DE GRUYTER

Int. J. Digit. Law Gov 2024; 1(1): 29–51

Le Cheng and Xiuli Liu*

Unravelling Power of the Unseen: Towards an Interdisciplinary Synthesis of Generative AI Regulation

Abstract: The regulations of generative AI, typified by ChatGPT and Sora, have become one of the most influential alternative technological imaginaries. Developed by states and civil society groups, such regulations are triggering a broad range of social actors seeking to nominalize the AI-related behavior. Against this backdrop, this study starts with interrogating the semiotic character of generative AI. Do these regulations support the AI futures, or do they involve a mere change in the social actors who benefit from the technological status quo? To answer this question, this study examines the rhetoric and realization of AI regulations by the European Union and the United States. The findings reveal a degree of AI regulatory alignment between the European Union and the United States, but these two jurisdictions also highlight and predict some structural challenges. Drawing upon the concept of panopticism by Foucault, the study explores the foundational origins of challenges by dissecting the (in)visibility of AI power. It underscores the necessity of regulating the power of the unseen and proposes a synthetic generative AI regulatory framework. We finally conclude that the integrity of sociosemiotics and panopticism provides a productive and paramount framework for understanding the powerful new capacities of AI-related regulations.

Keywords: generative AI; signifier; synthetic regulation; panopticism; (in)visibility; interdisciplinary

1 Introduction: Disentangling Generative AI

Embarking on a profound and potentially revolutionary trajectory of transformation, artificial intelligence (hereinafter referred to as AI) accelerates at unprecedented

*Corresponding author: Xiuli Liu, School of International Studies, Zhejiang University, Hangzhou, China, E-mail: liuxiuli@zju.edu.cn. https://orcid.org/0000-0001-8534-6753
**Le Cheng**, Guanghua Law School and School of Cyber Science and Technology, Zhejiang University, Hangzhou, China, E-mail: chengle163@hotmail.com. https://orcid.org/0000-0002-4423-8585

speed. Against this backdrop, AI is gaining perpetual momentum and has become a key component of organizational operations and everyday life (Desouza, Dawson, and Chenok 2020; Mikalef et al. 2022; Raisch and Krakowski 2021). At the technical level, AI functions as a system capable of imitating human cognitive abilities (Dennett 1990; Salomon 1988) and performing human-like behavior (Forbus and Hinrichs 2006). For instance, AI technologies are utilized for purposes such as speech recognition (e.g., Ran, Wang, and Qin 2021), computer vision (e.g., Wiley and Lucas 2018), machine translation (e.g., Wilks 1972), and machine learning (e.g., Linardatos, Papastefanopoulos, and Kotsiantis 2020), to name a few, depending on different application objectives. It is thus not surprising that Big Tech companies such as Google, Microsoft, Tencent, and others have initiated AI-related innovation and application competitions, in order to capture a larger market share. Apart from the technological attention, the "AI race" at both national and supranational levels (Hull et al. 2022) has become a matter of global dominance. AI-related research has thus sparked widespread interest across various sectors of society, including national research funders, which makes it the focus of academic attention. Governments generally support local AI research with a focus on AI strategy comparisons between nations and domestic public-private partnerships (e.g., Saran, Natarajan, and Srikumar 2018). Critical scholars focus on how AI technologies change the way social works (e.g., Kitchin and Lauriault 2014). Ethicists emphasize ethical principles and guidelines that should be considered in the design and actual operation of AI systems (e.g., Díaz-Rodríguez et al. 2023; Mcmillan 2023). Legal scholars and sociologists prioritize deep-seated systemic issues such as inequality (e.g., Wachter, Mittelstadt, and Russell 2021) and injustice caused by AI. AI-related research in each field has its own language, logic, and inquiries to be explored. Analogous to the ongoing convergence observed in pioneering investigations across the global AI landscape, there exists an anticipation within AI research for heightened interdisciplinary and cross-sector inquiry. Positioned at the nexus of legal studies, semiotics, discourse-power theory, and the perspective of panopticism, this study aims to produce fresh insights into AI regulation through the synthesis of different disciplinary perspectives.

1.1 Generative AI as a Floating Signifier

There is no doubt that the evolution of generative AI models has become the highlight and the latest frontier of AI technology and digital transformation. From a socio-semiotic perspective, generative AI can be defined as a sign infused with social political and economic elements, which has performative effects that align with the interests of vested stakeholders in the domain. In this sense, generative AI can be seen as a "floating signifier" which was named by the anthropologist Claude (1987).
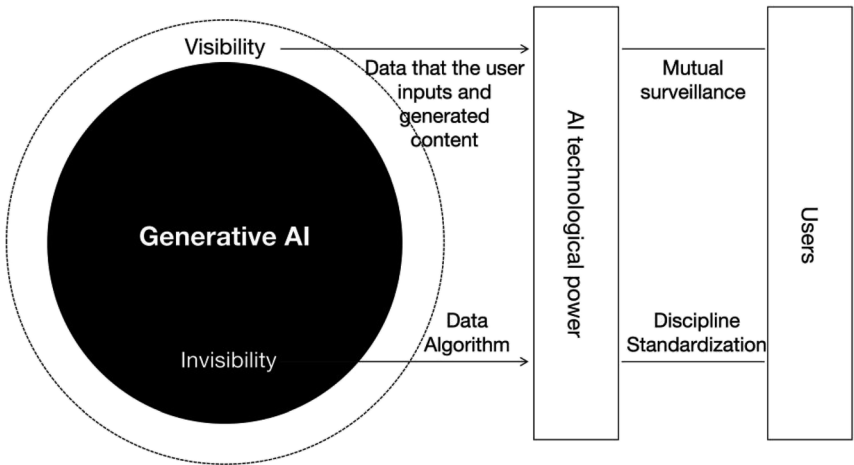
Figure 1: Visibility and Invisibility of generative AI.

While generative AI as a term performs a function that suggests a specific referent, in order to maximize its suggestive power, overly stringent definition should be avoided as much as possible. What we call "floating" is compatible with the iterative and evolutionary nature of generative AI. Firstly, the technical flexibility and the evolutionary characteristic of generative AI make it challenging to provide a fixed definition of such an object. Generative AI models leverage deep neural networks to learn patterns and structures from large training corpus to generate new content (Cheng and Liu 2023). This technology can generate various forms of content such as text, images, audio, animations, source code, and other data types in a continuous way. The most typical models in this regard include ChatGPT and Sora. It significantly expands the potential of chatbots through the integration of deep learning and language models built on the Generative Pre-trained Transformer (GPT) architecture (Radford et al. 2018). For instance, ChatGPT generates human-like responses to inquiries that are similar to those of human experts by combining supervised fine-tuning with unsupervised pre-training. In this sense, generative AI models can be seen as a dynamic ecosystem that is continually evolving and floating. Secondly, the vague definition also aims to maximize the operational space of generative AI models. Following the path of GPT, GPT-2, and GPT-3, Open AI has launched a more complex and powerful language model GPT-4, which is the latest milestone in OpenAI's expansion of deep learning. As a large multimodal model (accepting image and text inputs, emitting text outputs), while not as capable as humans in many real-world scenarios, it exhibits human-level performance on a

variety of professional and academic benchmarks (Open AI 2024). Widespread global adoption of ChatGPT has demonstrated the vast range of use cases for this technology, including software testing, poetry, prose, business correspondence, and contracts (Dwivedi et al. 2023).

Drawing from the linguistic theories of de Saussure (2011), the data utilized for training Large Language Models (LLMs) embody only form without inherent meaning, implying that generative AI systems have no access to *signifieds*, only *signifiers* (Magee, Arora, and Munn 2023). Generative AI as a signifier involves understanding how it represents a meaning (Wagner, Matulewska, and Cheng 2020) within the domain of digital society. Firstly, in its tangible form, generative AI can be seen as a signifier through its physical representation such as hardware components and software systems. In addition to its physical form, generative AI can also serve as a conceptual signifier which encompasses algorithms, automation and deep learning. It represents that generative AI models can perform human-like behavior. Generative AI as a sign also carries cultural and social meanings (Cheng, Cheng, and Sin 2014). It symbolizes the technological extension of the human imagination, which in turn reshapes human cognition. The interpretation and re-interpretation of generative AI as a signifier fluctuates depending on the context of its use and the viewpoints of diverse stakeholders. For instance, generative AI can signify technological innovation and more opportunities, while also raising concerns about regulations, data protection and ethical implications.

In essence, understanding generative AI as a floating signifier requires acknowledging its evolutionary and multifaceted nature. It is imperative to recognize it as both a product of technological advancement and a symbol within societal and cultural contexts. At the level of potentiality, it represents the "infinite" extension of human imagination and thought at the technical level, while on the level of feasibility, it requires "finite" regulation within the confines of human ethics and rules.

1.2 Risks Call for Regulations

We are witnessing the quantum leap in generative AI technology, with new large-scale models being launched on almost a weekly basis. This transformation is reshaping the way humans work and communicate (Hacker 2023). The latest wave and profound impact of generative AI have raised many concerns around potential and actual risks in the form of discrimination, privacy violations, manipulation, disinformation, amplification of bias, and unaccountable decision-making (Bakiner 2023).

The risks and challenges posed by generative AI are primarily concentrated in five main aspects. The first is the ethical risk and the potential for social alienation, which is manifested predominantly through the amplification of societal biases, discrimination, and inequalities, particularly evident in the domain of recruitment (Raub 2018). The second risk relates to intellectual property infringement, which is highly likely to occur when data is inputted into generative AI models without authorization from data providers. The third risk pertains to privacy and data protection, concerning the lawful and compliant collection and processing of data, as well as the handling of sensitive personal information. The fourth risk involves monopoly, which stems from the innovative characteristics of generative AI that result in significant entry barriers, leading to a high concentration of pertinent technology and market among current tech giants and potentially inhibiting the growth of small tech innovators (Cheng and Liu 2023). The fifth risk concerns cybercrime and data security, where the shift in paradigms of cybersecurity attacks and defences related to generative AI (Aksela et al. 2022) indicates an urgent need for further updates in both the preparedness level of cybersecurity agencies and measures to combat cybercrime.

Hence, to foster justice, it is crucial not just to grasp the essence of technology but to overhaul our regulatory outlook towards it. This shift, towards a top-down regulatory approach, is vital for promoting the benevolent evolution of generative AI. However, this poses a challenge to developing comprehensive and critical regulatory theory and, more crucially, to informing national AI strategies, supporting inclusive generative AI innovation, and implementing regulatory guidelines that can counteract its harms (Tacheva and Ramasubramanian 2023). To address these issues and create a shared regulatory framework capable of harmonizing different regulatory stances, we propose an examination of generative AI through the analytical perspective of "panopticism" (Foucault 1977).

The analysis proceeds in four steps. First, the article disentangles the meaning of generative AI, with a perspective of semiotics. Second, it traces the global trends in AI regulation, drawing primarily on the European Union (hereinafter referred to as the EU) and the United States (hereinafter referred to as the US). Third, the article uncovers the challenges associated with regulating AI-related power, and upon reflection through the lens of panopticism, it underscores the pressing need and necessity for regulating the power of the unseen. Finally, this study draws a conclusion on the future of synthetic generative AI regulation.

2 Global Trends in AI Regulation: Encounters and Contradictions

The international community is committed to continuously promoting the ethical development of AI. For instance, the United Nations Educational, Scientific and Cultural Organization produced the first-ever global standard on AI ethics, the Recommendation on the Ethics of Artificial Intelligence, which articulates 10 principles including proportionality and non-maleficence, safety and security, fairness and non-discrimination. Since 2018, the EU has persistently propelled the design, development, and deployment of AI, while working to regulate the use and management of AI and robots. The EU Artificial Intelligence Act (hereinafter referred to as the EU AI Act), which came into effect in early 2024, has promoted this effort to a climax (Veale and Zuiderveen Borgesius 2021), and even become a milestone in global AI regulation. The US places greater emphasis on AI development and innovation, primarily regulating AI through the Blueprint for an AI Bill of Rights (hereinafter referred to as the Blueprint). Given the relatively mature and representative nature of the AI governance measures in the EU and the US, the following analysis takes these two jurisdictions as cases to explore differing regulatory paths, with the aim of offering insights into the healthy development and effective governance of AI globally.

2.1 A Corpus Analysis of the AI Regulation

To compare the AI regulatory approaches between the EU and the US at the text level, we built two corpora: the EU corpus (hereinafter referred to as EUAIC) and the US corpus (hereinafter referred to as USAIC). Table 1 presents detailed information about the two corpora.

The following analysis was carried out in three steps. First, the materials for the two corpora were converted to plain text files, then into a corpus analysis tool *Lancsbox* (Brezina, McEnery, and Wattam 2015). Second, we conducted a keyword

Table 1: Information of the two corpora.

Corpus	EUAIC	USAIC
Tokens	46,660	30,513
Lemmas	2801	4160

analysis by comparing each corpus with the BNC to retrieve keywords. Keywords were identified by integrating relative frequency and Log Ratio statistics. After excluding Arabic numerals, we identified the top 30 keywords from each corpus for comparison, ensuring that the frequency of occurrence of each keyword exceeded 10 per cent of the text in each corpus (see Table 2). Third, we categorized the retrieved keywords into thematic groups, in order to obtain insights into the differing emphasis and shared concerns of the two jurisdictions in AI regulation with the

Table 2: The top 30 most significant words in EUAIC and USAIC.

Rank	EUAIC		USAIC	
	word	rel. freq.	word	rel. freq.
1	Regulation	14.67	Automated	13.76
2	High-risk	14.35	Technologies	12.83
3	EU	13.75	Algorithmic	12.77
4	Conformity	13.52	Blueprint	12.72
5	Referred	13.18	Protections	12.70
6	Notified	12.76	Surveillance	12.70
7	Requirements	12.67	Federal	12.40
8	Competent	12.61	Practices	12.40
9	Obligations	12.60	Expectations	12.25
10	Fundamental	12.55	Harms	12.25
11	Directive	12.46	Domains	12.18
12	Proposal	12.42	Center	12.00
13	Annex	12.40	Fallback	12.00
14	Assessment	12.35	Algorithms	11.88
15	Compliance	12.33	Panelists	11.83
16	Provider	12.30	Contexts	11.83
17	Enforcement	12.26	Discrimination	11.72
18	Surveillance	12.20	Tailored	11.70
19	Documentation	12.20	Assessments	11.70
20	Accordance	12.08	Assessment	11.70
21	Biometric	12.03	Deployment	11.60
22	Identification	12.03	Mitigation	11.60
23	Applicable	11.96	Outcomes	11.54
24	Regulatory	11.79	Sectors	11.37
25	Providers	11.67	Evaluation	11.37
26	Implementation	11.57	Ensuring	11.31
27	Appropriations	11.53	Concerns	11.31
28	Pursuant	11.38	Timely	11.25
29	Institutions	11.35	Communities	11.25
30	Harmonised	11.26	Accessibility	11.18

Table 3: The thematic categorization of AI regulation keywords.

Themes	Keywords in EUAIC	Keywords in USAIC
Actions	Regulation, conformity, referred, notified, requirements, assessment, compliance, enforcement, accordance, regulatory, implementation	Protections, practices, tailored, assessments, assessment, deployment, mitigation, evaluation
Actors	EU, provider, providers, institutions	Federal, panelists, sectors, communities
Issues	High-risk, competent, obligations, fundamental, directive, proposal, annex, surveillance, documentation, biometric, identification, applicable, appropriations, harmonised	Automated, technologies, algorithmic, blueprint, surveillance, expectations, harms, domains, center, fallback, algorithms, contexts, discrimination, outcomes, concerns, timely, accessibility

support of a closer concordance analysis. We eventually categorized the keywords into three themes as listed in Table 3: (i) actions: keywords related to measures and governance in AI regulation; (ii) actors: keywords pertaining to subjects or regulatory entities involved in AI regulation; (iii) issues: keywords associated with key concerns in AI regulation. To delve deeper into how these keywords function within specific themes, we further conducted the concordance analysis for a more detailed examination.

The very initial findings of the data analysis reveal some general differences between the regulatory approaches of the EU and the US. Firstly, concerning the theme of "actions", the EU appears to prioritize regulatory measures aligned with "hard law" more than the US does. The frequent occurrence of keywords such as "regulation", "regulatory", "enforcement", and "requirements" in the EUAIC most directly underscores this point. Additionally, keywords such as "conformity", "referred", "compliance", and "accordance" belong to the semantic category of relational terms, which refers to the state of being in agreement, adherence, or alignment with a particular standard, request, command, or expectation. Pragmatically, they can be used to persuade, command, request, or describe actions and behavior within the context of AI societies or institutions. For instance, in the case of "referred", the word is repeatedly used in the EU AI Act text to connect some annexes, decisions and other articles in the text, to achieve a legal citation effect through intertextuality (Cheng and Sin 2008), which further underscores the necessity of compliance with legal regulatory documents at different levels. In addition, although "assessment" appears frequently in both corpora, it is evident that within the USAIC, there is a greater prevalence of terms expressing evaluative connotations, such as "assessment(s)" and "evaluation". This phenomenon indicates a regulatory emphasis in the US on self-regulation and self-assessment within AI enterprises, wherein even

third-party evaluations operate within the realm of social regulation rather than direct legally coercive mandates.

(1)   [EUAIC.txt] As regards stand-alone high-risk AI systems that are *referred* to in Annex III,

(2)   [EUAIC.txt.] and the detection, localisation, identification or prosecution of perpetrators or suspects of the criminal offences *referred* to in Council Framework Decision 2002/584/JHA if those criminal offences are punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least 3 years and as they are defined in the law of that Member State.

(3)   [EUAIC.txt.] The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives *referred* to in paragraph 1 point d) shall take into account the following elements

Secondly, concerning the theme of "actors", it can be observed that the EU emphasizes regulation of the subject of obligations, whereas the US prioritizes coordination among various stakeholders. Within the EU AI Act, "provider(s)" is conceptualized in relation to the user. Within this dichotomous framework, users of AI systems are typically the party whose rights are protected, while providers are tasked with obligations or responsibilities. In the Blueprint, however, greater emphasis is placed on coordinating interests across different sectors to ensure that AI systems serve the specific interests of different specific industries.

(4)   [EUAIC.txt] It is appropriate that a specific natural or legal person, defined as the *provider*, takes the responsibility for the placing on the market or putting into service of a high-risk AI system, regardless of whether that natural or legal person is the person who designed or developed the system.

(5)   [EUAIC.txt] This Regulation should also apply to Union institutions, offices, bodies and agencies when acting as a *provider* or user of an AI system.

(6)   [USAIC.txt] These tools now drive important decisions across *sectors*, while data is helping to revolutionize global industries.

(7)   [USAIC.txt] Future *sector*-specific guidance will likely be necessary and important for guiding the use of automated systems in certain settings such as AI systems used as part of school building security or automated health diagnostic systems.

From the theme of "issues", we can find a shared concern between the EU and the US: "surveillance", which will be discussed in the following part from the perspective of panopticism. Furthermore, it is evident that "high-risk" ranks first in frequency of occurrence as a keyword in the EUAIC, reflecting a significant aspect of the EU AI

regulation, which employs a risk-based approach to AI governance. Another notable feature of the EU AI Act is indicated by "harmonised". This term co-occurs with "rules" or "standards" in the EUAIC. This reflects the EU's endeavour to establish uniform standards applicable within the EU and extend its ambition beyond EU borders, which is similar to its efforts and global impact achieved with GDPR (Bennett 2018).

(8)   [EUAIC.txt] This explanatory memorandum accompanies the proposal for a Regulation laying down *harmonised* rules on artificial intelligence (Artificial Intelligence Act).

(9)   [EUAIC.txt] the proposal defines common mandatory requirements applicable to the design and development of certain AI systems before they are placed on the market that will be further operationalised through *harmonised* technical standards.

Meaningful textual analysis, interpretation, and re-contextualization can only be achieved in its specific social context (Cheng and Machin 2023). Therefore, we will extend to the text-external factors like social, political and legal contexts to explore the different regulatory paths of the EU and the US.

2.2 The EU Approach: Prioritizing Safety While Ensuring Fairness

In terms of the legislative process, in April 2021, the European Commission issued a "Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts", which initiates the "hard law" trajectory of AI governance. By December 2022, the final version of the compromise draft of the EU AI Act was formulated. In June 2023, the European Parliament adopted a negotiating mandate draft for the AI Act and revised the original proposal. On December 8, 2023, the European Parliament, the Council of the European Union, and the European Commission reached an agreement on the AI Act, which stipulates comprehensive regulation of AI. On 13 February 2024, the European Parliament adopted the final text of the EU AI Act in a joint vote.[1] Overall, the EU AI Act establishes an ethical and legal framework for AI development and usage within the EU, supplemented by the Artificial Intelligence Liability Directive to ensure effective implementation. The

---

1 European Parliament. *Legislative Train Schedule of Artificial Intelligence Act.* https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence (accessed January 8, 2024).

discussions surrounding the EU AI Act predominantly revolve around the following aspects:

Firstly, the definition of AI and the scope of the Act. Article 3 (1) of the proposed version defined "AI system" as software developed with one or more of the technologies and approaches that can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with. This definition was broad and may encompass a wide range of software traditionally not considered as AI, which could be detrimental to AI development and governance. Henceforth, the current version constrains the definition of AI to "machine learning or logic and knowledge-based systems", designed to operate at varying degrees of autonomy, and capable of influencing outputs such as predictions, recommendations, or decisions within physical or virtual environments, either explicitly or implicitly directed towards specific goals. Simultaneously, it omits Annex I and the authorization for the European Commission to amend the definition of AI. Regarding its scope of application, the AI Act extends its jurisdiction beyond the borders of the EU, encompassing all providers and deployers of AI systems, irrespective of whether they are established within the EU or in third countries. Additionally, it extends to all distributors, importers, authorized representatives of providers, manufacturers of products established or situated within the European Union, and EU data subjects whose health, safety, or fundamental rights might be significantly impacted by the use of AI systems.

Secondly, the regulatory approach of AI. The EU AI Act proposes a proportionate risk-based approach that imposes regulatory burdens solely when an AI system is likely to present high risks to fundamental rights and safety (Chamberlain 2023). The first is unacceptable risk, which is prohibited from deployment by any company or individual. The second is high risk, which allows relevant parties to market or utilize the AI system only after fulfilling obligations such as pre-assessment, while mandating continuous monitoring during and after deployment. The third is limited risk, exempting the need for special licenses, certifications, or reporting obligations, but the principle of transparency should be followed to allow appropriate traceability and interpretability. The fourth is minimal risk, which can be deployed and used according to the free will of the corresponding subject.

2.3 The US Approach: Emphasizing Self-Regulation and Supporting Technological Innovation

Against the backdrop of global deliberations on AI legislation and policy-making, the US has gradually formulated a regulatory framework based on the voluntary

principle. A comprehensive regulation in the US is the Blueprint, released by the White House Office of Science and Technology Policy in October 2022, which aims to support the protection of civil rights throughout the design, deployment, and governance processes of automated systems.[2] Specifically, the right-oriented framework leads with a declaration of national values, supplemented with diverse resources and best practices, aimed at fostering greater transparency and reliability in automated systems and decision-making processes. The Blueprint contains five principles: safe and effective systems, algorithmic discrimination protections, data privacy, notice and explanation, and alternative options. As the aforementioned principles lack regulatory enforcement, the Blueprint does not constitute a legislative and executable Act for rights protection; rather, it serves as a forward-looking governance blueprint rooted in future aspirations.

Presently, the US Congress has adopted a relatively non-interventionist approach to AI regulation, despite indications from Democratic leadership of plans to propose a federal law aimed at regulating AI. US Senate Majority Leader Chuck Schumer has proposed a safe innovation framework, which outlines four pillars that he hopes will guide future legislation governing AI: security, accountability, protecting foundations and explainability. However, this framework is not legislative text, and it is not clear how long it will take to begin putting together legislative proposals. Confronted with strategic competitive pressures brought about by the EU AI Act and the broad-ranging security risks posed by generative AI, federal agencies in the US have embraced a proactive stance, engaging in regulatory oversight within their jurisdictional purview.

3 Challenges in Regulating AI-Related Power: Perspective of Panopticism

Technological progress is fundamentally positive because it directly contributes to improving the key aspects of human life (Tacheva and Ramasubramanian 2023) and liberating social productivity significantly. However, we also need to acknowledge that while AI technology fosters a more liberated and interconnected world, it also perpetuates and strengthens longstanding systems of surveillance and power oppression, even in a more covert manner. As previously mentioned, both the EU and the US have placed significant emphasis on surveillance within their AI regulatory

---

2 The White House. *Blueprint for an AI Bill of Rights*. https://www.whitehouse.gov/ostp/ai-bill-of-rights/. (accessed January 4, 2024).

frameworks, which is triggered by the inherent nature of AI and its path of technological advancement.

In order to track individuals' roles and positions in the world, AI necessitates constant surveillance and collect more data to update its own systems. This phenomenon constitutes a crucial aspect of what is commonly referred to as "surveillance capitalism" (e.g., Aho and Duffield 2020; Zuboff 2015, 2023), which is further magnified and highlighted within the AI context. The origins of this type of surveillance can be found in the idea of the "panopticon", which was first put forth by the British philosopher Bentham in the 18th century (Galič, Timan, and Koops 2017; Steadman 2012). The French philosopher Michel Foucault further developed this idea in the 20th century as part of his theory of discourse on power relations. In light of the changing social tendencies brought about by contemporary technology and digital transformation, "panopticism" has become a key social metaphor (Fludernik 2017) concerning power distribution.

3.1 (In) Visibility of Generative AI

This sub-section mainly takes the notion of "panopticism" and uses it to examine generative AI as a sign, breaking it down into two categories: visibility and invisibility (see Figure 1). Within these two discrete dimensions, it draws conclusions regarding regulatory approaches and power relations of generative AI. This study advocates for the manifestation of technical power in the AI society in an invisible, automatically operational manner, which achieves the apparent effect of separation of power and human beings. This portrayal clothes power in a guise of technical neutrality, thereby making individuals compliant, dependent, and compliant with standards.

In accordance with the panoramic prison theory of Bentham and Foucault, within the digital space under the control of algorithmic or AI power (Beer 2009), ordinary people are in a state of surveillance. Unlike social norms established by humans in traditional societies, in the digital or AI space, standards prioritize technical criteria, which forms a normalization of standards at the technical level and penetrates civil society in a more covert way. Netizens become the object of technological discipline, while large Internet enterprises and AI technology companies wield the power to discipline. At this juncture, it is imperative to regulate and control the technological power to prevent power generalization.

The underlying logic here is that this innovative, explosive technology exerts both visible and invisible forms of disciplinary power over traditional society. In situations where technological power holds a dominant position, the invisible dimension far surpasses the visible power, resulting in an iceberg effect. In the domain of generative AI, the visible aspect of technological power can be perceived

by the user, which is embodied in the input of data and instructions and the output of generated content (Onitiu 2021). While users enjoy the transformative breakthrough brought by science and technology, they rely on it in a proactive way (Brandtzaeg, Skjuve, and Følstad 2022). To a certain extent, users are willing and active to feed data to generative AI models and expect it to generate content they want for efficiency improvement and convenience in their work or life. Furthermore, many users take advantage of this instrumental nature for their own benefit. In this dimension, users and owners of technological power are in a state of mutual surveillance, engaged in interactive dynamics without unilateral exploitation or oppression.

This is only the visible dimension at the superficial level. Generative AI has sparked discussions and fears across various sectors of society (Ray 2023), not only among the general public but also among leaders in all walks of life. In the face of such tools, the expert identity will be stripped away and transformed into mere users. This underscores that every user is under the discipline of technical power when confronted with groundbreaking technology. This is also one of the reasons to regulate AI-related power. Under this power situation, which involves a game between technological power and traditional social power, regulatory authority must come into play. Appropriately limiting the generalization of technological power and incorporating human care and ethical considerations are needed to preserve human dignity.

The other dimension is the invisible power. Unlike previous technological revolutions and transformations (Song and Ma 2022), the invisible scope of Generative AI is broader, and its rapid iteration of technology brings greater unknown fears to society. This invisible dimension primarily refers to the layers of data, algorithms, and code. These highly technical domains are incomprehensible to most users and may even be mythologized, which exacerbates fear of AI technology at the cognitive level. This extends to the demand for transparency in AI. Therefore, based on this logic, the future focus of regulating generative AI should be on regulating the invisible dimension, namely, the deeper levels of algorithms and data.

The essence of this AI technological power is not fixed or absolute but rather a form of relational power. It can only develop positively when subject to regulatory constraints (Buiten 2019). Once technological power becomes absolute, it will lead to disorderly expansion and malignant development. At the societal level, it can provoke greater cognitive panic, resulting in group irrationality and active restrictions on technological development. Positive development requires legislators and regulators to deeply understand the underlying logic of technology and the characteristics of the invisible dimension of AI-related power. It is necessary to propose targeted regulatory suggestions, impose certain restrictions from a legal perspective, dispel technological fears at the societal level, and fully respect and protect human rights. Only then can technology be fostered towards benevolent development.

3.2 Structural Challenges of the AI-Related Regulation

The widespread adoption of AI technologies changes the ethical, sociological, and political boundaries of the regulatory framework in other ways. AI-related regulation reproduces long-term, structural problems going beyond issue-by-issue regulation, is embedded within social structures that produce cumulative effects and introduces additional challenges that require a discussion about the relationship between regulation and AI technology (Bakiner 2023).

The EU aims to establish global standards for AI regulation through the AI Act, thus enabling Europe to gain an advantage in the international AI competition. The AI Act sets relatively reasonable rules for governing AI systems, which to some extent can mitigate discrimination, surveillance, and other potential harms, especially in areas related to fundamental rights. For instance, the AI Act prohibits certain uses of AI, such as facial recognition in public spaces. However, the AI Act also has shortcomings in aspects such as risk classification, regulatory intensity, rights protection, and liability mechanisms. For instance, it adopts a horizontal legislative approach, which attempts to encompass all AI systems under regulatory scope without delving into the differing features among them. This may result in challenges in the implementation of relevant risk prevention measures. The current EU framework for AI regulation unjustifiably collapses fundamental distinctions between social and individual risk by equating high-risk AI systems in the AI Act with those under the liability framework (Hacker 2023). The challenge in the current AI regulatory path in the US lies in its focus on applying existing laws to AI rather than enacting specialized AI legislation. At present, the US Congress has not yet reached a consensus on the federal legislation of AI regulation, including specifics such as regulatory frameworks and risk classification. Consequently, it will likely take a considerable amount of time for federal-level AI regulatory legislation to emerge in the US.

Building upon the analysis conducted from the perspective of panopticism, which examines visibility and invisibility, this study further proposes an analysis of the challenges in regulating AI-related power along these two dimensions. The dimension of visibility includes issues of input and output quality, while the dimension of invisibility involves process-related concerns. These two dimensions collectively lead to the challenges of legal regulation risks.

The first is the issue of input quality. AI is composed of algorithms, computing power and data elements, with data serving as its foundation (Mantelero 2018), to a certain extent determining the accuracy and reliability of its outputs. Generative AI is a subtype of AI, so its outputs (generated content) are similarly influenced by

the quantity and quality of data. Generative AI must be trained with high-quality data (Whang et al. 2023); once the dataset is contaminated or tampered with, the generative AI may damage the basic rights of users, intellectual property rights, personal privacy and information data rights, and even produce social bias. The second issue pertains to output quality. In essence, risks stem from people's inadequate understanding and control over phenomena (Lupton 2013: 3), which leads to an inability to solve the problem in time before it sprouts or even erupts. From this perspective, the level of controllability of technology is inversely proportional to its associated risks; the more difficult a technology is to control, the higher the risks. Large language models endow generative AI with logical deduction capabilities, yet also render its output increasingly unpredictable. In other words, the controllability of generative AI is relatively low, thus posing higher potential risks. For instance, due to social and cultural disparities, the output of generative AI models may be appropriate in one cultural context but offensive in another. Humans can discern such differences, but generative AI may inadvertently produce inappropriate content (Jo 2023) due to a lack of cultural pre-design, thus failing to differentiate subtle cultural nuances. The third is the concerns in the processing stage. Apart from data, the algorithmic models used during training also impact the output of generative AI (AbuMusab 2023). Even with high-quality data, if the chosen algorithmic model is flawed or not aligned with the intended purpose, it cannot yield a well-performing AI system. Issues of AI discrimination and bias stemming from machine learning algorithms and training data are collectively referred to as pre-existing algorithmic biases (Bozdag 2013), contrasting with emergent algorithmic biases triggered by the emergence of new knowledge, formats, or scenarios. Technological advancements have not eradicated the problem of fake generation; rather, they have merely repackaged and disguised it. Therefore, generative AI often encounters emergent algorithmic biases, further increasing risks and challenges (Simon et al. 2020). The input quality problems, processing problems and output quality problems of generative AI push the regulatory difficulty to a new peak, resulting in the legal risk of regulatory failure. The legal risks of generative artificial intelligence are not limited to a specific field, but cross multiple fields and require the collaborative governance of multiple departments.

The challenges related to the quality of input, processing, and output of generative AI have pushed regulatory difficulties to a new peak, which leads to the legal risk of invalid regulation. The legal risks associated with generative AI are not limited to any specific field but cut across multiple sectors and require coordinated governance across various stakes.

4 Prospects: A Synthetic Generative AI Regulation

Despite some relevant contradictions, the approaches to AI regulation in the EU and the US focus on regulating the field through market-driven and technical standards, which are concerned with avoiding high-risk and safety issues (Amariles and Baquero 2023) to instruct the AI systems designation. However, they do not seem primarily concerned with the development of a synthetic human-centric AI regulation. The "hard" governance mechanisms such as legislation and regulator frameworks provide insufficient protection to individuals and society (Morley et al. 2021; Taeihagh 2021). In an attempt to overcome these limitations, it is suggestive to formulate "soft" governance mechanisms such as ethics, guidelines, and policy strategies (Radu 2021). In this paper, we argue for a synthetic approach to tackle these limitations and challenges. This synthetic approach does not entail specific standards and rules but rather applies dynamically in regulation in a manner compatible with generative AI, which functions as a "floating signifier".

The first is the regulation of the AI-related power of the unseen. It emphasizes the regulation of data and algorithms as the fundamental logic of generative AI. Algorithms are the key productivity components of generative AI models and are the driving force behind AI systems. However, the "algorithmic black box" – the opaqueness and uninterpretability of AI systems – has raised serious concerns about AI accountability and trust (Christin 2020; Reviglio and Agosti 2020). Although interpretability requirements in AI regulation have grown in importance (Ghosh and Kandasamy 2020; Vyas 2023), there are still a number of obstacles that must be overcome for effective implementation. In this context, it is necessary for regulators to improve algorithm transparency and foster user understanding through measures such as regulating the interpretability of AI and providing for the disclosure of information related to algorithms, so as to strengthen the respect for subjectivity and informed consent while mitigating AI technological power. Algorithms cannot work without data, but they can also produce data (Zaki and Meira 2014). The fairness and reliability of algorithmic operations are significantly impacted by the quality of the data. Inadequate or biased data inputs can engender algorithmic discrimination and compromise their reliability. Governing data entails meticulous regulation across various fronts, encompassing the compliance, privacy, and security aspects of data collection and storage processes, as well as addressing issues of data leakage and misuse during data processing and analysis, and risk control in the application of data to AI systems. Moreover, the emergence of generative AI models has spotlighted compliance challenges concerning synthetic data. Synthetic data, derived from AI-generated sources and utilized in training other AI models (Fonseca and Bacao

2023), is poised to become a pivotal asset in future AI development. Consequently, ensuring robust quality control mechanisms for such data has emerged as a pressing concern within the realm of AI regulation.

The second is to balance three sets of dialectical relations. Primarily, it involves striking a balance between security and developmental imperatives. In the domain of generative AI, this entails the concurrent safeguarding of data integrity, algorithmic robustness (Xu and Mannor 2012), and national security interests to foster continued development. Conversely, it necessitates the acquisition of the core algorithms of generative AI and high-quality data resources to drive the proliferation of market-oriented AI applications. The second aspect involves balancing the relationship between fostering technological innovation and ensuring effective technological governance. It underscores the imperative of integrating governance mechanisms into innovation processes while simultaneously fostering innovation within governance frameworks (Cheng, Qiu, and Yang 2023), which will guarantee that technology advancement adheres to the rule of law. To achieve this, policies should be strategically implemented to steer economic and societal advancement, actively encouraging enterprises to engage in technological innovation by reducing taxes, streamlining bureaucracy, and other similar measures. Furthermore, enterprises ought to be guided to propel broader economic and social advancement (Si and Liu 2022), with legislative measures affirming their legal rights and interests. Simultaneously, a steadfast commitment to legal governance principles should be upheld, which involves promptly addressing and regulating any potential violations or illegal activities by enterprises. The third facet pertains to striking a balance between the compliance duties imposed on enterprises and their capacity to bear such obligations. The effective governance of generative AI requires enterprises engaged in model training and providing generative services to undertake corresponding compliance obligations. However, such obligations must be proportionate and should not exceed the capacity of the AI enterprises.

The third is to make human-centered ethical considerations a fundamental principle of generative AI regulation and to embed them in the technical design of AI systems. AI and human-centered AI represent contrasting philosophies, drawing from Aristotelian rationalism and Leonardo da Vinci's empiricism, respectively (Shneiderman 2021). The former places faith in logical thinking and the strength of formal methods, and pursues AI algorithms driven by efficiency. While beneficial for algorithmic advancements, this approach may restrict the exploration of alternative options and maintain a binary stance. By contrast, empiricists acknowledge the complexity and diversity of the AI social landscape, question simple dichotomies and hierarchies, and cite causality as an important consideration in the refinement of rules. Within this mindset, human-centered AI design

attaches importance to human emotions and experiences, underscores the individual identity reconstructed by AI, and considers human welfare as the ultimate value proposition, so as to mitigate the surveillance and domination of people by AI systems as a form of power structure.

5 Conclusion: From Sight to Foresight

To sum up, this study seeks to track the evolving trends and inherent challenges surrounding the regulation of generative AI and propose corresponding solutions. To this end, we adopt a semiotic perspective to unpack the nature of generative AI as a "floating signifier", and underscore the imperative for regulatory measures to mitigate the social and legal risks it poses. Furthermore, employing a textual comparative approach, we conduct a corpus-level examination of keywords and concordance analysis across two significant global AI regulatory documents: the EUAI Act and the US Blueprint. The findings reveal both encounters and contradictions in AI regulation between these two jurisdictions. Drawing insights from the perspective of panopticism, we delve into the dimensions of visibility and invisibility of AI-related power, and highlight the importance of regulating the power of the unseen. In response to the multifaceted challenges faced with AI regulation across these dimensions, we propose a comprehensive, dynamic, and synthetic framework regulatory framework for generative AI.

Generative AI, to a considerable extent, has significantly reshaped the human subject by placing users under its disciplinary and authoritative power mechanisms, both consciously and unconsciously. It becomes evident that the intricate technicality of generative AI models transcends the mere field of computer science, but calls for analysis through interdisciplinary lenses. The capability of these models to emulate subjectivity and exert profound social impacts implies the relevance of amalgamating social semiotics with the perspective of panopticism as a part of discourse power theory. Such integration holds significant value for deconstructing and regulating generative AI effectively.

References

AbuMusab, Syed. 2023. "Generative AI and Human Labor: Who Is Replaceable?" *AI & Society*: 1–3. https://doi.org/10.1007/s00146-023-01773-3.

Aho, Brett, and Roberta Duffield. 2020. "Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China." *Economy and Society* 49 (2): 187–212.

Aksela, Matti, Samuel Marchal, Andrew Patel, Lina Rosenstedt, and WithSecure. 2022. *The Security Threat of AI-Enabled Cyberattacks*. Finland: Traficom publications.

Amariles, David Restrepo, and Pablo Marcello Baquero. 2023. "Promises and Limits of Law for a Human-Centric Artificial Intelligence." *Computer Law & Security Review* 48: 105795.

Bakiner, Onur. 2023. "The Promises and Challenges of Addressing Artificial Intelligence with Human Rights." *Big Data & Society* 10 (2): 1–13.

Beer, David. 2009. "Power Through the Algorithm? Participatory Web Cultures and the Technological Unconscious." *New Media & Society* 11 (6): 985–1002.

Bennett, Colin J. 2018. "The European General Data Protection Regulation: An Instrument for the Globalization of Privacy Standards?" *Information Polity* 23 (2): 239–46.

Bozdag, Engin. 2013. "Bias in Algorithmic Filtering and Personalization." *Ethics and Information Technology* 15: 209–27.

Brandtzaeg, Petter Bae, Marita Skjuve, and Asbjørn Følstad. 2022. "My AI Friend: How Users of a Social Chatbot Understand Their Human–AI Friendship." *Human Communication Research* 48 (3): 404–29.

Brezina, Vaclav, Tony McEnery, and Stephen Wattam. 2015. "Collocations in Context: A New Perspective on Collocation Networks." *International Journal of Corpus Linguistics* 20 (2): 139–73.

Buiten, Miriam C. 2019. "Towards Intelligent Regulation of Artificial Intelligence." *European Journal of Risk Regulation* 10 (1): 41–59.

Chamberlain, Johanna. 2023. "The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective." *European Journal of Risk Regulation* 14 (1): 1–13.

Cheng, Le, and Xiuli Liu. 2023. "From Principles to Practices: The Intertextual Interaction Between AI Ethical and Legal Discourses." *International Journal of Legal Discourse* 8 (1): 31–52.

Cheng, Le, and David Machin. 2023. "The Law and Critical Discourse Studies." *Critical Discourse Studies* 20 (3): 243–55.

Cheng, Le, and King Kui Sin. 2008. "A Court Judgment as Dialogue." In *Dialogue and Rhetoric*, edited by Edda Weigand, 267–81. Amsterdam: John Benjamins.

Cheng, Le, Winnie Cheng, and King-Kui Sin. 2014. "Revisiting Legal Terms: A Semiotic Perspective." *Semiotica* 2014 (202): 167–82.

Cheng, Le, Jiaxuan Qiu, and Yi Yang. 2023. "Constructing Cybersecurity Discourse via Deconstructing Legislation." *International Journal of Legal Discourse* 8 (2): 273–97.

Christin, Angèle. 2020. "The Ethnographer and the Algorithm: Beyond the Black Box." *Theory and Society* 49 (5-6): 897–918.

Claude, Levi-Strauss. 1987. *Introduction to the Work of Marcel Mauss*. London: Routledge.

Dennett, Daniel C. 1990. "Cognitive Wheels: The Frame Problem of AI." In *The Philosophy of Artificial Intelligence*, Vol. 147, 1–16.

Desouza, Kevin C., Gregory S. Dawson, and Daniel Chenok. 2020. "Designing, Developing, and Deploying Artificial Intelligence Systems: Lessons from and for the Public Sector." *Business Horizons* 63 (2): 205–13.

Díaz-Rodríguez, Natalia, Javier Del Ser, Mark Coeckelbergh, Marcos López de Prado, Enrique Herrera-Viedma, and Francisco Herrera. 2023. "Connecting the Dots in Trustworthy Artificial Intelligence:

From AI Principles, Ethics, and Key Requirements to Responsible AI Systems and Regulation." *Information Fusion* 99: 101896.

Dwivedi, Yogesh K., Nir Kshetri, Laurie Hughes, Emma Louise Slade, Jeyaraj Anand, Arpan Kumar Kar, Abdullah M. Baabdullah, et al. 2023. "'So what if ChatGPT Wrote it?' Multidisciplinary Perspectives on Opportunities, Challenges and Implications of Generative Conversational AI for Research, Practice and Policy." *International Journal of Information Management* 71: 102642.

Fludernik, Monika. 2017. "Panopticisms: From Fantasy to Metaphor to Reality." *Textual Practice* 31 (1): 1–26.

Fonseca, Joao, and Fernando Bacao. 2023. "Tabular and Latent Space Synthetic Data Generation: A Literature Review." *Journal of Big Data* 10 (1): 115.

Forbus, Kenneth D., and Thomas R. Hinrichs. 2006. "Companion Cognitive Systems: A Step Toward Human-Level AI." *AI Magazine* 27 (2): 83.

Foucault, Michel. 1977. 1926–1984. *Discipline and Punish: The Birth of the Prison*. New York: Pantheon Books.

Galič, Maša, Tjerk Timan, and Bert-Jaap Koops. 2017. "Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation." *Philosophy & Technology* 30: 9–37.

Ghosh, Adarsh, and Devasenathipathy Kandasamy. 2020. "Interpretable Artificial Intelligence: Why and When." *American Journal of Roentgenology* 214 (5): 1137–8.

Hacker, Philipp. 2023. "The European AI Liability Directives–Critique of a Half-Hearted Approach and Lessons for the Future." *Computer Law & Security Review* 51: 105871.

Hull, Alfred D., Jim Kyung-Soo Liew, Kristian T. Palaoro, Mark Grzegorzewski, Michael Klipstein, Pablo Breuer, and Michael Spencer. 2022. "Why the United States Must Win the Artificial Intelligence (AI) Race." *The Cyber Defense Review* 7 (4): 143–58.

Jo, A. 2023. "The Promise and Peril of Generative AI." *Nature* 614 (1): 214–6.

Kitchin, Rob, and Tracey P. Lauriault. 2014. "Towards Critical Data Studies: Charting and Unpacking Data Assemblages and Their Work." In *Geoweb and Big Data*, edited by J. Eckert, A. Shears, and J. Thatcher. Nebraska: University of Nebraska Press.

Linardatos, Pantelis, Vasilis Papastefanopoulos, and Sotiris Kotsiantis. 2020. "Explainable AI: A Review of Machine Learning Interpretability Methods." *Entropy* 23 (1): 1–18.

Lupton, Deborah. 2013. *Risk*. New York: Routledge.

Magee, Liam, Vanicka Arora, and Luke Munn. 2023. "Structured like a Language Model: Analysing AI as an Automated Subject." *Big Data & Society* 10 (2): 1–15.

Mantelero, Alessandro. 2018. "AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment." *Computer Law & Security Review* 34 (4): 754–72.

McMillan, John. 2023. "Generative AI and Ethical Analysis." *The American Journal of Bioethics* 23 (10): 42–4.

Mikalef, Patrick, Kristina Lemmer, Cindy Schaefer, Maija Ylinen, Siw Olsen Fjørtoft, Hans Yngvar Torvatn, Manjul Gupta, et al. 2022. "Enabling AI Capabilities in Government Agencies: A Study of Determinants for European Municipalities." *Government Information Quarterly* 39 (4): 1–15.

Morley, Jessica, Anat Elhalal, Francesca Garcia, Libby Kinsey, Jakob Mökander, and Lucinao Floridi. 2021. "Ethics as a Service: A Pragmatic Operationalisation of AI Ethics." *Minds and Machines* 31 (2): 239–56.

Onitiu, Daria. 2021. "Deconstructing the Right to Privacy Considering the Impact of Fashion Recommender Systems on an Individual's Autonomy and Identity." PhD diss., University of Northumbria at Newcastle. https://www.proquest.com/openview/6c2304d8fa4bd51f509897757fc78678/1?pq-origsite=gscholar&cbl=2026366&diss=y (accessed December 15, 2023).

OpenAI. 2024. "GPT-4 Technical Report." https://arxiv.org/abs/2303.08774 (accessed March 7, 2024).

Radford, Alec, Karthik Narasimhan, Tim Salimans, and Ilya Sutskever. 2018. "Improving Language Understanding by Generative Pre-training." https://www.mikecaptain.com/resources/pdf/GPT-1.pdf (accessed December 15, 2023).

Radu, Roxana. 2021. "Steering the Governance of Artificial Intelligence: National Strategies in Perspective." *Policy and Society* 40 (2): 178–93.

Raisch, Sebastian, and Sebastian Krakowski. 2021. "Artificial Intelligence and Management: The Automation–Augmentation Paradox." *Academy of Management Review* 46 (1): 192–210.

Ran, Duan, Yingli Wang, and Haoxin Qin. 2021. "Artificial Intelligence Speech Recognition Model for Correcting Spoken English Teaching." *Journal of Intelligent and Fuzzy Systems* 40 (2): 3513–24.

Raub, McKenzie. 2018. "Bots, Bias and Big Data: Artificial Intelligence, Algorithmic Bias and Disparate Impact Liability in Hiring Practices." *Arkansas Law Review* 71 (2): 529–70.

Ray, Partha Pratim. 2023. "ChatGPT: A Comprehensive Review on Background, Applications, Key Challenges, Bias, Ethics, Limitations and Future Scope." *Internet of Things and Cyber-Physical Systems* 3: 121–54.

Reviglio, Urbano, and Claudio Agosti. 2020. "Thinking Outside the Black-Box: The Case for "Algorithmic Sovereignty" in Social Media." *Social Media + Society* 6 (2): 1–12.

de Saussure, Ferdinand. 2011. *Course in General Linguistics*. Columbia: Columbia University Press.

Salomon, Gavriel. 1988. "AI in Reverse: Computer Tools That Turn Cognitive." *Journal of Educational Computing Research* 4 (2): 123–39.

Saran, Samir, Nikhila Natarajan, and Madhulika Srikumar. 2018. *In Pursuit of Autonomy: AI and National Strategies*. Delhi: Observer Research Foundation.

Si, Chunlei, and Yuxin Liu. 2022. "Exploring the Discourse of Enterprise Cyber Governance in the Covid-19 Era: A Sociosemiotic Perspective." *International Journal of Legal Discourse* 7 (1): 53–82.

Simon, Judith, Pak Hang Wong, and Gernot Rieder. 2020. "Algorithmic Bias and the Value Sensitive Design Approach." *Internet Policy Review* 9 (4): 1–16.

Shneiderman, Ben. 2021. "Human-Centered AI." *Issues in Science & Technology* 37 (2): 56–61.

Song, Lijue, and Changshan Ma. 2022. "Identifying the Fourth Generation of Human Rights in Digital Era." *International Journal of Legal Discourse* 7 (1): 83–111.

Steadman, Philip. 2012. "Samuel Bentham's Panopticon." *Journal of Bentham Studies* 14: 1–30.

Tacheva, Jasmina, and Srividya Ramasubramanian. 2023. "AI Empire: Unraveling the Interlocking Systems of Oppression in Generative AI's Global Order." *Big Data & Society* 10 (2): 1–13.

Taeihagh, Araz. 2021. "Governance of Artificial Intelligence." *Policy and society* 40 (2): 137–57.

Veale, Michael, and Frederik Zuiderveen Borgesius. 2021. "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 (4): 97–112.

Vyas, Bhuman. 2023. "Explainable AI: Assessing Methods to Make AI Systems More Transparent and Interpretable." *International Journal of New Media Studies: International Peer Reviewed Scholarly Indexed Journal* 10 (1): 236–42.

Wachter, Sandra, Brent Mittelstadt, and Chris Russell. 2021. "Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI." *Computer Law & Security Review* 41: 1–72.

Wagner, Anne, Aleksandra Matulewska, and Le Cheng. 2020. "Law as a Culturally Constituted Sign-System–A Space for Interpretation." *International Journal of Legal Discourse* 5 (2): 239–67.

Wiley, Victor, and Thomas Lucas. 2018. "Computer Vision and Image Processing: A Paper Review." *International Journal of Artificial Intelligence Research* 2 (1): 29–36.

Wilks, Yorick. 1972. *An Artificial Intelligence Approach to Machine Translation*. Stanford: Stanford University.

Whang, Steven Euijong, Yuji Roh, Hwanjun Song, and Jae-Gil Lee. 2023. "Data Collection and Quality Challenges in Deep Learning: A Data-Centric AI Perspective." *The VLDB Journal* 32 (4): 791–813.

Xu, Huan, and Shie Mannor. 2012. "Robustness and Generalization." *Machine Learning* 86: 391–423.

Zaki, Mohammed J., and Wagner Meira. 2014. *Data Mining and Analysis: Fundamental Concepts and Algorithms*. Cambridge: Cambridge University Press.

Zuboff, Shoshana. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30 (1): 75–89.

Zuboff, Shoshana. 2023. "The Age of Surveillance Capitalism." In *Social Theory Re-wired*, edited by Wesley Longhofer, and Daniel Winchester, 203–13. New York: Routledge.

Bionotes

Le Cheng
Guanghua Law School and School of Cyber Science and Technology, Zhejiang University, Hangzhou, China
chengle163@hotmail.com
https://orcid.org/0000-0002-4423-8585

Le Cheng is Chair Professor of Law, and Professor of Cyber Studies at Zhejiang University. He serves as the Executive Vice Dean of Zhejiang University's Academy of International Strategy and Law, Acting Head of International Institute of Cyberspace Governance, Editor-in-Chief of *International Journal of Legal Discourse*, Editor-in-Chief of *International Journal of Digital Law and Governance*, Co-Editor of *Comparative Legilinguistics (International Journal for Legal Communication)*, Associate Editor of *Humanities and Social Sciences Communications,* former Co-Editor of *Social Semiotics*, and editorial member of *Semiotica*, *Pragmatics & Society*, and *International Journal for the Semiotics of Law*. As a highly-cited scholar, he has published widely in the areas of international law, digital law and governance, cyber law, semiotics, discourse studies, terminology, and legal discourse.

Xiuli Liu
School of International Studies, Zhejiang University, Hangzhou, China
liuxiuli@zju.edu.cn
https://orcid.org/0000-0001-8534-6753

Xiuli Liu is Research Fellow at Zhejiang University. Her research interests lie in digital law, data protection law, legal discourse, corpus linguistics, and critical discourse studies. Her articles have been published in the *International Journal of Speech, Language and the Law*, *International Journal of Legal Discourse,* and the *International Journal for the Semiotics of Law.*