

## Research Article

Le Cheng\* and Xiuli Liu

# From principles to practices: the intertextual interaction between AI ethical and legal discourses

<https://doi.org/10.1515/ijld-2023-2001>

Received December 28, 2022; accepted March 31, 2023

**Abstract:** The ascendancy and ubiquity of generative AI technology, exemplified by ChatGPT, has resulted in a transformative shift in the conventional human–AI interaction paradigm, leading to substantial alterations in societal modes of production. Drawing on CDA approach, this study conducts a thematic intertextuality analysis of 29 AI ethical documents, and delves into the restructuring of the human–AI relations catalysed by ChatGPT, as well as the complex ethical and legal challenges it presents. The findings indicate that the thematic intertextuality between AI ethical discourse and legal discourse promotes the connection and convergence of narrative-ideological structures, which in turn primarily creates new meaningful texts and ethical frameworks that promote a holistic approach to a good AI society. This research also identifies the importance of integrating law-making efforts with substantive ethical analysis and appropriate discursive strategies to promote the responsible and ethical development of generative AI that benefits society as a whole.

**Keywords:** AI ethics; CDA and law; ChatGPT; generative AI; human–AI interaction; legal discourse; legal practice

## 1 Introduction

Artificial Intelligence (herein after AI) has ushered in major historical shifts in the realm of technological advancements and industrial applications, particularly in the field of generative AI (Jabotinsky and Sarel 2022). On November 30, 2022, OpenAI launched ChatGPT, an intelligent chatbot based on large language models that is

---

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

capable of fulfilling a wide variety of text-based requests, including interactive question-and-answer sessions, as well as complex tasks such as text creation and programming (Gao et al. 2023). As generative AI, exemplified by ChatGPT, intersects with traditional social paradigms and creates new environments for humans to interact with AI, the impact of AI on society and how to deal with it, ranging from the labour market (Acemoglu and Restrepo 2020), healthcare (Korngiebel and Mooney 2021; Panch et al. 2019), financial markets (McBride et al. 2022), academic writing (Stokel-Walker and Van Noorden 2023; Thorp 2023), and the protection of human rights (Zohny et al. 2023), has been widely discussed by academia and practitioners. Current research on the impact of AI on all facets of human social life is focused either on the formulation of ethical principles or on the investigation of laws and regulations. For instance, some scholars have accused ethical precepts of being toothless (Morley et al. 2023; Rességuier and Rodrigues 2020), while others argue that legal rules being too stringent to stifle technological advancement (Gordon et al. 2007; Ochigame 2019). These works, however, do not go deep into the theoretical elaboration in terms of the relationship between the law and ethical concerns. To fill in this gap, the present study applies critical discourse analysis (CDA), which has a multi-disciplinary character (Locke 2004), as an approach to analyze the interaction between ethical and legal discourse in the field of artificial intelligence through intertextuality, and to seek how the normative development of artificial intelligence entails shifting from general ethical principles to specific legal practices, from the natural law to the law *de facto*, and the underlying socio-ideological motivations.

In both ethical discourse and legal discourse of AI, there exists as the element of intelligent social practice, presenting a dialectical and mutual internalisation relationship with other elements such as the material world and social relations (Fairclough 2003: 207). Hence, the relationship between AI discourse and practice needs to be re-examined as AI reconfigures social life, namely how the ethical and legal discourse of AI is constrained by new social relations and how it positively constructs the AI society (Cheng and Liu 2022). In addition, demystification is also pursued by CDA (Wodak and Meyer 2009: 3). The opacity inherent in the algorithmic architecture of ChatGPT imbues it with an aura of mystique, which is one of the reasons it has sparked community debate. The CDA works to demystify the technological power of AI and to ensure the subjectivity and equality of people in society by investigating a range of semiotic resources. To be more precise, demystification involves revealing the interconnectedness of things in a specific context and rendering their interrelationships visible (Fairclough 1995: 36). Through the lens of “intertextuality”, the interconnectedness and interdependence of social life can be investigated in depth. Intertextuality has received increasing attention in the area of discourse analysis, particularly in critical linguistics (Fairclough 1992, 1995, 2003; Lemke 1985, 2002). As a fundamental feature of discourse, intertextuality analysis constitutes an

important aspect of discourse analysis. As Kristeva, the originator of the concept of intertextuality, puts it, any discourse is a change of substitution of other discourses, an intertext (Kristeva 1980: 36). Intertextuality derives from the combination of Saussure's structuralism and Bakhtin's dialogism (Haberer 2007: 57; Irwin 2004: 227). Dialogism, according to Bakhtin (1986: 91), is not only dialogue in the narrow sense of linguistic form but also the broader sense of socio-cultural dimensions. As such, the analysis of intertextuality places less emphasis on the number of intertextual manifestations within the discourse but more on exposing the ideological and power dynamics concealed inside the intertextual structure.

Based on the critical discourse analysis of Fairclough (2003), the current study aims to explore the restructurings of the dialectical relationship between AI ethical discourse and AI legal discourse that accompanied the breakthrough storm events brought about by the emergence of ChatGPT to the new capitalism (Cheng and Machin 2022). The detailed analytical research is bifurcated into two parts. The first is the social research that centres on the legal personality of ChatGPT and the challenges it poses to ethics and law. The second is the text analysis that focuses on the thematic intertextuality of ethical and legal texts on AI. The study employed a collection of twenty-nine AI ethical documents sourced from both the European Union (EU) and the United States (US). The rationale for the choice of materials from these two regions was based on the fact that the United States is the birthplace of the ChatGPT, while the European Union was the pioneer in enacting an AI Act. Subsequent to the introduction part, the study will begin by defining the position of ChatGPT within the intricate interplay between AI and human beings, followed by an exploration of the challenges that ChatGPT presents to our society, then move to the intertextual analysis of ethical and legal texts, and finally seek to facilitate the transformation of AI regulation from normative law to positive law (Kelsen 1967), as well as from ethical principles to legal practice.

## 2 Legal personality debate on ChatGPT

The latest advancement in generative AI has enabled the creation of long text outputs that closely resemble human language, thereby posing a challenge in discerning whether a given passage is of human or AI origin. The blurring of the boundaries between humans and AI (Warwick 2013), and has even called into question the fundamental distinction between the two. The underlying reason is rooted in the manner in which humans situate generative AI. The autonomous evolution of AI towards human consciousness has been a subject of speculation and discussion in science fiction for the past century. Asimov, a renowned science fiction author, proposed the Laws of Robotics as a solution to the issue of human and AI interaction

(Clarke 1993, 1994). His “three law of robotics” have since served as the principles that inform the contemporary ethical framework of AI (Murphy and Woods 2009). The discussion surrounding the attribution of legal personality to artificial intelligence is gaining momentum in the field of jurisprudence, alongside the advancement of related fields such as cyber law, and AI law. As per the predominant academic perspective (Čerka et al. 2015, 2017; Chesterman 2020), AI does not currently meet the criteria for legal personhood (Solaiman 2017), and therefore it remains suitable to govern it as an object of legal regulation.

In the case of ChatGPT, for instance, there is currently a heated debate about whether ChatGPT can be credited as an author. Within weeks of ChatGPT’s release, a number of scholars rapidly published articles, in which they recognized ChatGPT as a co-author (see King and ChatGPT 2023). This action could potentially be interpreted as a superficial or attention-grabbing tactic, or as an recognition of the impact of AI. Overall, the emergence of this phenomenon highlights the prevailing confusion surrounding the authorship of generative AI, prompting swift action by traditional publishing entities to address the matter and assert the inadmissibility of such conduct. As clarified by Science magazine, it is evident that AI cannot be an author or a co-author. Moreover, the publication of any text, graphics, or images generated by generative AI tools like ChatGPT has been explicitly prohibited (Thorp 2023). According to Nature (Van Dis et al. 2023), ChatGPT has been observed to diminish the quality and transparency of research, and significantly alters the independence of human research subjects. The discussion sparked by ChatGPT within the academic sphere highlights the issue of the ambiguous status of generative AI. The Law community is currently contending with the challenge of attributing generative content and creations produced by AI, leading to contemplations on the plausibility of endowing legal personhood to AI.

Debates have arisen concerning the legal personality of AI, with some advocating for the recognition of AI as a legal person or a quasi-one (Ponkin and Redkina 2018). This perspective draws parallels to the legal recognition of corporations, which bestows upon them the ability to enter into contracts and litigate in court. This view is grounded in reality, as evidenced by the occurrence of a traffic accident involving a Tesla self-driving car, which raised discussion about the liability of autonomous vehicles (Brodsky 2016; Stilgoe 2018). Additionally, the unique nature of AI-generated content implies that conferring legal personality upon AI appears to be a feasible approach for resolving the issue of interest attribution (Pearlman 2017). In order to comprehensively define the nature of AI, the proposal of AI legal personality as a viable alternative is essential. However, given contemporary technological advancements, it is impractical to confer personhood on AI in the legal sense. Firstly, from a jurisprudential perspective, it can be argued that the purpose and value of law are inherently subordinate to and intended to benefit human beings, commonly

referred to as “reasonable person” in civil law (Miller and Perry 2012). Hence, it can be inferred that the legal system assumes a rational actor as the normative and pre-established subject from the outset. The inherent nature of AI precludes it from possessing rationality and thus, it cannot be considered a rational agent. Despite the fact that a generative AI may possess the capacity to independently make decisions and engage in reasoning, it does not necessarily imply that it is capable of being rational. The aforementioned rationality falls under the classification of technical rationality. However, it is necessary to note that AI does not inherently possess technical rationality; rather, it functions as a channel for the projection and amplification of human technical rationality within the AI framework. Secondly, from the perspective of legal personality, the basic requirements for legal personality in the formation of a legal relationship are the ability to hold rights and the ability to undertake actions (Flynn and Arstein-Kerslake 2014). Generative AI, on the one hand, lacks the legal capacity to engage in legal relationships, possess legal rights or undertake legal obligations, thus lacking “personhood” in the legal sense. On the other hand, it lacks independent awareness of the nature, meaning and consequences of its actions and the capacity to control and take responsibility for its actions. The decisions made by AI are produced by human beings “feed” with data (O’Leary 2013), and are the result of data calculations and algorithmic computations. As such, AI cannot be deemed as possessing independent consciousness, nor can it be qualified to undertake responsibility. Finally, from the practical point of view, it is evident that the existing challenges posed by generative AI cannot be resolved solely by conferring legal personality on it. Product liability regulation may cover legal issues that stem from the deployment of autonomous driving technology, while copyright law can regulate intellectual property disputes that might emerge from generative AI. The advent of novel technologies does not necessarily entail a wholesale upheaval of preexisting legal standards. The relationship between humans and artificial intelligence ultimately boils down to a relationship between humans and objects, and whether it is generative AI or other types of AI, exists as objects regulated by law.

### 3 Social challenges posed by generative AI

Generative AI has brought about substantial advances in technology. However, it has also presented a range of potential risks and challenges to society. Such challenges extend beyond the realm of AI governance and may impact specific legal regulations (Wu and Cheng 2022). The identification and analysis of these issues within the context of an AI-based society are necessary to figure out the appropriate solutions that will contribute to the realisation of a “good AI society” (Floridi et al. 2018).

### 3.1 AI ethics

Generative AI further challenges the existing moral and ethical principles of AI, posing a series of ethical risks and the potential of alienation which cannot be ignored. The widespread use of generative AI, as exemplified by ChatGPT, has resulted in an increasing reliance on algorithms as a mechanism for re-structuring social connections (Curchod et al. 2020), as well as a growing degree of algorithmic influence on human interaction, behaviour, and decision-making. The commercialization of generative AI has the potential to produce an incremental effect on the socio-economic structure. The deployment and development of these algorithms by companies in different regions may exacerbate ethical dilemmas, such as bias and inequity. Prior work by Raub (2018) has demonstrated that algorithms have a tendency to amplify social biases and discrimination within the realm of recruitment. Typically, ethical and moral mechanisms to mitigate the risks associated with the widespread deployment and application of AI in society consist of four types: principles, codes, recommendations, and guidelines. The present challenge concerning the ethics of AI resides in their ineffective presentation, which stems from their non-binding nature and susceptibility to misinterpretation or unrealistic expectations (Rességuier and Rodrigues 2020). Such shortcomings render them seemingly futile and severely curtail their potential for social governance.

As algorithms increasingly permeate people's daily social lives, generative AI such as ChatGPT deepens the opacity and incomprehensibility of algorithms, complicating the already unresolved concerns surrounding AI fairness and discrimination, and further exacerbating the political leanings of the speech generated. The current concentration is on how to transform the general principles of AI ethics into concrete, actionable practice. With this comes two models that are distinct but interrelated. One is soft law governance, a system of self-government built on non-legislative and policy-based instruments. Soft law governance manifests itself in the form of AI ethical guidelines produced by enterprises, stakeholder organisations, standard-setting agencies, and others, and these self-regulatory documents play an important function in setting the baseline for AI governance (Wallach and Marchant 2018). The other is mandatory legal norms, usually enacted by the legislature, to regulate rights and obligations and prohibitions on behaviour in order to set standards that align with the attributes of AI systems (Jobin et al. 2019). Such legal norms encompass a range of specialised AI laws as well as traditional sectoral norms, such as tort law, contract law, labour law, and intellectual property law, which are relevant to the regulation of algorithms. In general, the current legal regulation of AI will continue to evolve in three main directions: the revision and

interpretation of existing laws, the enactment of new general AI legislation, and the formulation of specific legislation in areas such as generative AI.

### 3.2 Intellectual property protection

Typically, copyrighted materials refer to “original work” that has been produced by a human being and is presented in a physical or digital format, such as a literary work, an artistic painting, or a piece of software. Text, images, and other forms of content created by generative AI are indistinguishable from those produced by humans, resulting in a number of lawsuits and disputes. The points of contention involved are specified in three areas: unauthorised use, copyright ownership of the generated content, and protection of the intellectual property rights of third parties.

At the outset, generative AI models must be fed with data before they can output content. If the data is not authorised by the data supplier at the time of input, intellectual property infringement issues may arise. Getty Images initiated legal action against Stability AI in January 2023, alleging that the latter had utilised millions of images without obtaining proper authorization for training its artificial intelligence technology.<sup>1</sup> The capability of ChatGPT to imitate style has raised concerns among writers and artists regarding the extensive training of generative AI to reproduce their distinctive style. Another issue raised by generative AI is how generated content is defined within the realm of copyright law. Specifically, it questions whether such content is entitled to the same safeguarding as that of its human originators in terms of intellectual property. Wang (2017) posits that the primary consideration is whether the same content originating from human creation qualifies as a work, and if it satisfies the tenets of copyright law, then the matter of authorship and copyright attribution will be further considered. Despite the fact that AI-generated content may not be protected by copyright law, it does not mean that it is unprotected from usage since there are still concerns about the intellectual property rights of third parties. Responses from ChatGPT may include copyright-protected content, such as text that has been copied exactly from other sources or images with registered trademarks. Copyrights, trademarks, and patents held by rights holders other than the person or entity using ChatGPT-generated content are examples of third-party intellectual property rights. In situations where there is a risk of infringing the intellectual property rights of others, it is necessary to obtain to

---

<sup>1</sup> See Jennifer Korn. Getty Images suing the makers of popular AI art tool for allegedly stealing photos. <https://edition.cnn.com/2023/01/17/tech/getty-images-stability-ai-lawsuit/index.html> (accessed 18 January 2023).

obtain permission or authorisation from the right holder in order to use the content in a lawful manner.

In a nutshell, the emergence of generative AI poses major worries regarding intellectual property that require resolution to guarantee that the use of these technologies respects the rights and privileges of human creators. The use of generative AI in the creative process, and the extent to which it is to be interpreted and explained, requires collaboration between legislators, technologists, corporations and government authorities to come up with an effective legal framework (Bingham 2009).

### 3.3 Privacy and personal data protection

Large language models (LLM) used by ChatGPT necessitate an enormous quantity of data. The more data is trained on, the better the model performs in generating textual content. However, users may inadvertently enter sensitive personal information into the databases when giving instructions to ChatGPT. For instance, a lawyer may use ChatGPT for a draft divorce agreement review, which then becomes part of the ChatGPT database. It implies that this type of sensitive information will be used for further training and may appear in responses to other users. Due to privacy concerns, the Italian data protection authority Garante issued an urgent decision on 31 March 2023 requesting that OpenAI cease using the personal information of Italian users contained in its training data. In response, OpenAI terminated ChatGPT access for Italian users.<sup>2</sup>

In the context of the GDPR, there are main reasons for Garante to ban ChatGPT. The first is that even though the ChatGPT service is only available to users who are thirteen or older, according to OpenAI's privacy policy, there is no procedure in place to confirm users' true ages. However, the lack of suitable verification procedures could expose minors to age-inappropriate content. Secondly, there are instances where ChatGPT's processing of information about data subjects is inaccurate or even incorrect. Thirdly, users are not informed that their data is being collected. Fourthly, and most importantly, OpenAI does not state any legal basis for the collection of personal data and the processing of that data for the purpose of training algorithms that serve the operation of ChatGPT. Article 6 of the GDPR establishes the lawfulness of processing personal data (Tikkinen-Piri et al. 2018), which includes the informed consent, the performance of a contract, the compliance with a legal obligation, the protection of vital interests of individuals, the protection of the public interest, and the pursuit of legitimate interests. The collection and processing of personal data by

---

<sup>2</sup> See ChatGPT banned in Italy over privacy concerns. <https://www.bbc.com/news/technology-65139406> (accessed 31 March 2023).



OpenAI to train ChatGPT lack a legitimate basis under the GDPR. Even though OpenAI argues that it collects and processes personal data in the public interest, this justification is insufficient as a for-profit enterprise. In this context, the potential threats to privacy and personal data when engaging with ChatGPT cannot be disregarded by users. And for companies involved in generative AI projects, the lawful and regulatory collection and processing of data is a crucial matter that requires attention.

### 3.4 Monopoly and competition law

The technological innovation driven by competition is reflected in the significant improvement in the accuracy and relevance of search results due to ChatGPT's advances in natural language processing. ChatGPT can be used as a substitute for and even outperform standard search engines for users or consumers. From an antitrust standpoint, ChatGPT has the potential to generate significant market disruption in the future, thereby exerting competitive influence on the broader internet search engine industry. Moreover, in the event that confidential commercial information is fed into ChatGPT and subsequently disclosed to a third party, it may give rise to instances of unfair competition. The innovative characteristics of generative AI lead to significant entry barriers, resulting in a high concentration of pertinent technologies and markets among the current large tech giants, potentially inhibiting the growth of small and medium-sized tech innovators.

The emergence of generative AI triggered market and technology monopolies in four primary domains. First, monopoly at the computing capacity level. AI relies heavily on computational performance (Ghosh et al. 2018), so the development of generative AI necessitates high computational performance. It is claimed that the training of GPT-3 demands a computational power that far exceeds the previous capabilities of Microsoft systems.<sup>3</sup> The infrastructure and computing power demands pose a financial burden for small enterprises, thereby setting a high barrier to market entry. Second, monopoly at the data level. Generative AI depends on training and real-time access to large amounts of data, and those technology companies that have already gathered and amassed massive volumes of data will be in a dominant leadership position in the field of generative AI services. Current core digital service platforms, in particular, possess more valuable data than any AI startup. Third, the monopoly at the algorithmic level. The significance and indispensable function of algorithmic models within an AI framework cannot be underestimated, despite their being just one constituent part of the system.

---

3 See Microsoft + OpenAI: Inside Tech's Hottest Romance. <https://www.theinformation.com/articles/microsoft-openai-inside-techs-hottest-romance> (accessed 11 January 2023).

Individuals who possess the ability to independently create algorithmic models are frequently recruited by prominent technology companies. Fourth, the monopoly at the AI research level. AI products come in a diverse array of forms, and generative AI models can be integrated into the majority of them. Considering the integrity of physical level (typically critical information infrastructure), data level, information level and social level (Cheng et al. 2021), the extensive information infrastructure, users, data and other advantages possessed by large tech giants can facilitate their extensive expansion of diverse AI products and the assimilation of generative AI models into their extensive range of products. This self-reinforcing circular growth model results in a “winner-takes-all” situation (Naudé and Dimitri 2020), where large enterprises take an increasingly large share of the AI market and continue to squeeze out the survival of start-up AI companies.

The concentration of significant AI resources is limited to a few commercial technology enterprises, raising concerns about the adequacy of their ethics. How to regulate the market monopolistic behaviour of generative AI is becoming an important issue at the moment. The European Union leads the way in international market regulation, having enacted the Digital Services Act (DSA) and the Digital Markets Act (DMA) in 2022, both of which aim to promote public competition and create fair and open digital markets. However, the absence of the term “AI as a platform” implies that there is a need for additional exploration into the legal concerns regarding competition adjudication within the AI sector.

### 3.5 Cyber crime and data security

The challenges posed by generative AI on cybersecurity governance are primarily manifested in the heightened complexity of content governance. Cyber information content is the primary focus of cyber governance, with a particular emphasis on regulating the organisations that make up the cyber sector as well as the producers and service platforms for cyber information content (Wang et al. 2020). However, the widespread use of generative AI has resulted in a notable decrease in the expenses associated with generating Internet information content. This has, in turn, presented challenges in terms of regulating the production and utilisation of such content, as well as verifying its authenticity. As a result, the governance of Internet information content has become increasingly complex. More importantly, despite the neutrality of technology, generative AI can be motivated or trained to generate content with extreme ideology or a strong political bias.

The domain of data security encounters challenges posed by generative AI, primarily concerning data leakage and cross-border data security. In the process of pre-training and post-user interaction, a large amount of data resources are gathered in ChatGPT. If data leakage occurs, it means that personal data, especially sensitive

personal data, is exposed in an unsafe state, which may cause possible damage to the personal and property rights of the data subject (Lupton 2018). Regarding the matter of cross-border data security, it is stated in Section 9 of the OpenAI Privacy Policy that the use of the service implies acknowledgement of the transfer of one's personal data to devices and servers located in the United States. In addition, the legal foundation for the processing of personal data is addressed distinctly for global users across various geographical locations. When international users input personal data, even sensitive data, into ChatGPT, this may raise security concerns regarding the cross-border storage, circulation, and processing of data.

Generative AI technology has the potential to decrease the expenses associated with AI-driven cybercrime, while simultaneously increasing the severity of such criminal activities. ChatGPT can be trained on a dataset of authentic phishing emails to generate new and more deceptive phishing emails at a fraction of the cost, making it easier for cybercriminals to launch broad-scale cyber attacks (Pei et al. 2022). ChatGPT symbolises a mere starting point for AI-driven cybercrime, with research suggesting that the ongoing advancement of generative AI will change the paradigm of cybersecurity attacks and defences over the next five years (Aksela et al. 2022), and this means that the level of cybersecurity preparedness and measures to deal with cybercrime is in urgent need of further updating.

## 4 Analysis on intertextuality: from ethical and legal perspective

According to Fairclough (2003: 52), 'intertextuality is a matter of recontextualization', then the movement from ethical principles to legal practice is often accompanied by a particular transformation resulting from the shift and recontextualisation of the corresponding textual material within a new context. This section, therefore, addresses two interconnected issues: the relationship between the themes of the ethical AI texts and the rest of the texts; and the relationship between the AI ethical texts and the legal AI texts. The present study identified 29 documents containing ethical principles or guidelines for AI (see the appendix for details), which can be objectified units of discourse (Gal 2006: 178) to provide basic evidence for the quantitative analysis. The selection of data material for this study on AI ethics consisted of two parts: EU and US AI ethics documents retrieved from AI ethics documents summarized in the work edited by Jobin et al. (2019); the supplementary AI ethics documents searched on website dated after their study.

The results of our content and thematic analysis revealed ten overarching ethical values and principles (cf. Table 1). These are, according to the number of

Table 1: Top 10 ethical principles identified in existing AI ethics.

Number	Theme	Frequency	Code number
1	Accountability	19 (0.66)	1U;2U;4U;5U;8U;9U;11U;12U;13U;14U;16U;17U;19U;20U;24E;25E;26E;28E;29E
2	Privacy	15 (0.52)	1U;3U;4U;5U;8U;10U;11U;15U;19U;20U;24E;25E;26E;28E;29E
3	Transparency	15 (0.52)	2U;3U;4U;6U;13U;14U;15U;17U;18U;20U;23E;24E;25E;27E;29E
4	Fairness	14 (0.48)	1U;4U;8U;12U;14U;15U;16U;17U;18U;20U;21U;25E;27E;29E
5	Security	13 (0.45)	1U;4U;6U;15U;16U;17U;18U;23E;24E;26E;27E;28E;29E
6	Safety	13 (0.45)	3U;4U;7U;8U;15U;16U;17U;18U;23E;24E;25E;28E;29E
7	Non-discrimination	12 (0.41)	1U;9U;10U;12U;14U;19U;21U;22U;24E;25E;27E;29E
8	Accessibility	8 (0.28)	1U;2U;6U;10U;11U;15U;19U;29E
9	Explainability	8 (0.28)	2U;6U;9U;11U;17U;18U;21U;29E;
10	Responsibility	7 (0.24)	3U;5U;12U;15U;23E;24E;28E

sources in which they appeared most frequently: Accountability, Privacy, Transparency, Fairness, Security, Safety, Non-discrimination, Accessibility, Explainability, and Responsibility. As indicated in Table 1, no single principle appeared to be a common one that is currently referenced in all documents, reflecting the fact that there is no global consensus in the domain of AI ethics. The principle of accountability, which is the most frequently mentioned topic, seems to garner the most significant amount of attention. Certain principles, such as safety and security, may appear interchangeable in common parlance but assume distinct roles within the ethical framework of artificial intelligence. Further textual and thematic scrutiny will elucidate the semantic connotations and distinctions of these principles in detail, with the aim of fostering consistent comprehension and implementation.

Accountability is the most prevalent principle in the current documents. As a risk mechanism, this principle is primarily concerned with the question of which subjects should be held accountable, on what aspects, and how and to what extent accountability mechanisms should be put in place (Breeze 2021). In general, accountability rests with the institution that primarily designs and uses the algorithm (see 1U, 13U), as well as with the algorithm engineer (see 24E). Aspects of accountability include the current impact of the development, deployment and/or use of AI systems (see 29E), as well as the potential future societal impact (see 24E). Specific forms of accountability include notification, rectification and redress for those affected by automated decision-making by AI systems (see 1U), explanation to third parties and the design of adequate remedial measures to address possible adverse effects (see 29E, 2U).

In an age of ubiquitous and extensive collection of data through digital communication technologies, the right to protection of personal data and the right to respect for privacy are crucially challenged (Song and Ma 2022). Privacy is protected as a fundamental human right closely tied to the protection of personal data (see 26E, 28E), as well as respected as a value that concerns the human spirit and mentality (29E). The right to privacy must be upheld without exception, which encompasses the obligation to respect the user's right to informed consent (see 8U, 19U, 21U, 24E), abstain from processing personal data beyond the scope of its primary use and duration of storage, provide user controls that protect privacy (see 15U, 24E), and are subject to privacy reviews at the legal level (see 5U, 15U).

Transparency in the context of AI refers to the degree to which the underlying mechanisms and procedures governing the operation of AI systems are understandable (see 4U, 27E). People are more likely to trust an AI system that is transparent and forthcoming about its use of technology, and an AI is more likely to be trusted if people understand that the system is working to serve their needs and is clear about its limitations (see 15U). Hence, the principle of transparency always appears together with the principle of explainability. Explainability refers to the

ability to explain the technical processes of an AI system and the reasoning behind the decisions or predictions made by the AI system, which is essential for forging and sustaining user trust in the AI system (see 9U, 11U, 17U, 21U, 29E). In order to uphold fundamental human rights, it may be necessary to put in place further metrics of explainability, such as traceability (see 29E), auditability (see 2U, 20U, 22U), and open communication regarding the capabilities of AI systems. The degree to which explanation is needed is contingent upon the context and gravity of the consequences of incorrect or inaccurate output on the well-being of people.

AI algorithms and datasets have the potential to reflect, reinforce, or reduce unfair biases. Unfairness caused by AI to people includes those effects related to sensitive characteristics such as race, ethnicity, gender, nationality, income, sexual orientation, ability, and political or religious beliefs (see 8U). As such, the fair treatment of all people by AI is always associated with non-discrimination (see 9U, 12U, 19U, 22U, 25E). In addition to unfair bias, fair accessibility is also sought by the ethical principles of AI (see 25E). It means that AI systems should not have a one-size-fits-all approach and should consider Universal Design principles that serve a diverse range of users and adhere to pertinent accessibility standards. The aforementioned approach will promote fair and equal accessibility and participation of all people in existing and emerging computer-mediated human activities and assistive technologies (see 29E).

Although literally safety and security seem to have the same connotation, and indeed in some documents the two are used interchangeably (see 17U, 18U), the semantic distinction between the two principles can be clearly identified through collocation analysis (Stubbs 1995). Based on the examination of pairing among current texts, it can be inferred that security and privacy are consistently associated, while safety often co-occurs with reliability. Typically, security and privacy are often reviewed jointly to ensure the optimal level of depth and breadth of security review coverage to prevent potential security breaches, cyber-attacks and personal data breaches and to achieve privacy-friendly AI (see 15U, 24E). Safety, which typically refers to the reliability (see 3U, 4U), accuracy and repeatability of AI systems throughout their lifecycle (see 25E), requires cautious design and testing of AI systems and ongoing monitoring of their operation after deployment (see 8U).

The principle of responsibility underpins AI research and application. As the potential misuse of autonomous AI technologies poses a major challenge, risk awareness and a precautionary approach are essential. The principle of liability is therefore primarily concerned with the regulation of designers, implementers and operators of AI (see 3U, 5U), which involves legal responsibility, particularly in civil responsibility (liability and insurance) (see 24E). For instance, some purposes may inherently require human judgement, empathy and expertise, or a very high level of reliability and accuracy, such as healthcare diagnosis or driving, where it is essential

to consider the nature and type of possible errors in the performance of AI systems and the damage they may cause to the user.

A notable discrepancy arises when comparing the main themes of the AI ethics documents in the EU and US (cf. Table 2), whereby the former places greater emphasis on security, while the latter prioritises fairness. The notable disparity observed between the two regions in terms of AI development and regulation can be attributed to their divergent values and ideologies: the EU is more security-oriented and the US is more development-oriented. In the case of ChatGPT, the liberal environment in the US has given ChatGPT ample room for design and growth (Cath et al. 2018), but the neglect of the security risks raised by AI has hindered the further development of OpenAI. The European Union faces a dilemma whereby the setting of excessively stringent regulatory standards and the enforcement of heavy fines have led to a lag in the advancement of AI applications. As such, either over-emphasis on security or over-encouragement of development can bring corresponding social concerns, and neither security nor development can be compromised in the normative evolution of generative AI.

Thematic intertextuality analysis between ethical texts and legislative texts involves identifying and analyzing themes that are common to both types of texts, and how these themes are interconnected and intertwined (Hanks 1989). The majority of references to specific legal documents in AI ethics documents are presented as explicit intertextuality, either augmenting arguments or directly refuting them. In the discussion of the specific practice of accountability (see 1U), the text employs an oppositional intertextual strategy, citing laws in the US to refute the provisions, thus constituting an opposing value orientation between the legal text and the present text (Lemke 2005: 43).

However, certain U.S. laws, such as the Computer Fraud and Abuse Act (CFAA) and the Digital Millennium Copyright Act (DMCA), threaten to limit or prohibit this research by outlawing “unauthorized” interactions with computing systems, even publicly accessible ones on the internet. These laws should be clarified or amended to explicitly allow for interactions that promote such critical research.

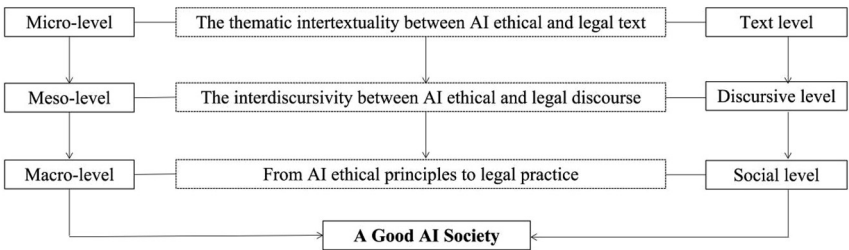
Whether it is a rebuttal to a legislative text or a supplement of a legislative text to support the arguments of an ethical principle, the underlying reason lies in the

**Table 2:** Top 5 ethical principles identified in EU and US.

Number	EU		US	
	Theme	Frequency	Theme	Frequency
1	Security	86 %	Accountability	63 %
2	Accountability	71 %	Fairness	50 %
3	Privacy	71 %	Privacy	45 %
4	Transparency	71 %	Transparency	45 %
5	Safety	57 %	Safety	36 %

“toothless” of the ethical principle (Rességuier and Rodrigues 2020), which enhances its reliability and credibility by citing a formal legal text with compulsory binding force. Although the themes identified in the AI ethics documents are mentioned in both the US and EU legislative texts (Li and Kit 2021), ethical principles are usually incorporated into the legislative language in an implicit or abstract way. For instance, the interpretation of ethical principles in the EU Artificial Intelligence Act refers to formally enacted laws and regulations but makes less reference to documents of ethical principles, even though they express the same values. In the US National Artificial Intelligence Initiative Act of 2020, the absence of a reference to the principle of accountability does not mean ignorance of this highly important AI ethical principle but rather reflected it in an abstract and implicit way by imposing obligations on related subjects in the “risk management” section. Similarly, the Act does not explicitly address or explicate the principle of accessibility, but rather situates it within the cultural context of the United States by employing the terms “adequate access” and “equitable access”. While legislative texts profoundly influence ethical documents, ethical texts may also inform legal frameworks. Legal and ethical texts on artificial intelligence show an increasing trend towards thematic intertextuality.

The intertextuality between legislative texts and ethical texts is characterized by a complex and dynamic relationship between legal and ethical norms and principles (cf. Figure 1). At the micro-textual level, thematic intertextuality analysis deconstructs the existing order established by the original text (Lemke 2002), offering the possibility of reconfiguring the arrangement of the thematic elements within the textual system and providing a reference for the reconstruction of a new meaningful text. At the meso-discursive level, ethical and legal discourses hold separate semantic scopes, but they can yield varying interpretations and reconstructions of the AI ethical principles through intertextual dialogue. At the macro-social level, AI ethical discourse can decode the ‘professionalization’ of legal narratives, provide explanations and promote the acceptability of ethical principles, while legal discourse can compensate for the ‘ineffectiveness’ of ethical discourse. Within such an intertextuality embracing dialogue (Cheng and Sin 2008), AI ethical principles exist as independent, concise and binding narrative elements and promote the jurisprudential interpretative power.



**Figure 1:** The dialectical relationship between AI ethical and legal discourse.



# 5 Conclusions

Generative AI, as a new technological application, has a noteworthy influence on the interaction between humans and AI, while presenting considerable potential for advancement at both the societal and industrial levels. The current debate regarding the potential replacement of humans by AI is of limited relevance, given that the primary aim of AI is to augment human welfare. For now, establishing a framework of governance for AI that adheres to the principles and fundamental principle of “anthropocentrism” is of paramount importance. This research employs critical discourse analysis as an approach, shedding light on the contemporary philosophical, ethical, and legal challenges associated with ChatGPT at the level of social research, demonstrating the necessity of incorporating ethical principles into legal norms to enhance the efficacy of ethical principles through intertextuality analysis at the text analysis level. The design of ethical guidelines and the formulation of legal policies for generative AI ought to uphold human dignity, with the welfare of human beings as the paramount value. While it may not be possible to entirely eradicate the issue of bias or discrimination in generative AI systems, it is imperative to undertake all possible measures to mitigate the associated risks. This includes refraining from transgressing legal and ethical boundaries and avoiding gradual compromises on the use of AI technology that may undermine the value of human subjects. The future of human-centred AI could be supported by a synergy of scientifically sound ethical guidelines and AI legal norms to ensure a space for innovation in AI-based technologies, products, and services while reducing external risks in areas such as privacy, security, competition, and accountability.

# Appendix

Code number	Name of document	Issuer	Country	Date of publishing
1U	The AI Now Report. The Social and Economic Implications of Artificial Intelligence Technologies in the Near-Term	AI Now Institute	USA	Sep-2016
2U	Statement on Algorithmic Transparency and Accountability	Association for Computing Machinery (ACM)	USA	Jan-2017
3U	AI Principles	Future of Life Institute	USA	Aug-2017
4U	AI – Our approach	Microsoft	USA	Oct-2017
5U	Artificial Intelligence. The Public Policy Opportunity	Intel Corporation	USA	Oct-2017
6U	IBM’s Principles for Trust and Transparency	IBM	USA	Jan-2018

(continued)

Code number	Name of document	Issuer	Country	Date of publishing
7U	OpenAI Charter	OpenAI	USA	Apr-2018
8U	Our principles	Google	USA	Jun-2018
9U	Everyday Ethics for Artificial Intelligence. A practical guide for designers & developers	IBM	USA	Sep-2018
10U	Governing Artificial Intelligence. Upholding Human Rights & Dignity	Data & Society	USA	Oct-2018
11U	Intel's AI Privacy Policy White Paper. Protecting individuals' privacy and data in the artificial intelligence world	Intel Corporation	USA	Oct-2018
12U	Introducing Unity's Guiding Principles for Ethical AI	Unity Technologies	USA	Nov-2018
13U	The Future Society, Law & Society Initiative, Principles for the Governance of AI	The Future Society	USA	Jul-2017
14U	AI Now 2018 Report	AI Now Institute	USA	Dec-2018
15U	Responsible bots: 10 guidelines for developers of conversational AI	Microsoft	USA	Nov-2018
16U	Preparing for the future of Artificial Intelligence	Executive Office of the President; National Science and Technology Council; Committee on Technology	USA	Oct-2016
17U	The National Artificial Intelligence Research and Development Strategic Plan	National Science and Technology Council; Networking and Information Technology Research and Development Subcommittee	USA	Oct-2016
18U	The National Artificial Intelligence Research and Development Strategic Plan 2019 updated	Selected Committee on Artificial Intelligence of the National Science & Technology Council	USA	Jun-2019
19U	AI Now 2019 Report	AI Now Institute	USA	Dec-2019
20U	AI Now 2023 Landscape	AI Now Institute	USA	Apr-2023
21U	Introduction to guidelines for human-AI interaction	Microsoft	USA	Apr-2023
22U	Standards for protecting at-risk groups in AI bias auditing	IBM	USA	Nov-2022
23E	Position on Robotics and Artificial Intelligence	The Greens (Green Working Group Robots)	EU	Nov-2016
24E	Report with recommendations to the Commission on Civil Law Rules on Robotics	European Parliament	EU	Jan-2017

(continued)

Code number	Name of document	Issuer	Country	Date of publishing
25E	Ethics Guidelines for Trustworthy AI	High-Level Expert Group on Artificial Intelligence	EU	Apr-2019
26E	An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations	AI4 People	EU	Nov-2018
27E	European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment	Concil of Europe: European Commission for the efficiency of Justice (CEPEJ)	EU	Dec-2018
28E	Statement on Artificial Intelligence, Robotics and ‘Autonomous’ Systems	European Commission, European Group on Ethics in Science and New Technologies	EU	Mar-2018
29E	Assessment List for Trustworthy Artificial Intelligence	the High-Level Expert Group on Artificial Intelligence (AI HLEG)	EU	Jul-2020

References

Acemoglu, Daron & Pascual Restrepo. 2020. The wrong kind of AI? Artificial intelligence and the future of labour demand. *Cambridge Journal of Regions, Economy and Society* 13(1). 25–35.

Aksela, Matti, Samuel Marchal, Andrew Patel, Lina Rosenstedt & WithSecure. 2022. *The security threat of AI-enabled cyberattacks*. Finland: Traficom Publications.

Bakhtin, Mikhailovich Mikhail. 1986. *Speech genres and other late essays*. Austin: University of Texas press.

Bingham, Lisa Blomgran. 2009. Collaborative governance: Emerging practices and the incomplete legal framework for public and stakeholder voice. *Journal of Dispute Resolution* 2009(2). 269–325.

Breeze, Ruth. 2021. Translating the principles of good governance: In search of accountability in Spanish and German. *International Journal of Legal Discourse* 6(1). 43–67.

Brodsky, Jessica S. 2016. Autonomous vehicle regulation: How an uncertain legal landscape may hit the brakes on self-driving cars. *Berkeley Technology Law Journal* 31(2). 851–878.

Cath, Corinne, Wachter Sandra, Mittelstadt Brent, Taddeo Mariarosaria & Floridi Luciano. 2018. Artificial intelligence and the ‘good society’: The US, EU, and UK approach. *Science and engineering ethics* 24. 505–528.

Čerka, Paulius, Jurgita Grigienė & Gintarė Sirbikytė. 2015. Liability for damages caused by artificial intelligence. *Computer Law & Security Report* 31(3). 376–389.

Čerka, Paulius, Jurgita Grigienė & Gintarė Sirbikytė. 2017. Is it possible to grant legal personality to artificial intelligence software systems? *Computer Law & Security Report* 33(5). 685–699.

Cheng, Le & David Machin. 2022. The law and critical discourse studies. *Critical Discourse Studies* 20(3). 243–255.

Cheng, Le & Xiuli Liu. 2022. Politics behind the law: Unveiling the discursive strategies in extradition hearings on Meng Wanzhou. *International Journal of Legal Discourse* 7(2). 235–255.

- Cheng, Le, Yuxin Liu & Yun Zhao. 2021. Exploring the U.S. Institutional discourse about critical information infrastructure protection (CIIP): A corpus-based analysis. *International Journal of Legal Discourse* 6(2). 323–347.
- Cheng, Le & King-kui Sin. 2008. A court judgment as dialogue. In Edda Weigand (ed.), *Dialogue and rhetoric*, 267–281. Amsterdam: Benjamins.
- Chesterman, Simon. 2020. Artificial intelligence and the limits of legal personality. *International and Comparative Law Quarterly* 69(4). 819–844.
- Clarke, Roger. 1993. Asimov's laws of robotics: Implications for information technology-Part I. *Computer* 26(12). 53–61.
- Clarke, Roger. 1994. Asimov's laws of robotics: Implications for information technology-Part II. *Computer* 27(1). 57–66.
- Curchod, Corentin, Patriotta Gerardo, Laurie Cohen & Neysen Nicolas. 2020. Working for an algorithm: Power asymmetries and agency in online work settings. *Administrative Science Quarterly* 65(3). 644–676.
- Fairclough, Norman. 1992. *Discourse and social change*. Cambridge: Polity Press.
- Fairclough, Norman. 1995. *Critical discourse analysis: The critical study of language*. London & New York: Longman.
- Fairclough, Norman. 2003. *Analysing discourse: Textual analysis for social research*. London: Routledge.
- Floridi, Luciano, Cows Josh, Beltrametti Monica, Chatila Raja, Chazerand Patrice, Dignum Virginia, Luetge Christoph, Madelin Robert, Pagallo Ugo, Francesca Rossi, Burkhard Schafer, Valcke Peggy & Vayena Effy. 2018. AI4People—an ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines* 28. 689–707.
- Flynn, Eilionóir & Anna Arstein-Kerslake. 2014. Legislating personhood: Realising the right to support in exercising legal capacity. *International Journal of Law in Context* 10(1). 81–104.
- Gal, Susan. 2006. Linguistic anthropology. In Keith Brown (ed.), *Encyclopedia of language and linguistics*, 171–185. Oxford: Elsevier.
- Gao, Yubing, Wei Tong, Q. Wu Edmond, Wei Chen, Guangyu Zhu & Fei-Yue Wang. 2023. Chat with chatgpt on interactive engines for intelligent driving. *IEEE Transactions on Intelligent Vehicles* 3. 1–3.
- Ghosh, Ashish, Debasrita Chakraborty & Anwesha Law. 2018. Artificial intelligence in Internet of things. *CAAI Transactions on Intelligence Technology* 3(4). 208–218.
- Gordon, Thomas F., Prakken Henry & Walton. Douglas. 2007. The Carneades model of argument and burden of proof. *Artificial Intelligence* 171(10–15). 875–896.
- Haberer, Adolphe. 2007. Intertextuality in theory and practice. *Literatura* 49(5). 54–67.
- Hanks, William F. 1989. Text and textuality. *Annual review of anthropology* 18(1). 95–127.
- Irwin, William. 2004. Against intertextuality. *Philosophy and Literature* 28(2). 227–242.
- Jabotinsky, Hadar Yoana & Roe Sarel. 2022. Co-Authoring with an AI? Ethical dilemmas and artificial intelligence. *Ethical Dilemmas and Artificial Intelligence* 12. 1–29.
- Jobin, Anna, Marcello Ienca & Effy Vayena. 2019. The global landscape of AI ethics guidelines. *Nature Machine Intelligence* 1(9). 389–399.
- Kelsen, Hans. 1967. *Pure theory of law*. California: University of California Press.
- King, Michael R. & ChatGPT. 2023. A conversation on artificial intelligence, chatbots, and plagiarism in higher education. *Cellular and Molecular Bioengineering* 16(1). 1–2.
- Korngiebel, Diane M. & Sean D. Mooney. 2021. Considering the possibilities and pitfalls of Generative Pre-trained Transformer 3 (GPT-3) in healthcare delivery. *NPJ Digital Medicine* 4(1). 93.
- Kristeva, Julia. 1980. *Desire in language: A semiotic approach to literature and art*. New York: Columbia University Press.

- Lemke, Jay L. 1985. Ideology, intertextuality, and the notion of register. *Systemic perspectives on discourse* 1. 275–294.
- Lemke, Jay L. 2002. Ideology, intertextuality and the communication. In David Lockwood, Peter Fries, William Spruiell & Michael Cummings (eds.), *Relations and functions within and around language*, 32–56. London: Continuum.
- Lemke, Jay L. 2005. *Textual politics: Discourse and social dynamics*. London: Taylor & Francis.
- Li, Siyue & Chunyu Kit. 2021. Legislative discourse of digital governance: A corpus-driven comparative study of laws in the European union and China. *International Journal of Legal Discourse* 6(2). 349–379.
- Locke, Terry. 2004. *Critical discourse analysis*. London and New York: Bloomsbury Publishing.
- Lupton, Deborah. 2018. How do data come to matter? Living and becoming with personal data. *Big Data & Society* 5(2). 1–11.
- McBride, Russ, Alireza Dastan & Poorya Mehrabinia. 2022. How AI affects the future relationship between corporate governance and financial markets: A note on impact capitalism. *Managerial Finance* 48(8). 1240–1249.
- Miller, Alan D. & Ronen Perry. 2012. The reasonable person. *New York University Law Review* 87(2). 323–392.
- Morley, Jessica, Kinsey Libby, Elhalal Anat, Francesca Garcia, Ziosi Marta & Floridi Luciano. 2023. Operationalising AI ethics: Barriers, enablers and next steps. *AI & Society* 38. 411–423.
- Murphy, Robin & David D. Woods. 2009. Beyond Asimov: The three laws of responsible robotics. *IEEE Intelligent Systems* 24(4). 14–20.
- Naudé, Wim & Nicola Dimitri. 2020. The race for an artificial general intelligence: Implications for public policy. *AI & Society* 35. 367–379.
- Ochigame, Rodrigo. 2019. The invention of ‘ethical AI’: How big tech manipulates academia to avoid regulation. In Thao Phan, Jake Goldenfein, Declan Kuch & Monique Mann (eds.), *Economies of virtue*, 49–59. Amsterdam: Institute of Network Cultures.
- O’Leary, Daniel E. 2013. Artificial intelligence and big data. *IEEE Intelligent Systems* 28(2). 96–99.
- Panch, Trishan, Heather Mattie & Leo Anthony Celi. 2019. The “inconvenient truth” about AI in healthcare. *NPJ Digital Medicine* 2(1). 77.
- Pearlman, Russ. 2017. Recognizing artificial intelligence (AI) as authors and investors under US intellectual property law. *Richmond Journal of Law and Technology* 24(2). 1–22.
- Pei, Jiamin, Dandi Li & Le Cheng. 2022. Media portrayal of hackers in China daily and the New York times: A corpus-based critical discourse analysis. *Discourse & Communication* 16(5). 598–618.
- Ponkin, Igor V. & Alena I. Redkina. 2018. Artificial intelligence from the point of view of law. *RUDN Journal of Law* 22(1). 91–109.
- Raub, McKenzie. 2018. Bots, bias and big data: Artificial intelligence, algorithmic bias and disparate impact liability in hiring practices. *Arkansas Law Review* 71(2). 529–570.
- Rességuier, Anaïs & Rowena Rodrigues. 2020. AI ethics should not remain toothless! A call to bring back the teeth of ethics. *Big Data & Society* 7(2). 1–5.
- Solaiman, Sheikh M. 2017. Legal personality of robots, corporations, idols and chimpanzees: A quest for legitimacy. *Artificial Intelligence and Law* 25. 155–179.
- Song, Lijue & Changshan Ma. 2022. Identifying the fourth generation of human rights in digital era. *International Journal of Legal Discourse* 7(1). 83–111.
- Stilgoe, Jack. 2018. Machine learning, social learning and the governance of self-driving cars. *Social studies of science* 48(1). 25–56.
- Stokel-Walker, Chris & Richard Van Noorden. 2023. The promise and peril of generative AI. *Nature* 614, 214–216.
- Stubbs, Michael. 1995. Collocations and semantic profiles: On the cause of the trouble with quantitative studies. *Functions of language* 2(1). 23–55.

- Tikkinen-Piri, Christina, Rohunen Anna & Jouni Markkula. 2018. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Report* 34(1). 134–153.
- Thorp, H. Holden. 2023. ChatGPT is fun, but not an author. *Science* 379(6630). 313.
- Van Dis, A.M. Eva, Bollen Johan, Willem Zuidema, Robert van Rooij & Claudi L. Bockting. 2023. ChatGPT: Five priorities for research. *Nature* 614(7947). 224–226.
- Wang, Chunhui, Le Cheng & Jiamin Pei. 2020. Exploring the cyber governance discourse: A perspective from China. *International Journal of Legal Discourse* 5(1). 1–15.
- Wallach, Wendell & Gary E. Marchant. 2018. An agile ethical/legal model for the international and national governance of AI and robotics. In *Paper presented at the AAAI/ACM conference on AI, ethics, and society, New Orleans, LA, USA, 2–3 February*.
- Wang, Qian. 2017. Qualitative research on the content of artificial intelligence in copyright law. *Science of Law (Journal of Northwest University of Political Science and Law)* 35(5). 148–155.
- Warwick, Kevin. 2013. *Artificial intelligence: The basics*. London: Routledge.
- Wodak, Ruth & Michael Meyer. 2009. *Methods of critical discourse studies*. London: SAGE.
- Wu, Zhonghua & Le Cheng. 2022. Exploring Metaphorical representations of law and order in China's government work reports: A corpus-based diachronic analysis of legal Metaphors. *Critical Arts* 36(5–6). 96–112.
- Zohny, Hazem, John McMillan & Mike King. 2023. Ethics of generative AI. *Journal of Medical Ethics* 49(2). 79–80.

## Bionotes

### Le Cheng

Guanghua Law School and School of International Studies, Zhejiang University, Hangzhou, China  
**chengle163@hotmail.com**  
<https://orcid.org/0000-0002-4423-8585>

Le Cheng is Chair Professor of Law and Professor of Legal Discourse and Translation at Zhejiang University. He serves as the Executive Vice Dean of Zhejiang University's Academy of International Strategy and Law. His research interests and publications are in the areas of international law, digital law, data governance, semiotics, discourse studies, terminology, and legal discourse and translation.

### 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 in the School of International Studies, Zhejiang University. Her research fields include legal discourse, digital law, critical discourse studies, and corpus linguistics.