching instrument to mitigate the harmful effects of AI, including harm to democracy, is the prohibition of specific AI systems and practices. Each of the four documents examined – the GDPR, DSA, TTPA, and the AIA – includes such prohibitions. The GDPR bans processing biometric data and data relating to ethnic

origins, political opinions, religious or philosophical beliefs, trade union membership, sex life, and sexual orientation.[24] The DSA bans online platforms from displaying ads based on profiling with GDPR-restricted data.[25] Similarly, the TTPA bans targeting and amplification in political ads using data processing prohibited by the GDPR and Regulation 2018/1725.[26] Advancing further, the AIA classifies AI-associated risks into three categories: unacceptable, high, and low or minimal risk, with only systems identified as posing an unacceptable risk being banned. Seven types of such AI are distinguished, including AI under free and open-source licence: (1) AI systems that deploy subliminal techniques; (2) AI systems that exploit vulnerabilities such as age, disability, or socio-economic situation; (3) AI systems that evaluate or classify people based on their social behaviour or personal characteristics (i.e. social scoring); (4) AI system that assess criminal offence risk based on profiling or on personality characteristics; (5) AI systems that create or expand facial recognition databases by indiscriminately collecting facial images from the internet or CCTV footage; (6) AI systems that infer emotions within workplace and education institutions; and (7) real-time remote biometric identification systems in public spaces for the purposes of law enforcement.[27]

Together, these prohibition measures offer robust protection against a range of AI profiling and manipulation techniques that threaten democracy. However, a closer look shows that they mainly aim to avert rights-based harm towards individuals, collectives, and groups.[28] Accordingly, the prohibition articles can only mitigate the systemic harm to democracy that is channelled through the violations of individual, collective, and group rights, such as social fragmentation emerging from the discrimination of certain social groups. Systemic harm detached from rights-based concerns, such as polarization propelled by pervasive false information, remains beyond the scope of the prohibition articles. Lastly, many prohibition articles lack detailed definitions or legal qualifications for the practices they aim to restrict. For instance, a sensory threshold distinguishing a technology as subliminal rather than supraliminal remains unspecified.[29] This suggests that even with an expanded list of prohibited AI systems and practices, a narrow interpretation of these practices could still leave considerable room for rights-based and systemic harm to democracy.

Transparency

The EU's most prominent instrument envisioned to protect democracy from AI harm is transparency. Given transparency's long-standing role in upholding democracy, this is unsurprising. The tech world also widely adopts the concept, with Jobin and colleagues noting it as the most widely used principle in numerous global ethical guidelines on AI.[30] In broad terms, transparency refers to "the availability of information about an actor allowing other actors to monitor the workings or performance of this actor."[31] However, transparency is not just one thing.[32] It is a multifaceted concept whose objectives can be achieved through diverse instruments, each designed to make different information available to different parties for different purposes. We have, therefore, identified three broad transparency instruments in EU regulation to protect democracy from rights-based and systemic AI harm: (1) transparency to individuals, (2) operational transparency, and (3) reporting transparency. As noted earlier, these instruments do not exclusively address rights-based or systemic AI harm but vary in focus, aligning with our view that

AI harms are not strictly separable and providing a crucial perspective for evaluating these tools.

Transparency to individuals

Transparency to individuals regulates the interaction between individuals and AI systems. This category encompasses two types of transparency: one concerning personal data privacy and the other related to digital content. GDPR is the EU's primary tool for regulating personal data privacy. Notwithstanding the prohibitions discussed earlier, the GDPR does not question the use of personal data in AI-based systems. It only stipulates that such use should be based on valid consent, achieved when those collecting and processing personal data are transparent about their activities. They must provide data subjects with clear information regarding the type of data being collected, the purpose of data processing, and the right to object or limit such processing.[33] In this way, the EU assumes that if an individual has relinquished their data privacy via informed consent, the harm to their rights is prevented, and, by extension, a degree of democratic protection is achieved.

A similar assumption guides transparency measures for individuals interacting with AI-generated content such as text or deep-fakes. While there are a few exceptions, the EU does not question this content per se but is concerned that individuals might be unaware that they are interacting with social bots and synthetic media. Consequently, the remedy is found in disclosures, facilitated through terms and conditions and transparency notices. The DSA and TTPA thus demand clear labelling of advertisements and disclosure of any use of algorithmic profiling, targeting, or recommender systems, while the AIA demands clearly and visibly labelling AI systems that interact with humans, as well as placing transparency labels for AI-generated content such as deepfakes and synthetic text.[34]

Operational transparency

The second transparency instrument we identified within EU digital regulation is operational transparency. This form of transparency, well-acknowledged in algorithmic transparency literature, chiefly focuses on AI systems' design choices and operations.[35] The actions taken are intended to provide supervisory authorities, individuals, and other interested stakeholders, such as academics and journalists, with insight into the rules for developing AI systems and the practices for their daily operations. Concerning the former, the GDPR, DSA, TTPA, and the AIA require developers and providers of AI systems to create codes of conduct, technical documentation, certifications, and quality management systems, ensuring AI systems are developed following regulatory requirements and professional standards.[36] A key aspect of operational transparency involves being open about the data used to train algorithmic systems. The AIA introduces a mandate for this type of transparency, aiming not just to safeguard copyright interests but also to ensure the data is unbiased, crucial for preventing rights-related harm and reducing errors that could undermine trust.[37] Regarding the daily operations of AI systems, these four documents mandate adherence to record-keeping practices and automatically generated logs, which are crucial for understanding why a particular AI system yielded a specific (unfair, unsafe, or biased) result.[38] Operational transparency aims to enhance the accountability of AI systems, thus providing authorities, individuals, groups, and collectives with remedial measures against AI-induced damage.

Reporting transparency

The third and final transparency instrument we identified in our analysis is reporting transparency. Transparency in this context means creating publicly available documents that provide information and metrics concerning the internal governance of digital service providers. The DSA, for example, requires digital service providers that transmit or store third-party content to release comprehensive reports on their content moderation practices at least once a year. These reports are expected to include information such as the number and type of content removal orders received from member states and trusted flaggers, the amount and type of content removed, and whether automated tools were used in the process.[39] Similarly, TTPA requires, among other things, digital advertising publishers to disclose the funding they received for specific campaigns and whether campaigns relied on profiling, targeting, and amplification.[40] The AIA also introduces certain mechanisms for reporting and notification that vary from a basic duty to report non-compliance with standards of high-risk AI to specific alerts for AI systems that are classified as general-purpose AI.[41] In addition to regular reports, these documents also lay out guidelines for government agencies, civil society, researchers, and journalists to request access to specific information from digital service providers, including advertising services.

Collectively, the transparency instruments within EU digital regulation seem to establish a robust legal framework against rights-based and systemic AI harm to democracy. They strive to keep individuals informed about the collection and handling of their private data in the context of practices such as profiling and targeting (individual transparency) and aim to foster trust and accountability through revealing information about the design and functioning of AI systems, as well as the elimination of damaging digital content (operational and reporting transparency). Still, these measures are not bulletproof, and some might even pave the way for harm. For example, while transparency measures aimed at individuals safeguard their rights, they also acquaint them with AI practices and related harm they might not have been aware of earlier. Individuals might use this new insight to withhold consent for data collection, but they might also become disenchanted, distrustful, and politically apathetic. This could, in turn, lead to a loss of trust in democratic institutions and processes. A measure intended to protect against rights-based harm could thus, paradoxically, exacerbate harm to democracy on a systemic level.

Transparency measures directed at individuals could also serve as a tool for legitimizing profiling, targeting, social bots, and deep fakes. As highlighted earlier, the issue is not whether we want these practices and technologies used in the democratic process but whether we are informed and individually consent to their deployment. While consent and awareness provide a degree of protection for people's rights, they can also open the door to systemic harm to democracy. Even if citizens willingly receive tailored messages and interact with synthetic content, political polarization might intensify if these messages are deliberately designed to exacerbate such divisions. Moreover, if certain segments of society embrace these practices while others reject them, democratic fragmentation may arise not from the AI itself but from disputes over the use of AI. Finally, merely having access to extensive transparency information does not inherently facilitate understanding of this information or using it to hold AI developers and providers accountable.[42]

Risk management

The third instrument for protecting democracy against AI harm we identified within the EU digital regulation is *risk management*. Although related to operational transparency, the two are distinct: while operational transparency predominantly focuses on making visible *how* AI systems are constructed and operate, risk management concentrates on *what* AI systems are capable of doing or will do once they come in contact with individuals and societies. Risk management, therefore, encompasses a range of practices for *assessing* the risk of AI systems before their deployment and *monitoring* practices that are initiated once an AI system is operational. Prior to the system's deployment (although not exclusively) the GDPR requires conducting *impact assessments*, while the DSA and TTPA call for *risk assessments*.[43] The AIA – which explicitly recognizes the administration of justice and democratic process as areas in which the deployment of AI systems can produce high risks by influencing voting behaviour and election outcomes – requires *conformity assessments* and, critically for addressing potential harm to democracy, mandates *fundamental rights impact assessments*.[44] These assessments are designed to identify the categories of individuals or groups that could be impacted by an AI system and the specific risks they may face. Additionally, the AIA allows for the use of regulatory sandboxes and real-world experimentation with AI systems and sees these practices not only as a way of promoting innovation but also as helping uncover unforeseen risks or assessing the scale of known risks, including in the realm of democracy.[45]

All four documents also outline various practices for monitoring AI risk post-deployment, thus acknowledging that not all risks can be anticipated and there may be cases of misuse. The GDPR thus introduces a notification system for personal data breaches; the DSA requires reporting of illegal content, suspicious activities, or criminal offences, and also outlines the role of trusted flaggers; the TTPA focuses on the flagging of potentially non-compliant political advertisements; and the AIA sets up comprehensive risk management systems, mandates human oversight, post-market surveillance, model evaluation, the reporting of serious incidents, and the notification of systemic risks for general-purpose AI by the scientific panel.[46]

The detection of risk, be it prior or after an AI system's deployment, is never done for its own sake. It is inextricably tied with remedial action ranging from harmful content removal and change in the system's design to initiating full-scale crisis response mechanisms upon identifying severe threats to public security or health.[47] Finally, it is crucial to highlight that besides outlining various pathways to implement these and earlier provisions, these documents also create a network of national and EU-level institutions and bodies charged with ensuring AI systems' compliance with the provisions, overseeing adherence and AI risk, and initiating corrective and enforcement actions when necessary.[48]

It is worth noting that the European Commission has already implemented several initiatives under Articles 34 and 35 of the DSA aiming to protect the democratic character of elections. For example, in accordance with Article 35, the Commission has launched a public consultation to collect feedback on the preliminary DSA guidelines regarding election integrity.[49] These guidelines recommend best practices and preventive strategies for very large online platforms

and search engines to tackle systemic risks to democratic electoral processes. Additionally, in December 2023, the Commission began proceedings against platform X (previously known as Twitter), targeting the spread of illegal content within the EU and examining its transparency measures and measures to combat mis- and disinformation.[50]

Providing a broad assessment of risk management strategies in reducing rights-based and systemic threats to democracy is challenging, as these strategies are extensive and cover the entire lifecycle of an AI system. Still, some general issues can be raised, mainly pertaining to the definition of risk. Despite being a risk-based regulation, the AIA does not define risk in any strict manner or provide an exhaustive list of AI-related risks. On the one hand, this is understandable considering that risks are extensive, and many remain unforeseen, particularly those related to systemic harm. By adopting open and flexible risk management clauses, the AI Act thus embraces a more adaptable and context-sensitive approach that recognizes that AI risks, as well as our understanding of them, are likely to evolve as the technology advances and becomes more widely implemented.

On the other hand, to be detectable, risks will have to be defined at some point. Given the AIA's embedding in the New Legislative Framework, which aims to improve and strengthen conditions for placing a wide range of products on the EU's common market, this will primarily be done by standardization bodies. To facilitate AI system providers' compliance with the AIA, these bodies will be tasked with creating harmonized standards for each AIA risk domain, including democracy. Standardization bodies are thus places where the real AI rule-making will occur.[51] However, this approach has significant problems. Standardization bodies are typically used for products such as cars and washing machines, ensuring their safety before being allowed on the common market. However, although standardization is never easy and often involves political challenges, it will be particularly difficult for value-laden issues such as the relationship between AI and democracy, which is not merely a technical problem in search of a technical solution, but an issue requiring careful consideration of rights-based and systemic AI risks and their complex relationship. The problem is further exacerbated by the fact that standardization bodies rarely, if ever, include in their work a diversity of stakeholders. Accordingly, they are in danger of not only lacking the competencies to make standards on the AI's risk to democracy but the standards they end up making can themselves be considered undemocratic.[52]

The second issue involves determining the threshold at which specific measures to mitigate AI risks will positively affect the prevention, reduction, or even elimination of harms to democracy. This is particularly relevant when dealing with harmful AI content such as the spread of disinformation and other forms of public opinion manipulation. Efforts to eliminate such content are intuitively justified, yet the challenge arises from our lack of understanding of the precise threshold at which the removal of such content begins to alleviate societal distrust, apathy, fragmentation, and polarization. To put it simply, since completely eliminating harmful content from our information systems is unrealistic, the precise amount of disinformation that needs to be removed to reduce these systemic harms to democracy remains unknown. This issue is ever more important considering that such harms have the potential to enact lasting changes in society rather than merely causing temporary disruptions.

Education

To prevent the rights-based and systemic harm caused by AI, the EU not only regulates the developers and employers of AI systems but also dedicates resources to empowering its citizens with the necessary skills to navigate the digital world autonomously and in an informed manner. In other words, it focuses on its citizens' digital education. Besides prohibitions and transparency, fostering digital education is thus the fourth key measure the EU employs to protect democracy from the adverse impacts of AI.

Digital education is a cornerstone of both the European Digital Strategy and the European Digital Decade, rooted in the conviction that "engaged, informed, and empowered citizens are the best guarantee for the resilience of democracy."[53] With this in mind, the EU has set itself an ambitious target to increase the number of citizens with basic digital skills from 54% in 2021 to at least 80% by 2030.[54] The strategies to attain this target are delineated across multiple documents (see Appendix, Table 1), especially spelled out in legally non-binding documents. An analysis of these documents highlights two key areas deemed crucial for fostering an inclusive democratic process and empowering citizens to discern disinformation and make fact-based decisions: one, media and AI literacy, and two, informed participation in the digital democratic process.

First, the EU strives to enable its citizens to make informed and independent decisions in the digital realm. The Eurobarometer survey highlights a need for training in handling disinformation, with 69% reporting frequent encounters with misleading or false information.[55] Thus, the EU has engaged in developing methods to equip its citizens with skills to discern between reliable and unreliable sources and verify the authenticity of information before sharing it.[56] Particular focus is given to enhancing media literacy among young people, who access and interact with news differently than prior generations. Consequently, the EU has initiated various media literacy programmes, partnered with stakeholders such as journalists and educational institutions, and provided them with additional financial support. Besides media literacy, the AIA also promotes AI literacy defined as "skills, knowledge and understanding that allows providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause."[57] The EU's approach includes teaching about AI's functions, various applications, risks, benefits, and impact on daily life. By enhancing media and AI literacy, the EU hopes to enable its citizens to identify fake news, flag harmful content, and report disinformation, contributing to a trustworthy digital ecosystem. They are also supposed to enable citizens to take full advantage of the transparency measures we discussed earlier.

Second, the EU recognizes that constant active participation of citizens in the democratic process is crucial.[58] Engaging the public in political decision-making and fostering active involvement bolsters trust in political institutions, serving as a linchpin for a resilient and functioning democracy. Hence, the EU proposes enhancing election transparency and trust in the democratic processes in the context of AI through measures such as supporting multidisciplinary teams of fact-checkers and funding research projects aimed at deepening our understanding of disinformation dissemination and effective countermeasures.

While the EU's initiative to educate its citizens on safeguarding their various rights in the face of an increasingly AI-driven democracy and averting systemic harm is commendable, expecting individuals to manage their private information and discern false information consistently and collectively may be overly optimistic. To begin with, access to digital education is not equally available. Most EU campaigns target young people in educational settings, leaving adults and non-digital natives, who are no longer part of the educational system and might need AI curricula tailored to their cognitive level, somewhat overlooked.[59] Moreover, the EU has not sufficiently addressed a crucial point highlighted in the literature: training AI developers on AI harm to ensure the creation of systems that adhere to the standards of fairness, accountability, transparency and ethics, and democracy in general.[60]

Still, even with citizens and developers being highly educated about AI risks and the measures available to mitigate them, protecting democracy at both rights-based and systemic levels is not guaranteed. While digital literacy is necessary, it is not sufficient. Even experienced social media moderators find identifying disinformation campaigns and information propagated by social bots challenging. This challenge grows exponentially with large language models capable of flooding the system with misleading content. Moreover, even digitally literate individuals might become distrustful and apathetic if they feel overwhelmed by the constant need to differentiate between genuine information and disinformation and handling their private data. Ironically, this could contribute to systemic harm to democracy rather than protecting against it.

Conclusion

In this study, we mapped the diverse measures the EU has implemented or plans to implement to protect democracy from the growing harm associated with AI technologies. The mapping was guided by the distinction we made between rights-based and systemic AI harm to democracy, resulting in four categories of measures: prohibition, transparency, risk management, and education. As a mapping exercise, our analysis trades an in-depth examination of the EU regulation for a bird's eye perspective on the regulatory landscape. Yet, this approach enables us to infer several insights that could prompt a deeper analysis of these measures in the future.

We note that when we expand our focus beyond the AIA to other binding and non-binding EU documents that address to some degree the harm of AI to democracy, we see that the EU has developed a quite robust toolbox of protective measures, catering to both rights-based and systemic harm. Especially in the realm of systemic harm, which existing literature identifies as inadequately addressed, we map a variety of measures that can be seen as efforts to institute continuous oversight of AI systems' development and deployment.[61]

However, despite the inclusion of these provisions, AI still has significant potential to produce systemic harm to democracy. Based on this, we propose that the challenge with AI systemic harm in the EU's AI regulation is not just its insufficient coverage, as highlighted by existing research, but also that such harm is inherently difficult, perhaps even impossible, to effectively regulate.

First, as underscored throughout the article, highly protected rights and an AI-literate public can, paradoxically, engender systemic harm to democracy. Many people consenting to being profiled and targeted, even with non-deceptive content, can

foster the creation of echo chambers, which, in turn, may lead to political polarization and fragmentation. Moreover, a public possessing a high level of knowledge about AI practices may grow disillusioned with its integration into the democratic process, consequently becoming more distrustful and politically apathetic.

Second, the aggregated nature of systemic harm, coupled with the fact that it arises not solely from AI but from its intertwining with pre-existing social conditions, makes pinpointing its exact causes challenging. However, without such precision, it is difficult to establish parties accountable for systemic harm or a threshold at which measures targeting only its AI component would be effective. For example, while social media companies contribute to increasing political polarization, it is unclear whether eliminating mis- and disinformation from these platforms would alleviate this issue or, importantly, what amount would need to be removed before we see a positive shift.

Against this backdrop, we propose two avenues for further research: one analytical and the other normative. Analytically, there is a need for a thorough examination of the EU's regulatory instruments to mitigate the harms AI can cause to democracy at a fundamental level. This examination should be mindful of both rights-based and systemic AI harm as well as of the broader regulatory landscape we outlined. Scrutiny of this type could act as a catalyst for regulatory improvements and policy recommendations, which are urgently needed given AI's rapid advancement and widespread adoption. Normatively, it may be time to acknowledge that regulation and policy can go only so far and that we need to start thinking about a novel paradigm of democracy in which AI would not be only a problem to be managed but its integral component.[62]

Notes

1. Smuha, "From a 'Race to AI' to a 'Race to AI Regulation'."
2. After adopting the Artificial Intelligence Act (AIA) on 13th March 2024, the European Parliament issued corrections on 16th April 2024. This corrected version is cited in this paper and represents the final draft of the AI Act, which is awaiting final approval by the Council of the European Union at the time of writing this paper.
3. See: Hildebrandt, "Algorithmic Regulation and the Rule of Law"; Kolt, "Algorithmic Black Swans"; Smuha, "Beyond a Human Rights-Based Approach to AI Governance"; Smuha, "Beyond the Individual"; Uuk, "Manipulation and the AI Act"; van der Sloot and van Schendel, "Procedural Law for the Data-Driven Society"; Yeung, "AI Governance by Human Rights-Centered Design."
4. European Commission's High-Level Expert Group on Artificial Intelligence, "A Definition of AI", 1.
5. Cf. Kaplan, "Artificial Intelligence, Social Media, and Fake News," 153.
6. See: Brkan, "Artificial Intelligence and Democracy"; Djeffal, "AI, Democracy and the Law"; Eubanks, *Automating Inequality*; Hinsch, "Differences That Make a Difference"; Kertysova, "Artificial Intelligence and Disinformation"; McSweeny, "Psychographics, Predictive Analytics, Artificial Intelligence & Bots"; O'Neil, *Weapons of Math Destruction*; von Ungern-Sternberg, "Discriminatory AI and the Law."
7. See: Brkan, "Artificial Intelligence and Democracy"; Djeffal, "AI, Democracy, and the Law"; Ienca, "On Artificial Intelligence and Manipulation"; Kaplan, "Artificial Intelligence, Social Media, and Fake News"; Kertysova, "Artificial Intelligence and Disinformation"; König and Wenzelburger, "Opportunity for Renewal or Disruptive Force?"; Milan and Agosti, "Personalisation Algorithms and Elections"; Mogaji et al. "Using AI to Personalise Emotionally Appealing Advertisement"; Narayanan, *Understanding Social Media Recommendation Algorithms*; Zachary, "Digital Manipulation."

8. See: Brkan, "Artificial Intelligence and Democracy"; Diakopoulos, "Automating the News"; Ferrara et al., "The Rise of Social Bots"; García-Orosa et al., "Algorithms and Communication"; Keller et al. "Social Bots in Election Campaigns"; Shao et al., "The Spread of Low-Credibility Content."
9. See: Habgood-Coote, "Deepfakes and the Epistemic Apocalypse"; Hameleers et al., "You Won't Believe What They Just Said!"; Jacobsen and Simpson, "The Tensions of Deepfakes"; Westerlund, "The Emergence of Deepfake Technology"; Whyte, "Deepfake News."
10. For an overview see: Farahany, *The Battle for Your Brain;* Neuwirth, "Prohibited Artificial Intelligence Practices"; Neuwirth, *The EU Artificial Intelligence Act.*
11. See: Neuwirth, *The EU Artificial Intelligence Act,* 25–26 and 94.
12. McKay and Tenove, "Disinformation as a Threat to Deliberative Democracy"; Tenove, "Protecting Democracy from Disinformation."
13. For an overview, see: Warren, "A Problem-Based Approach to Democratic Theory."
14. Mansbridge et al., "A Systemic Approach to Deliberative Democracy", 11-12.
15. For an overview, see: Shelby, "Sociotechnical Harms of Algorithmic Systems."
16. Smuha, "Beyond a Human Rights-Based Approach to AI Governance"; Smuha, "Beyond the Individual"; Yeung, "AI Governance by Human Rights–Centered Design."
17. Hildebrandt, "Algorithmic Regulation and the Rule of Law"; Kolt, "Algorithmic Black Swans"; Smuha, "Beyond the Individual"; Uuk, "Manipulation and the AI Act"; van der Sloot and van Schendel, "Procedural Law for the Data-Driven Society."
18. Cf. Jungherr "Artificial Intelligence and Democracy"; König and Wenzelburger, "Opportunity for Renewal or Disruptive Force."
19. In "Beyond the Individual," Smuha differentiates between individual, collective, and societal harm AI can cause. Conversely, we adopt a perspective grounded in the systemic deliberative definition of democracy, which emphasizes participation rights for both individuals and groups, along with the systemic conditions necessary for exercising these rights. Consequently, we offer a binary categorization of AI harm: rights-based and systemic harm. While there are significant overlaps, our classification diverges from Smuha's by being anchored in a specific understanding of democracy rather than a broad societal viewpoint.
20. See for a discussion on the group right to privacy in the context of biomedical data, Floridi 2014.
21. Cf., DiResta et al., "The Tactics & Tropes."
22. Cf., Woolley and Guilbeault, "United States."
23. See: Smuha, "Beyond the Individual," 10; Kernohan, Andrew. "Accumulative Harms."; Kolt, "Algorithmic Black Swans."
24. GDPR, Regulation (EU) 2016/679, Article 9.
25. DSA, Regulation (EU) 2022/2065, Article 26 and 28. DSA also prohibits designing online interfaces in a manipulative way, Article 25.
26. European Parliament and the Council of the European Union, Regulation on the Transparency and Targeting of Political Advertising, PE 90 2023 INIT, Article 18.
27. Some of these prohibitions come with exceptions, for details see: European Parliament, Corrigendum, Artificial Intelligence Act, P9_TA(2024)0138, Article 5. For detailed analysis and criticism of these practices see: Neuwirth, "Prohibited Artificial Intelligence Practices,"; Neuwirth, *The EU Artificial Intelligence Act.*
28. Cf. Smuha, "Beyond the Individual."
29. Neuwirth, "Prohibited Artificial Intelligence Practices," 4.
30. Jobin et al., "The Global Landscape of AI Ethics Guidelines." See also: Mike and Crawford. "Seeing Without Knowing"; Gorwa and Ash, "Democratic Transparency in the Platform Society"; Larsson, Stefan, and Fredrik Heintz, "Transparency in Artificial Intelligence."
31. Albert Meijer as quoted in Diakopoulos, "Transparency," 198.
32. Heald, "Varieties of Transparency."
33. GDPR, Regulation (EU) 2016/679, Article 12 and 13. Transparency measures relating to the handling of private data can also be found in GDPR's Articles 5, 6, 7, 8, 11, 14, 15, 16, 17, 18, 19, 20, 21, 22, and 34.
34. DSA, Regulation (EU) 2022/2065, Articles 14, 17, 20, 26, 27, 28, 38, and 39; European Parliament and the Council of the European Union, Regulation on the Transparency and Targeting of Political Advertising, PE 90 2023 INIT, Articles 11, 12, 18, and 19; European Parliament, Corrigendum, Artificial Intelligence Act, P9_TA(2024)0138, Articles 13 and 50. It is important

to highlight that Article 50 extends to AI under a free and open-source licence. Some critics view this as an insufficient measure for this type of AI, which is often regarded as particularly risky for its potential to harm democracy, including via the widespread dissemination of disinformation. See, e.g.: Giannaccini and Kleineidam, How the EU's Soft Touch on Open-Source AI Opens the Door to Disinformation.

35. See: Andrada et al., "Varieties of Transparency"; Diakopoulos, "Transparency"; Walmsley, "Artificial Intelligence and the Value of Transparency."
36. GDPR, Regulation (EU) 2016/679, Article 25, 40, 41, and 42.; DSA, Regulation (EU) 2022/2065, Articles 44 to 77; European Parliament, Corrigendum, Artificial Intelligence Act, P9_TA (2024)0138, Articles 10, 11, 12, 13, 15, 17, 18, 44, 47, 48, 49 and 77.
37. European Parliament, Corrigendum, Artificial Intelligence Act, P9_TA(2024)0138, Articles 13 and 53.
38. GDPR, Regulation (EU) 2016/679, Article 30 and 32; DSA, Regulation (EU) 2022/2065, Articles 37 and 40; European Parliament and the Council of the European Union, Regulation on the Transparency and Targeting of Political Advertising, PE 90 2023 INIT, Articles 9 and 19; European Parliament, Corrigendum, Artificial Intelligence Act, P9_TA(2024)0138, Articles 12, 19, 53, and 55.
39. DSA, Regulation (EU) 2022/2065, Articles 10, 15, 24, and 42.
40. European Parliament and the Council of the European Union, Regulation on the Transparency and Targeting of Political Advertising, PE 90 2023 INIT, Articles 14, 16, 17, and 20.
41. European Parliament, Corrigendum, Artificial Intelligence Act, P9_TA(2024)0138, Articles 20, 27, 52, 77, and 91.
42. Ananny and Crawford, "Seeing Without Knowing."
43. GDPR, Regulation (EU) 2016/679, Articles 35 and 36; DSA, Regulation (EU) 2022/2065, Article 34; European Parliament and the Council of the European Union, Regulation on the Transparency and Targeting of Political Advertising, PE 90 2023 INIT, Article 19.
44. European Parliament, Corrigendum, Artificial Intelligence Act, P9_TA(2024)0138, Articles 27 and 43 and Annex III(8).
45. European Parliament, Corrigendum, Artificial Intelligence Act, P9_TA(2024)0138, Articles 57 and 60.
46. GDPR, Regulation (EU) 2016/679, 33; DSA, Regulation (EU) 2022/2065, Articles 16, 18, 22, and 23; European Parliament and the Council of the European Union, Regulation on the Transparency and Targeting of Political Advertising, PE 90 2023 INIT, Article 15; European Parliament, Corrigendum, Artificial Intelligence Act, P9_TA(2024)0138, Article 9, 14, 55, 72, 73, 74, 75, 76, 89, and 90.
47. Remedial and mitigation articles can be either independent or a part of some other article. For example, see: DSA, Regulation (EU) 2022/2065, Articles 9, 16, 18, 22, 23, 35, 36, and 48; European Parliament, Corrigendum, Artificial Intelligence Act, P9_TA(2024)0138, Articles 15, 20, 55, and 57.
48. The GDPR establishes the Data Protection Officer, Lead Supervisory Authority, European Data Protection Board, and National Data Protection Authorities; the DSA establishes the Digital Services Coordinator, European Board for Digital Services; and the AIA establishes the AI Office, European Artificial Intelligence Board, Advisory Forum, Scientific Panel of Independent Experts, Notifying Authority, Market Surveillance Authority, and Conformity Assessment Body.
49. European Commission, Commission is Gathering Views on Draft DSA Guidelines for Election Integrity.
50. Austin, "The DSA now Applies in Full."
51. Veale and Borgesius, "Demystifying the Draft Eu Artificial Intelligence Act," 105.
52. Edwards, *Regulating AI in Europe*.
53. European Commission, COM (2020) 790 final, 3.
54. See: https://ec.europa.eu/eurostat/cache/metadata/en/isoc_sk_dskl_i21_esmsip2.htm
55. European Commission, Standard Eurobarometer 98, QF8.1, T150.
56. On trustworthiness of sources, see: European Commission, COM (2020) 790, 23. On sharing the information, see: European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01); The Strengthened Code of Practice on Disinformation (2022 COM (2020) 624 final); Tackling Online Disinformation: A European Approach (COM (2018) 236

final); White Paper on Artificial Intelligence: A European approach to excellence and trust (COM (2020) 65 final).
57. European Parliament, Corrigendum, Artificial Intelligence Act, P9_TA(2024)0138, Article 3 (56).
58. European Commission, COM (2020) 790 final, 3.
59. Chan, "A Comprehensive AI Policy Education Framework"; Kaplan, "Artificial Intelligence, Social Media, and Fake News"; Laupichler et al., "Artificial Intelligence Literacy in Higher and Adult Education"; Lee, "Fake News, Phishing, and Fraud"; Yang, "Artificial Intelligence Education for Young Children".
60. Bogina et al. "Educating Software and AI Stakeholders"; Borenstein and Howard, "Emerging Challenges in AI"; Schiff, "Education for AI, not AI for Education."
61. Cf. Smuha, "Beyond the Individual," 16-23.
62. See: Susskind, *On Freedom and Democracy*; Coeckelberghm, *Why AI Undermines Democracy*.

Acknowledgment

The authors wish to express their gratitude to Yushu Soon for her assistance and patience during the literature review for this article, and to the reviewers for their insightful and constructive comments.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Jelena Cupać is a Post-Doctoral Research Fellow at the WZB Berlin Social Science Center. She holds a PhD from the European University Institute (EUI) in Florence. Her research explores the transformation of international organizations, the global anti-gender movement, and efforts to govern AI's impact on democracy.

Mitja Sienknecht is a postdoctoral researcher at the Europen New School of Digital Studies/ European University Viadrina. Her current research focuses on the transformation of war through AI technologies, the general impact of AI systems on democratic societies, and related ethical questions.

ORCID

Jelena Cupać http://orcid.org/0000-0002-7471-7624
Mitja Sienknehct http://orcid.org/0000-0001-5217-1432

Bibliography

Ananny, Mike, and Kate Crawford. "Seeing Without Knowing: Limitations of the Transparency Ideal and its Application to Algorithmic Accountability." *New Media & Society* 20, no. 3 (2018): 973–989.
Andrada, Gloria, Robert W. Clowes, and Paul R. Smart. "Varieties of Transparency: Exploring Agency within AI Systems." *AI & Society* 38, no. 4 (2023): 1321–1331.
Bogina, Veronika, Alan Hartman, Tsvi Kuflik, and Avital Shulner-Tal. "Educating Software and AI Stakeholders about Algorithmic Fairness, Accountability, Transparency and Ethics." *International Journal of Artificial Intelligence in Education* 32, no. 3 (2021): 808–833.
Borenstein, Jason, and Ayanna Howard. "Emerging Challenges in AI and the Need for AI Ethics Education." *AI and Ethics* 1, no. 1 (2021): 61–65.
Brkan, Maja. "Artificial Intelligence and Democracy: The Impact of Disinformation,: Social Bots and Political Targeting." *Delphi* 1, no. 2 (2019): 66–71.
Chadha, Anupama, Vaibhav Kumar, Sonu Kashyap, and Mayank Gupta. "Deepfake: An Overview." In *Proceedings of Second International Conference on Computing, Communications, and Cyber-*

Security, edited by Pradeep Kumar Singh, Sławomir T. Wierzchoń, Sudeep Tanwar, Maria Ganzha, and Joel J. P. C. Rodrigues, 557–566. Singapore: Springer Singapore, 2021.
Chan, Cecilia Ka Yuk. "A Comprehensive AI Policy Education Framework for University Teaching and Learning." *International Journal of Educational Technology in Higher Education* 20, no. 1 (2023): 1–25.
Coeckelbergh, Mark. *Why AI Undermines Democracy and What to Do about It*. Cambridge: Polity Press, 2024.
Davis, Austin. "The DSA Now Applies in Full: What Can we Expect?", Democracy Reporting International, 21 February 2024.: https://democracy-reporting.org/en/office/EU/publications/dsa-day-taking-stock-and-looking-ahead-to-a-super-election-year.
Diakopoulos, Nicholas. "Transparency." In *The Oxford Handbook of Ethics of AI*, edited by Markus D. Dubber, Frank Pasquale, and Sunit Das, 197–213. New York: Oxford University Press, 2020.
Diakopoulos, Nicholas. *Automating the news: How algorithms are rewriting the media*. Cambridge, Massachusetts: Harvard University Press, 2019.
DiResta, Renee, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson. "The Tactics & Tropes of the Internet Research Agency." *Congress of the United States: U.S. Senate Document*, 2019. https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1003&context=senatedocs.
Djeffal, Christian. "AI, Democracy, and the Law." In *The Democratization of Artificial Intelligence*, edited by Andreas Sudmann, 255–284. Bielefeld: Transcript, 2019.
DSA, Digital Services Act,: Regulation (EU) 2022/2065, October 19, 2022.
Edwards, Lilian. *Regulating AI in Europe: Four Problems and Four Solutions*. London: Ada Lovelace Institute, 2022.
Eubanks, Virginia. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press, 2018.
European Commission's High-Level Expert Group on Artificial Intelligence: A Definition of AI: Main Capabilities and Scientific Disciplines, Brussels, 18 December 2018.
European Commission. "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan," COM (2020) 790 final, December 12, 2020.
European Commission. *Standard Eurobarometer 98 - Winter 2022-2023. Public opinion in the European Union,* 2023. https://europa.eu/eurobarometer/surveys/detail/2872.
European Commission. "Commission is Gathering Views on Draft DSA Guidelines for Election Integrity," Press Release, 8 February 2024. https://digital-strategy.ec.europa.eu/en/news/commission-gathering-views-draft-dsa-guidelines-election-integrity.
European Parliament. "Corrigendum to the Legislative resolution of 13 March 2024 on the position of the European Parliament adopted at first reading with a view to the adoption of Regulation (EU) 2024/ … … of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139, and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797, and (EU) 2020/1828 (Artificial Intelligence Act), P9_TA(2024)0138, (COM (2021)0206 – C9-0146/2021–2021/0106(COD))".
European Parliament and the Council of the European Union: Regulation on the Transparency and Targeting of Political Advertising, PE 90 2023 INIT, February 29, 2024.
Farahany, Nita A. *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology*. New York: St. Martin's Press, 2023.
Ferrara, Emilio, Onur Varol, Clayton Davis, Filippo Menczer, and Alessandro Flammini. "The Rise of Social Bots." *Communications of the ACM* 59, no. 7 (2016): 96–104.
Floridi, Luciano. "Open Data, Data Protection, and Group Privacy." *Philosophy & Technology* 27 (2014): 1–3.
García-Orosa, Berta, João Canavilhas, and Jorge Vázquez-Herrero. "Algorithms and Communication: A Systematized Literature Review." *Comunicar* 31, no. 74 (2023): 9–21.
GDPR. General Data Protection Regulation, Regulation (EU) 2016/679, April 4, 2016.
Giannaccini, Francesca, and Tobias Kleineidam. "How the EU's Soft Touch on Open-Source AI Opens the Door to Disinformation," The Parliament, 16 April 2024. https://www.theparliamentmagazine.eu/news/article/how-the-eus-soft-touch-on-opensource-ai-opens-the-door-to-disinformation.

Gorwa, Robert, and Timothy Garton Ash. "Democratic Transparency in the Platform Society." In *Social Media and Democracy: The State of the Field and Prospects for Reform*, edited by Nathaniel Persily, and Joshua A. Tucker, 286–312. Cambridge: Cambridge University Press, 2020.

Habgood-Coote, Joshua. "Deepfakes and the Epistemic Apocalypse." *Synthese* 201, no. 103 (2023): 1–23.

Hameleers, Michael, Toni G.L.A. van der Meer, and Tom Dobber. "You Won't Believe What They Just Said! The Effects of Political Deepfakes Embedded as Vox Populi on Social Media." *Social Media + Society* 8, no. 3 (2022): 1–12.

Hamon, Ronan, Henrik Junklewitz, and Ignacio Sanchez. "Robustness and Explainability of Artificial Intelligence." *Publications Office of the European Union* 207 (2020.

Heald, David Albert. "Varieties of Transparency." In *Transparency: The Key to Better Governance? Proceedings of the British Academy*, edited by Christopher Hood, and David Heald, 25–43. Oxford: Oxford University Press, 2006.

Hildebrandt, Mireille. "Algorithmic Regulation and the Rule of Law." *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, no. 2128 (2018): 20170355. https://doi.org/10.1098/rsta.2017.0355.

Hinsch, Wilfred. "Differences That Make a Difference: Computational Profiling and Fairness to Individuals." In *The Cambridge Handbook of Responsible Artificial Intelligence*, edited by Silja Voeneky, Philipp Kellmeyer, Oliver Mueller, and Wolfram Burgard, 229–251. Cambridge: Cambridge University Press, 2022.

Ienca, Marcello. "On Artificial Intelligence and Manipulation." *Topoi* 42 (2023): 1–10.

Jacobsen, Benjamin N., and Jill Simpson. "The Tensions of Deepfakes." *Information, Communication & Society* (2023): 1–15. https://doi.org/10.1080/1369118X.2023.2234980.

Jobin, Anna, Marcello Ienca, and Effy Vayena. "The Global Landscape of AI Ethics Guidelines." *Nature Machine Intelligence* 1, no. 9 (2019): 389–399.

Jungherr, Andreas. "Artificial Intelligence and Democracy: A Conceptual Framework." *Social Media + Society* 9, no. 3 (2023): 1–14.

Kaplan, Andreas. "Artificial Intelligence, Social Media, and Fake News: Is This the End of Democracy?" In *Digital Transformation in Media & Society*, edited by Ayşen Akkor Gül, Yıldız Dilek Ertürk, and Paul Elmer, 149–161. Istanbul: Istanbul University Press, 2020.

Keller, Tobias R., and Ulrike Klinger. "Social Bots in Election Campaigns: Theoretical,: Empirical, and Methodological Implications." *Political Communication* 36, no. 1 (2019): 171–189.

Kernohan, Andrew. "Accumulative Harms and the Interpretation of the Harm Principle." *Social Theory and Practice* 19, no. 1 (1993): 51–72.

Kertysova, Katarina. "Artificial Intelligence and Disinformation: How AI Changes the Way Disinformation Is Produced: Disseminated, and Can Be Countered." *Security and Human Rights* 29, no. 1–4 (2018): 55–81.

Kolt, Noam. "Algorithmic Black Swans." *Washington University Law Review* 101, (forthcoming).

König, Pascal D., and Georg Wenzelburger. "Opportunity for Renewal or Disruptive Force? How Artificial Intelligence Alters Democratic Politics." *Government Information Quarterly* 37, no. 3 (2020): 101489.

Larsson, Stefan, and Fredrik Heintz. "Transparency in Artificial Intelligence." *Internet Policy Review* 9, no. 2 (2020): 1–16.

Laupichler, Matthias Carl, Alexandra Aster, Jana Schirch, and Tobias Raupach. "Artificial Intelligence Literacy in Higher and Adult Education: A Scoping Literature Review." *Computers and Education: Artificial Intelligence* 3, no. 100101 (2022): 1–15.

Lee, Nicole M. "Fake News,: Phishing, and Fraud: A Call for Research on Digital Media Literacy Education Beyond the Classroom." *Communication Education* 67, no. 4 (2018): 460–466.

Mansbridge, Jane, James Bohman, Simone Chambers, Thomas Christiano, Archon Fung, John Parkinson, Dennis F. Thompson, and Mark E. Warren. "A Systemic Approach to Deliberative Democracy." In *Deliberative Systems: Deliberative Democracy at the Large Scale*, edited by Jane Mansbridge, and John Parkinson, 1–26. Cambridge: Cambridge University Press, 2012.

McKay, Spencer, and Chris Tenove. "Disinformation as a Threat to Deliberative Democracy." *Political Research Quarterly* 74, no. 3 (2021): 703–717.

McSweeny, Terrell. "Psychographics,: Predictive Analytics, Artificial Intelligence, & Bots: Is the FTC Keeping Pace?" *Georgetown Law Technology Review* 2 (2018): 514.

Milan, Stefania, and Claudio Agosti. "Personalisation Algorithms and Elections: Breaking Free of the Filter Bubble." *Internet Policy Review*, 7 February (2019). https://policyreview.info/articles/news/personalisation-algorithms-and-elections-breaking-free-filter-bubble/1385.

Mogaji, Emmanuel, Sunday Olaleye, and Dandison Ukpabi. "Using AI to Personalise Emotionally Appealing Advertisement." In *Digital and Social Media Marketing: Emerging Applications and Theoretical Developments*, edited by Nripendra P. Rana, Emma L. Slade, Ganesh P. Sahu, Hatice Kizgin, Nitish Singh, Bidit Dey, Anabel Gutierrez, and Yogesh K. Dwivedi, 137–150. Cham: Springer, 2020.

Narayanan, Arvind. *Understanding Social Media Recommendation Algorithms*. New York: Kings First Amendment Institute at Columbia University, 2023.

Neuwirth, Rostam J. "Prohibited Artificial Intelligence Practices in the Proposed EU Artificial Intelligence Act (AIA)." *Computer Law & Security Review* 48 (2023): 105798.

Neuwirth, Rostam J. *The EU Artificial Intelligence Act: Regulating Subliminal AI Systems*. New York: Routledge, 2023.

O'Neil, Cathy. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown, 2017.

Susskind, Jamie. *The Digital Republic: On Freedom and Democracy in the 21st Century*. London: Bloomsbury Publishing, 2022.

Schiff, Daniel. "Education for AI,: not AI for Education: The Role of Education and Ethics in National AI Policy Strategies." *International Journal of Artificial Intelligence in Education* 32, no. 3 (2022): 527–563.

Shao, Chengcheng, Giovanni Luca Ciampaglia, Onur Varol, Kai-Cheng Yang, Alessandro Flammini, and Filippo Menczer. "The Spread of Low-Credibility Content by Social Bots." *Nature Communications* 9, no. 1 (2018): 1–9.

Shelby, Renee, Shalaleh Rismani, Kathryn Henne, Ajung Moon, Negar Rostamzadeh, Paul Nicholas, N'Mah Yilla-Akbari, et al. "Sociotechnical Harms of Algorithmic Systems: Scoping a Taxonomy for Harm Reduction." In *Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society* (2023): 723–741.

Smuha, Nathalie A. "Beyond a Human Rights-Based Approach to AI Governance: Promise,: Pitfalls, Plea." *Philosophy & Technology* 34, no. Suppl 1 (2021): 91–104. https://doi.org/10.1007/s13347-020-00403-w.

Smuha, Nathalie A. "Beyond the Individual: Governing AI's Societal Harm." *Internet Policy Review* 10, no. 3 (2021): 1–32.

Smuha, Nathalie A. "From a 'Race to AI' to a 'Race to AI Regulation': Regulatory Competition for Artificial Intelligence." *Law, Innovation and Technology* 13, no. 1 (2021): 57–84.

Tenove, Chris. "Protecting Democracy from Disinformation: Normative Threats and Policy Responses." *The International Journal of Press/Politics* 25, no. 3 (2020): 517–537.

Uuk, Risto. "Manipulation and the AI Act." *The Future of Life Institute* (2022).

van der Sloot, Bart, and Sascha van Schendel. "Procedural Law for the Data-Driven Society." *Information & Communications Technology Law* 30, no. 3 (2021): 304–332.

Veale, M., and F. Z. Borgesius. "Demystifying the Draft EU Artificial Intelligence Act—Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach." *Computer Law Review International* 22, no. 4 (2021): 97–112.

von Ungern-Sternberg, Antje. "Discriminatory AI and the Law: Legal Standards for Algorithmic Profiling." In *The Cambridge Handbook of Responsible Artificial Intelligence*, edited by Silja Voeneky, Philipp Kellmeyer, Oliver Mueller, and Wolfram Burgard, 252–278. Cambridge: Cambridge University Press, 2022.

Walmsley, Joel. "Artificial Intelligence and the Value of Transparency." *AI & Society* 36, no. 2 (2021): 585–595.

Warren, Mark E. "A Problem-Based Approach to Democratic Theory." *American Political Science Review* 111, no. 1 (2017): 39–53.

Westerlund, Mika. "The Emergence of Deepfake Technology: A Review." *Technology Innovation Management Review* 9, no. 11 (2019): 39–52.

Whyte, Christopher. "Deepfake News: AI-enabled Disinformation as a Multi-Level Public Policy Challenge." *Journal of Cyber Policy* 5, no. 2 (2020): 199–217.

Woolley, Samuel C., and Douglas Guilbeault. "United States: Manufacturing Consensus Online." In *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, edited by Samuel C. Woolley, and Philip N. Howard, 185–211. Oxford: Oxford University Press, 2018.

Yang, Weipeng. "Artificial Intelligence Education for Young Children: Why,: What, and How in Curriculum Design and Implementation." *Computers and Education: Artificial Intelligence* 3, no. 100061 (2022): 1–7.
Yeung, Karen, Andrew Howes, and Ganna Pogrebna. "AI Governance by Human Rights–Centered Design, Deliberation, and Oversight." In *The Oxford Handbook of Ethics of AI*, edited by Markus D. Dubber, Frank Pasquale, and Sunit Das, 77–106. New York: Oxford University Press, 2020.
Zachary, G. Pascal. "Digital Manipulation and the Future of Electoral Democracy in the US." *IEEE Transactions on Technology and Society* 1, no. 2 (2020): 104–112.

Appendix

Table 1. Binding and Non-Binding Documents of the European Union Relating to Digitalization.

Binding legal instruments	
Regulation and Proposals for Regulation	**General Data Protection Regulation (GDPR)**
	Digital Services Act (DSA)
	Artificial Intelligence Act (AIA)
	Transparency and Targeting of Political Advertising (TTPA)
	Digital Markets Act (DMA)
	Media Freedom Act
	Data Governance Act
	Cybersecurity Act
	Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data by the Union Institutions, Bodies, Offices, and Agencies and on the Free Movement of Such Data
	Gigabit Infrastructure Act
	European Digital Identity
	The European Health Data Space
	Data Act
	Chips Act
	Proposal for Regulation on the Digitalization of Judicial Cooperation and Access to Justice in Cross-Border Civil, Commercial and Criminal Matters, and Amending Certain Acts in the Field of Judicial Cooperation
	Proposal for Amending Regulation (EU) No 904/2010 as Regards the VAT Administrative Cooperation Arrangements Needed for the Digital Age
Directives	Data Protection Law Enforcement Directive
	e-Privacy Directive
	Directive on combating the sexual abuse and sexual exploitation of children and child pornography
	Audiovisual Media Services Directive (AVMSD)
	Directive concerning measures for a high common level of security of network and information systems across the Union
Non-Binding Legal instruments	
Declarations	**Declaration on European Digital Rights and Principles for the Digital Decade**
	Declaration: Cooperation on Artificial Intelligence
Communications	**Communication on protecting election integrity and promoting democratic participation**
	Tackling Online Disinformation: a European Approach
	Action Plan against Disinformation
	Artificial Intelligence for Europe
	Coordinated Plan on Artificial Intelligence
	Building Trust in Human Centric Artificial Intelligence
	Fostering a European Approach to Artificial Intelligence (+Annex)
	Protecting Election Integrity and Promoting Democratic Participation
	Digitalization of Justice in the European Union
	EU Policy on Cyber Defence
	Media and Audiovisual Action Plan
	European Strategy for Data
	Digital Education Action Plan 2021–2027
	A Chips Act for Europe

	Digitalization of Justice in the European Union
	Union of Equality: Strategy for the Rights of Persons with Disabilities (2021-2030)
	A Digital Decade for Children and Youth: The New European Strategy for a Better Internet for Kids (BIK+)
	A European Health Data Space: Harnessing the Power of Health Data for People, Patients and Innovation
	A European strategy on Cooperative Intelligent Transport Systems, a Milestone Towards Cooperative, Connected and Automated Mobility
	FinTech Action plan: For a more competitive and innovative European financial sector
White papers	**White Paper on Artificial Intelligence: A European Approach to Excellence and Trust**
Non-legal instruments	
Policies, Programmes, Initiatives	**Shaping Europe's Digital Future**
	European Democracy Action Plan
	Digital Education Action Plan 2021–2027
	European Green Digital Coalition
	Next Generation Internet Initiative (NGI)
	Policy Guidance on AI for Children
	Global Gateway
	Get Digital Initiative
Codes of Practice	**The Strengthened Code of Practice on Disinformation**

Table 2. Classification of the EU's measures to mitigate AI harm to democracy*.

		Transparency				
EU documents	Prohibition	Transparency to individual	Operational transparency	Reporting Transparency	Risk management	Education**
GDPR	Articles 9	Articles 5, 6, 7, 8, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 34	Articles 25, 30, 32, 40, 41, 42	Article 31, 47	Articles 33, 35, 36	Article 57
DSA	Articles 25, 26, 28	Articles 14, 17, 20, 26, 27, 28, 38, 39	Articles 37, 40, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77	Articles 10, 15, 24, 42	Articles 9, 16, 18, 22, 23, 34, 35, 36, 48	
AIA	Article 5	Articles 13, 50	Articles 10, 11, 12, 13, 15, 17, 18, 19, 44, 47, 48, 49, 53, 55, 77	Article 20, 27, 52, 77, 91	Articles 9, 14, 15, 20, 27, 43, 55, 57, 60, 72, 73,74, 75, 76, 89, 90	Article 3
TTPA	Article 18	Articles 11, 12, 18, 19	Article 9, 19	Articles 14, 16, 17, 20	Article 15, 19	

*The table selectively highlights articles most pertinent to rights-based and systemic AI harm to democracy, excluding those with lesser relevance. Articles may cross several categories, reflecting their interconnected roles in the documents.

** The EU deals with education-related measures primarily in its non-binding legal instruments and non-legal instruments while regulations only sporadically cover this aspect.