

RESEARCH ARTICLE

Gender in a stereo-(gender)typical EU AI law: A feminist reading of the AI act

Anastasia Karagianni 

Doctoral Researcher at Law Science Technology and Society (LSTS) Research Group, Faculty of Law and Criminology, Vrije Universiteit Brussels (VUB), Former FARI Scholar, Brussels, Belgium
Email: anastasia.karagianni@vub.be

(Received 3 November 2024; revised 4 March 2025; accepted 17 April 2025)

Abstract

This paper examines the European Regulation (EU) 2024/1689 on harmonised rules on artificial intelligence (AI), commonly known as AI Act, through a feminist lens, analysing how the proposed regulatory framework addresses gender, non-discrimination and systemic power imbalances. Drawing on Miranda Fricker's theory of hermeneutical injustice, Catharine MacKinnon's feminist legal theory on male dominance, Aníbal Quijano's concept of "coloniality of power" and Walter Mignolo's theory of epistemology and the decoloniality of law, the paper critiques the AI Act's approach to gender bias and discrimination. The findings argue that while the AI Act seeks to mitigate gendered risks, it falls short of addressing the structural biases embedded in AI technologies, which disproportionately harm marginalised groups. Following an introduction that highlights the significance of this research, the paper provides a background on the formulation of the AI Act's final text and outlines the methodological approach used to select key provisions for analysis. The main section critically examines specific articles of the AI Act with gendered implications, demonstrating how existing provisions either reinforce or fail to challenge algorithmic discrimination. The conclusion underscores the necessity of stronger mechanisms to address gender-based inequities in AI development and deployment from an intersectional perspective. The paper closes by proposing feminist-informed revisions to the AI Act that emphasise gender inclusivity, intersectionality and accountability in AI governance, advocating for a more equitable AI framework that reflects the lived experiences of women, LGBTQIA+ people and marginalised communities.

Keywords: AI Act; feminism; gendered risks; intersectionality; structural inequalities

1. Introduction

Artificial intelligence (AI) technology often reinforces societal biases, resulting in discriminatory outcomes across various domains (Halberstam, 1991). For example, Amazon's AI recruitment tool, designed to automate hiring processes, was found to disadvantage women by favouring male-dominated language due to biased training data, ultimately leading to its discontinuation (Andrews & Bucher, 2022). In healthcare, AI applications, such as gynaecologic cancer detection, operate within binary gender frameworks, often misgendering transgender and non-binary patients (Taylor & Bryson, 2016). Additionally, generative AI raises legal concerns, particularly in the proliferation of non-consensual sexualised deepfakes, which constitute a form of gender-based violence (Holliday, 2021). Given these challenges, the regulation of AI through a gender-sensitive approach is imperative.

This paper critically examines the AI Act (European Commission, 2024) through a feminist lens, employing feminist legal methods to analyse its interaction with EU law and assess its implications for gender inclusivity, non-discrimination and accountability. The AI Act, intended to mitigate risks associated with high-risk AI systems, includes provisions allowing for the processing of “special categories of personal data” under specific conditions to prevent algorithmic discrimination (Scientific Research Committee of the European Parliament, 2025). However, gender is not classified as a “special category” under Article 9 (1) General Data Protection Regulation (GDPR) (European Commission, 2016), creating legal ambiguities that may impede efforts to address systemic gender inequalities.

The absence of explicit references *inter alia* to gender equality in early drafts of the AI Act – largely due to opposition from Member States such as Poland – underscores broader gaps in AI governance (Stolton, 2020). A gender-responsive text analysis reveals that while the AI Act references “non-discrimination” in multiple provisions, explicit references to “gender equality” appear only twice in the Recitals (Recitals 27 and 48 AI Act) and once in Article 95(2)(e) AI Act, which concerns codes of conduct for voluntary application. Moreover, while the AI Act acknowledges gender-based discrimination, it fails to account for inclusive gender identities such as transgender, non-binary, intersex and gender non-conforming people, highlighting the need for more inclusive regulatory frameworks.

A *de lege lata* interpretation of the AI Act recognises that the AI Act incorporates human rights protections, yet its approach remains largely formalistic, treating algorithmic bias as a technical rather than structural issue (Frischhut, 2022; Tzimas, 2021). A *de lege ferenda* analysis, however, reveals deeper limitations in addressing gendered power imbalances within AI governance (Stierle, 2021). Drawing from Miranda Fricker’s theory of hermeneutical injustice (MacKinnon, 2013), MacKinnon’s dominance theory (Fricker, 2007) and intersectionality as developed by Ann Julia Cooper (Cooper, 1988) and Kimberlé Crenshaw (Crenshaw, 1991), this paper argues that AI regulation assumes legal neutrality while overlooking systemic gendered and racialised biases. Hermeneutical injustice is particularly relevant in AI governance, as marginalised groups often lack the epistemic resources to contest discriminatory AI systems (Rafanelli, 2022). MacKinnon’s critique of formal equality further illustrates how algorithmic decision-making reflects male-dominated norms embedded in legal and data structures (Bird-Pollan, 2020). MacKinnon’s dominance theory is particularly relevant, as algorithmic decision-making frequently reflects male-dominated norms due to biased training data and the legal system’s implicit androcentrism (Doh, Canali & Karagianni, 2024). Rather than treating gender bias as an incidental flaw, a substantive equality approach necessitates active restructuring of AI policies to dismantle male dominance in data collection, model training and regulatory oversight. Without such structural interventions, the AI Act risks reinforcing, rather than mitigating, existing inequalities by treating AI bias as a technical issue rather than a deeply entrenched social and legal challenge.

Yet, hermeneutical approaches from decolonial scholars argue that law should be interpreted with historical consciousness, acknowledging colonial violence, racial capitalism and epistemic injustice. Decolonial theorists like Aníbal Quijano (Quijano, 2000) and Walter Dignolo (Dignolo, 2012) argue that modern law is deeply rooted in coloniality – the ongoing dominance of Western epistemologies, legal structures and institutions (de Sousa Santos, 2024). Legal hermeneutics within colonial and postcolonial contexts often interprets laws through Eurocentric frameworks, marginalising Indigenous, African and non-Western jurisprudence. AI systems have been shown to disproportionately misclassify racialised and gender-diverse individuals, reinforcing structural inequalities. A decolonial feminist approach to AI law demands that regulatory frameworks centre marginalised identities rather than treating them as afterthoughts (Ricaurte & Zasso, 2023).

The European Parliament’s LIBE and FEMM Committees played a pivotal role in shaping amendments to the AI Act, particularly advocating for transparency, privacy protection and anti-discrimination measures (Scientific Research Committee-European Parliament, 2024). Their

contributions emphasised the necessity for AI systems to be interpretable, especially in high-risk domains such as law enforcement and social services, to ensure compliance with the GDPR and safeguard fundamental rights. A primary focus of these amendments was mitigating biases in AI algorithms, particularly those that could lead to discrimination based on gender, race or other protected characteristics in hiring, credit scoring and surveillance technologies. The European Parliament introduced additional requirements for high-risk AI systems, including provisions for human oversight, transparency, non-discrimination and social responsibility (Scientific Research Committee-European Parliament, 2024). However, these amendments fell short of addressing the deeper social construction of gender, raising concerns about the effectiveness of gender equality measures in AI governance.

This paper critically examines the AI Act across three key stages: (1) pre-market regulation during the design phase for product manufacturers and providers, (2) the responsibilities of AI providers and (3) the post-release obligations of deployers, aligning with the categorisation of responsibilities between product manufacturers,¹ deployers² and providers.³ While the AI Act requires bias testing (Article 10 (2) (g) AI Act) and human oversight (Article 14 (2) AI Act), it does not mandate intersectional gender audits (Article 17 AI Act) or diverse AI development teams (Recital 165 AI Act). In the post-release phase, providers must monitor AI performance (Article 72 AI Act), but the AI Act relies heavily on self-regulation, lacking strong redress mechanisms for algorithmic discrimination. Without robust structural interventions, the AI Act risks reinforcing – rather than mitigating – existing gendered inequalities in AI governance. This paper argues for feminist legal interventions that emphasise intersectionality, accountability and the dismantling of structural biases in AI regulation.

2. A feminist reading of the AI act as a pre-market regulation

In the pre-market design phase, under Article 6 AI Act, high-risk obligations apply to AI systems classified as a “safety component” under Annex I, Section A, or as a “high-risk AI system” under Annex III. Developers of such systems must adhere to a series of regulatory requirements to ensure compliance. These obligations include establishing and implementing risk management processes (Article 9 AI Act) and using high-quality training, validation and testing data (Article 10 AI Act). Additionally, systems must maintain transparency and provide user information (Article 13 AI Act) and integrate human oversight measures (Article 14 AI Act). Further, developers must establish a quality management system (Article 17 AI Act).

In case of General Purpose AI (GPAI) models, they are subject to specific obligations under Article 53 AI Act. Developers must create and maintain technical documentation and provide it to the AI Office upon request. Additionally, they must ensure that providers integrating AI models have access to necessary documentation while balancing transparency with intellectual property protection. Furthermore, developers must publish a publicly available summary of the AI model's training data using a standardised template provided by the AI Office. If a GPAI model functions as, or is integrated into, a high-risk AI system, additional obligations under Recital 85 may apply, either directly or indirectly. However, a key responsibility is to avoid exploiting vulnerabilities which constitutes a prohibited practice (Article 5 AI Act). A feminist perspective on the definition of “vulnerabilities” and the interpretation of this provision is essential.

¹The product manufacturer places on the market or puts into service an AI system together with their product and under their own name or trademark (Article 3 (2-8) AI Act and Recital 87 AI Act).

²Deployer is any natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity (Article 3 (2-8) AI Act and Recital 87 AI Act).

³Provider is a natural or legal person, public authority, agency or other body that develops an AI system or a general purpose AI model (or that has an AI system or a general purpose AI model developed) and places them on the market or puts the system into service under its own name or trademark, whether for payment or free of charge (Article 3 (2-8) AI Act and Recital 87 AI Act).

2.1. *Vulnerability in prohibited practices: insights from feminism*

Article 5 of the AI Act outlines AI practices that pose unacceptable risks to safety and fundamental rights, identifying specific AI systems and techniques that are banned outright due to their potential to cause harm. These include social scoring AI systems (Article 5(1)(c)), which evaluate or categorise individuals based on their social behaviour or personal characteristics, as well as manipulative techniques (Articles 5(1)(a) and (b)) that exploit individual vulnerabilities, such as those affecting children, to manipulate behaviour (Longo, 2023). The protection of vulnerability is further enshrined in Recital 110 of the AI Act. However, what is considered as “vulnerable” under this provision?

The concept of vulnerability originates from Computer Science, where it refers to security flaws, glitches or weaknesses in software code that can be exploited by attackers (Praveen Kumar, 2022). In contrast, in the Social Sciences and Gender Studies, vulnerability is framed within the context of self-determination, as it diminishes an individual’s capacity and implies a reliance on others for support (Longo, 2023). For example, the portrayal of Indigenous women as naked frequently intersects with narratives of vulnerability, reinforcing harmful stereotypes and colonial power dynamics. Such depictions have historically been used to strip Indigenous women of their dignity, autonomy and humanity, framing them as inherently vulnerable and sexualised beings (Levine, 2008). This intersection of nudity and vulnerability is deeply rooted in colonialism, exoticism and patriarchy, shaping contemporary perceptions and treatment of Indigenous women. These critical concerns extend to the design and deployment of AI technologies, raising important questions about their impact on marginalised communities.

With the proliferation of AI technologies designed by global tech monopolies and deployed worldwide, the concept of decolonisation in AI governance has become increasingly relevant. Decolonisation entails a critical, evidence-informed appraisal of colonial histories and their entanglements with the present, particularly in relation to power and gender imbalances. Addressing these historical legacies is crucial for exposing oppressive AI systems and advancing intersectional approaches to AI ethics and governance (Rachel, 2021; Shakir, 2020; Siapera, 2022).

Oppression, broadly defined as the exercise of power in a burdensome, cruel or unjust manner, has historically been used to subordinate marginalised groups, including women and gender minorities. AI systems are embedded in historical and systemic forms of oppression, often reflecting biases present in their training data. In *Data Feminism*, Catherine D’Ignazio and Lauren F. Klein highlight the ways in which power structures influence data collection, presentation and interpretation, thereby shaping AI-driven decision-making (D’Ignazio, 2020). This analysis aligns with Patricia Hill Collins’ *matrix of domination*, a framework that examines interlocking systems of oppression – white supremacy, patriarchy, capitalism and settler colonialism – across structural, disciplinary, hegemonic and interpersonal domains (Costanza-Chock, 2020; Hill Collins, 2009). Within this context, intersectionality serves as a methodological approach that helps uncover the multifaceted layers of discrimination embedded in AI systems. As many AI systems reflect racial, gender and socio-economic biases due to flawed data collection practices, *Feminist Data Set* by Caroline Sindors seeks to counteract these biases by ensuring diverse and representative data sources that prioritise fairness, intersectionality and accountability (Sindors, 2020).

In this regard, an analysis of Article 5(1)(e-h) AI Act reveals the need for a feminist perspective, as this provision prohibits biometric categorisation systems that rely on sensitive characteristics, such as political and religious beliefs, race or sexual orientation, in public spaces. While these provisions emphasise the importance of privacy, dignity and non-discrimination, they notably exclude gender from the list of protected characteristics, raising concerns about how gender will be safeguarded in AI-driven assessments of social behaviour and gender performativity (Butler, 1990, 2024). Similarly, under Articles 4(14) and 9 of the GDPR (European Parliament & Council of the European Union, 2016), “biometric data” are defined as personal data derived from technical processing of physical, physiological or behavioural characteristics to uniquely identify an individual. However, gender is not

explicitly included in these provisions, meaning it is not recognised as a special category of protected data. In their *Joint Opinion 5/2021* (European Data Protection Supervisor (EDPS) & European Data Protection Board (EDPB), 2021; Malgieri & Fuster, 2022), the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) recommended a ban on AI biometric categorisation systems that classify individuals based on gender. Nevertheless, despite these recommendations, this provision does not appear to have been incorporated into the AI Act, which was formally adopted in 2024.

To conclude, *vulnerability* under the AI Act refers to the potential risks and harms that individuals or groups may face due to the deployment and use of AI systems, particularly those involving sensitive data or high-risk applications. The concept of vulnerability in AI encompasses the various ways in which individuals, groups, systems or even entire societies can be at risk due to the development, deployment or use of AI technologies. Current literature highlights the limited conceptualisation of vulnerability within the Act and calls for a more comprehensive approach that addresses the vulnerabilities of all stakeholders in AI, including developers and organisations (Galli & Novelli, 2024). Issues such as gender stereotyping embedded in AI systems (Doh et al., 2024) and the lack of regulation surrounding the harmful development and deployment of generative AI technologies – such as the creation of non-consensual sexualised deepfakes (Karagianni, 2025) – should be properly addressed within the AI Act. While Article 5(b) of the EU Gender-Based Violence (GBV) Directive (European Parliament and Council, 2024) criminalises the production, manipulation and dissemination of non-consensual intimate or altered material, it is essential that this gendered harm be acknowledged within the AI Act to ensure that accountability provisions are explicitly included.

3. The responsibilities of AI providers

The AI Act introduces distinct but interconnected processes to regulate AI systems in the European Union. The harmonisation process (Articles 1 (2), 4 and 52 AI Act) aims to create a unified regulatory framework, ensuring cooperation between national authorities and consistency across EU member states by setting common rules, definitions and risk classifications for AI systems, thus preventing fragmentation in national regulations. Harmonisation process ensures a unified regulatory approach across the European Union. On the other hand, conformity assessment verifies compliance with the AI Act's legal and technical requirements (Articles 6, 16, 30 and 43 AI Act). The conformity assessment process ensures that AI systems, particularly those deemed high-risk, meet the AI Act's requirements, either through internal self-assessment (Article 20 AI Act) or third-party evaluation by a Notified Body (Article 43 AI Act). Successful completion of this assessment may result in the issuance of a CE marking, enabling the AI system's market entry within the EU. To this extend, the standardisation process (Articles 40 and 41 AI Act) involves the development of technical standards by recognised European bodies, providing guidelines for AI design, risk management and performance, which, although not legally binding, facilitate conformity assessments. Together, these processes ensure regulatory coherence, technical compliance and legal market access for AI systems across the EU. In this section, the harmonisation requirement, the conformity assessment and the standardisation process will be examined to address gender stereotyping and male dominance in AI, ensure compliance with gender equality and non-discrimination in standards and promote accountability for gendered harms.

3.1. Exploring feminist perspectives on EU harmonisation requirement

The AI Act aims to create a harmonised legal framework across EU Member States, ensuring consistency in AI regulations (Articles 1 (2), 4 and 52 AI Act). This involves setting uniform rules, definitions and risk-based classifications for AI systems to prevent fragmentation across different

national regulations. It ensures that AI providers and deployers operate under the same legal requirements regardless of the country within the EU. Article 6 of the AI Act addresses the requirements for high-risk AI systems to ensure they comply with specific standards for safety, transparency and accountability. By establishing common standards for high-risk AI systems, Article 6 of the AI Act aims to harmonise regulations across EU Member States, promoting a unified approach to AI governance while protecting fundamental rights. *Harmonisation*, in this context, refers to aligning national laws with EU law to create a single legal framework across the European Union (Klamert, 2015). Significant pieces of EU legislation, such as the GDPR (European Commission, 2016), the Digital Services Act (European Parliament & Council of the European Union, 2022a), the Digital Markets Act (European Parliament & Council of the European Union, 2022b) and the EU Equality and Non-Discrimination Law (European Union, 2000), aim to regulate data use, online platforms, competition and human rights protection. Through these laws, Article 6 AI Act seeks to ensure consistency, interoperability and fairness. When considering this legislation from feminist perspectives, it becomes crucial to examine how these laws impact the inclusion of a gender equality and non-discrimination angle within the AI Act.

A feminist perspective on Article 6 AI Act provides critical insight into the potential and pitfalls of EU harmonisation efforts. Feminist scholars and activists often evaluate how such legislation addresses issues of gender equality, inclusivity and intersectionality (Anagnostou & Millns, 2013). Women, particularly in marginalised communities, face specific risks related to privacy breaches and surveillance, as in cases of domestic violence where their data can be weaponised. Feminist scholars argue that the GDPR needs stronger protections that explicitly account for these *vulnerabilities* (Malgieri & Fuster, 2022) – as was explained above – particularly around location tracking, personal data exposure and consent (Sovacool, Furszyfer-Del Rio & Martiskainen, 2021). They also emphasise that data protection laws, such as the GDPR, should be interpreted with a focus on bodily autonomy, allowing individuals – particularly women – to have more control over their personal data, especially in cases of image-based sexual abuse (Rigotti & McGlynn, 2022) and the generation of non-consensual sexualised deepfakes (Karagianni & Doh, 2024).

Regarding the harmonisation of the AI Act with the EU Equality and Non-Discrimination Law,⁴ the key feminist concept of intersectionality deserves special attention. The concept of *intersectionality*, first introduced by Ann Julia Cooper in 1892 (Cooper, 1988) and later popularised by American scholar Professor Kimberlé Crenshaw (Crenshaw, 1991), examines how different aspects of a person's identity intersect. Crenshaw used the concept to describe how Black women experience discrimination differently from both white women (who face sexism but not racism) and Black men (who face racism but not sexism). She highlighted how traditional feminist and anti-racist movements had often failed to fully account for the unique challenges faced by Black women, who experience both sexism and racism simultaneously in ways distinct from those faced by men of colour or white women. *Intersectionality* refers to how different forms of discrimination (e.g., gender, race, class) intersect and compound one another. Therefore, EU harmonisation efforts must not only focus on gender equality in isolation but should also address how different forms of marginalisation interact (Xenidis, 2018). For instance, a woman of colour may face discrimination that is both gendered and racialised in online spaces, requiring specific protections. From a feminist perspective, harmonisation should not lead to homogenisation – a “one-size-fits-all” approach that fails to account for the diverse social, economic and cultural contexts of EU Member States. Instead, harmonisation should actively prioritise gender equality, inclusivity and the protection of marginalised groups, extending beyond the goal of merely ensuring market efficiency and consistency. This requires embedding feminist principles, such as intersectionality, inclusivity and accountability, into the development, implementation and monitoring of EU laws.

⁴European Equality and Non-Discrimination Law encompasses all the European legislation on equal treatment and non-discrimination.

In this regard of harmonising the AI Act with EU Equality and Non-Discrimination Law,⁵ the contributions of González Sabzée (Salzberg, 2019) and Gyan (Guyan, 2022) are particularly significant. More specifically, González Sabzée critiques the limitations of human rights law in fully addressing the complexities of sexual and gender identities. The existing framework often operates under binary categories of male/female and heterosexual/homosexual, which can marginalise individuals who do not conform to these categories. González Sabzée argues that while human rights law is evolving, it still tends to reinforce these binary and normative understandings, thus overlooking the lived experiences of queer and trans individuals (Salzberg, 2019). González Sabzée explores the process of “queering” human rights law, which involves examining how legal norms around human rights can be expanded and challenged through queer theory. Queer theory critiques traditional norms related to gender, sexuality and identity, which are often heteronormative (focused on heterosexuality as the norm) and cisnormative (focused on cisgender identities). In this context, “queering” human rights law means questioning and altering the existing legal frameworks to be more inclusive of diverse and non-binary gender identities, as well as sexual orientations (Salzberg, 2019). To this extent, Guar also emphasises the importance of critically analysing how data about gender, sex and sexuality are gathered and used (Guyan, 2022). He argues that the collection of such data is often limited and standardised, reflecting heteronormative and cisnormative assumptions that overlook the complexities of queer identities (Guyan, 2022). By queering data, Guar seeks to challenge these conventional frameworks and encourage more inclusive data practices.

These contributions clearly demonstrate that gender equality should not be understood as solely concerning women in isolation or reinforcing exclusionary gender norms. Instead, a feminist analysis seeks to dismantle patriarchal structures that affect people of all genders, including men, non-binary and gender non-conforming people. Various feminist perspectives, such as intersectional feminism and queer feminism, emphasise that gender justice is deeply interconnected with factors such as race, class, sexuality and disability (Ahmed, 1996; Delmar, 2018; Lewis, 2025). These perspectives highlight how systems of power shape experiences differently across social groups and advocate for a more inclusive approach that extends beyond women’s issues alone.

3.2. *Rethinking conformity assessments in the context of gender equality*

Under the AI Act, high-risk AI systems (Article 6 AI Act) require a conformity assessment to ensure compliance with safety and ethical standards, involving the review of documentation, risk management processes (Article 9 AI Act), data governance (Article 10 and Annex VII AI Act) and technical measures (Articles 9 and 13 and Annex IV AI Act). In some cases, the assessment must be carried out by a Notified Body (Article 43 AI Act), an independent third-party organisation designated by EU Member States. For low-risk AI systems, a self-assessment suffices (Article 20 AI Act), where providers verify that the system meets basic requirements such as data quality and transparency. The conformity assessment process is described in Chapter III AI Act and involves several steps: risk management, where providers demonstrate a risk assessment; documentation, including technical records of compliance with the AI Act; testing, to evaluate adherence to required standards; and audit trails, ensuring accountability and human oversight. If successful, the AI system receives a CE marking – *a marking by which a provider indicates that an AI system is in conformity with the requirements set out in Chapter III* (Article 3 point 24 AI Act), signifying compliance with EU regulations, and can be marketed within the EU. For high-risk systems, the provider must also make the assessment and documentation available to relevant authorities.

Article 6 AI Act focuses on ensuring safety, transparency and accountability in AI technologies, while Article 43 AI Act creates a centralised body to facilitate cooperation and guidance among EU

⁵European Equality and Non-Discrimination Law encompasses all the European legislation on equal treatment and non-discrimination.

Member States. This dual approach aims to promote responsible AI development and use while protecting the rights and interests of individuals. Annex III, point 4 (a) of the AI Act mandates that AI systems used for targeted job advertisements, application filtering and candidate evaluation undergo a conformity assessment. This requirement arises from the well-documented risks of algorithmic bias, particularly when AI models are trained on historically biased datasets, which can systematically disadvantage women and marginalised groups. For instance, automated resume filtering systems may penalise career gaps, disproportionately affecting women, particularly those who have taken maternity leave (Ajunwa, 2019). Similarly, AI-driven video interviews, which analyse facial expressions, speech patterns or other biometric data, may introduce bias against candidates with disabilities, accents or non-Western communication styles, further exacerbating barriers to employment (Biswas et al., 2024).

As was explained above, conformity assessment refers to the evaluation of AI systems to determine whether they meet specific standards, regulations and ethical guidelines before deployment or use (O'Connor & Liu, 2024). These assessments typically aim to ensure that AI systems are safe, reliable, fair and free from bias. However, from a feminist perspective, issues such as gender bias, inclusivity and power structures must be critically examined, particularly in light of systemic inequalities and the risk of reinforcing these disparities if assessments are not designed through an intersectional lens. One of the most pressing feminist concerns regarding AI is its potential to perpetuate gender biases through biased algorithms and training data. AI systems are often trained on historical datasets that reflect existing social inequalities (Keyes, 2018). Consequently, conformity assessments should mandate comprehensive bias audits that extend beyond detecting overt discrimination to uncover subtle, structural biases that disproportionately affect women – particularly women of colour, LGBTQIA+ people and other marginalised groups (Kobayashi & Nakao, 2020; Magee, Ghahremanlou, Soldatic & Robertson, 2021). For example, AI systems used in recruitment or healthcare may disadvantage women by underrepresenting their experiences or needs in training datasets. In recruitment, AI-driven hiring tools may favour male candidates due to past hiring patterns (Di Stasio & Larsen, 2020), while in healthcare, AI models trained primarily on male-centric data may fail to adequately diagnose or treat conditions that disproportionately affect women (Tan & Benos, 2025). These issues underscore the necessity of rigorous, intersectional conformity assessments (Di Stasio & Larsen, 2020; Tan & Benos, 2025) to ensure that AI systems do not reinforce existing inequalities but instead promote fair and equitable outcomes.

In this context, intersectional data analysis in AI conformity assessments is essential. Gender bias should not be examined in isolation; rather, assessments must account for the ways in which gender intersects with race, class, disability and other identity factors, ensuring that AI systems do not disproportionately harm marginalised communities (Nativi & Nigris, 2021). To achieve this, conformity assessments should be conducted by diverse teams that reflect a range of genders, races and social backgrounds. A more inclusive group of auditors enhances multi-perspective evaluation, reducing the risk of bias and increasing the fairness and accountability of AI systems (Henriksen, Enni & Bechmann, 2021). Moreover, these assessments should incorporate input from the communities most affected by AI technologies, including women of colour, women with disabilities and other underrepresented groups. Their lived experiences and expertise can help identify hidden biases that might otherwise go unnoticed. Furthermore, there is a pressing need for independent oversight bodies to ensure that AI conformity assessments are free from conflicts of interest and genuinely committed to addressing bias and harm (Calvi & Kotzinos, 2023). These bodies should be empowered to enforce compliance, set clear accountability standards and hold AI developers responsible for violations. By implementing robust, intersectional and community-informed oversight, AI conformity assessments can contribute to the development of fairer and more equitable AI systems that actively challenge – rather than reinforce – existing structural inequalities.

3.3. Feminist standards in AI standardisation process

Standardisation in the context of the AI Act (Articles 40 and 41 AI Act) refers to the creation of technical standards that AI systems must adhere to in order to meet regulatory requirements. These standards are typically developed by recognised European standardisation bodies, such as the European Committee for Standardisation (CEN),⁶ the European Committee for Electrotechnical Standardisation (CENELEC)⁷ and ETSI,⁸ often with input from the European Commission. They provide detailed guidelines for AI system design, risk management and performance metrics. Although these standards are not legally binding, compliance with them facilitates the conformity assessment process and aids companies in demonstrating their adherence to regulatory obligations, thus simplifying market access and ensuring alignment with the AI Act's provisions.

The AI standardisation process involves the creation of guidelines, technical specifications and best practices to ensure that AI systems are safe, reliable, transparent and ethically designed. Standardisation plays a crucial role in fostering innovation while minimising risks related to bias and discrimination as it is described in Article 40 and Recital 121 AI Act. Recital 121 AI Act highlights the role of standardisation in ensuring that high-risk AI systems comply with the requirements set out by the regulation. It emphasises the importance of creating harmonised standards⁹ across the European Union to promote consistent application of the AI Act's provisions. Various bodies like the European Standards Organisations, National Standards Bodies, European Stakeholder Organisations, Harmonised Standards Consultants and the European Commission are working on creating frameworks to regulate AI (Klumbyte, 2023). Among the standards having been set are human-centred AI, security and privacy, transparency, data governance, explainability and accountability.

From a feminist perspective, standardisation processes in AI can be viewed as a tool to ensure that AI systems do not inadvertently reinforce stereotypes or discriminatory practices, particularly against women and marginalised groups (Lütz, 2023). Feminists would argue that the development of technical standards by bodies such as CEN, CENELEC and ETSI should actively address issues like gender bias in AI algorithms, data collection and risk management practices. Furthermore, conformity assessments, based on the harmonised standards, should ensure that AI systems undergo rigorous scrutiny for fairness, inclusivity and accountability, particularly regarding the disproportionate impact that AI can have on women and other marginalised communities. By incorporating feminist principles into the standardisation process, like *intersectionality*, inclusivity, equity and participation, the AI Act could contribute to creating a more equitable AI ecosystem that actively works against systemic inequalities.

Feminist principles in AI standardisation emphasise the importance of diverse representation in the development and design of AI systems, ensuring that datasets reflect a wide range of populations, including women, LGBTQIA+ people and underrepresented communities, to prevent biases that perpetuate inequalities (Balahur et al., 2022). Feminist and anti-colonial theories offer a valuable framework for examining patriarchal dynamics, focusing on the power relations involved in data practices and advocating for self-determination and collective empowerment (Huang L, 2022). Feminist and anti-colonial theories offer a valuable framework for examining patriarchal dynamics, focusing on the power relations involved in data practices and advocating for self-determination and collective empowerment (Varon, 2021).

⁶See <https://www.cencenelec.eu/about-cen/>.

⁷See <https://www.cencenelec.eu/about-cenelec/>.

⁸See <https://www.etsi.org>.

⁹See Article 2(1), point (c), of Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R1025>.

Additionally, feminist approaches stress the need for bias mitigation and equity, requiring AI systems to undergo rigorous testing for gender, racial and socioeconomic biases in algorithms, data sets and outcomes (Szczerkocka, Tarnec & Pieczerek, 2022). In this context, the standardisation process should also promote accountability and transparency, ensuring clear documentation of how AI models are developed, data are collected and decisions are made, which allows for scrutiny and prevents unjust practices (Schwartz et al., 2022). Furthermore, intersectional feminist theory (Cooper, 1988; Crenshaw, 1991), particularly through the lens of *intersectionality*, highlights the importance of considering how multiple, overlapping identities, such as race, class, sexuality and disability, shape how AI systems affect individuals, advocating for standards that avoid exacerbating intersectional inequalities, such as differential treatment of women of colour compared to white women.

Feminist Science, Technology, and Society (STS) scholarship has been pivotal in shaping feminist AI ethics, particularly around the concept of accountability. From Donna Haraway's metaphor of the cat's cradle (Haraway, 2014) – emphasising the interconnectedness and situatedness of knowledge production – to Karen Barad's theory of agential realism (Murriss, 2022), feminist scholars have advocated for a critical examination of socio-technical systems (Drage, 2024). Accountability in this context refers to clearly defining the roles and responsibilities of every actor within the AI value chain and establishing mechanisms for control and oversight (Megarry, 2020). An accountable AI system requires clear identification of who is responsible in the event of a flawed design or malfunction.

To conclude, inclusive standardisation, which involves diverse stakeholders such as women of colour and other marginalised groups in the creation of AI guidelines, is crucial to ensuring that the perspectives of those most affected by AI technologies are taken into account. Gender-aware standards are also essential, as they should include specific measures to address gender bias and inequality, such as mandatory bias audits, the use of diverse datasets and ensuring that algorithms are explainable to impacted communities. However, there is a risk of tokenism (Yoder, 1991) – where the involved stakeholders may make only superficial efforts to appear inclusive, without making meaningful changes to achieve gender equity. This is connected to the fact that AI standardisation process remains largely dominated by powerful corporations and governments, which can hinder feminist efforts to promote true inclusivity and equity in the development and regulation of AI systems.

4. A feminist reading of the AI act – the post-release obligations of deployers

The AI Act outlines post-market oversight and corrective actions in the event that AI systems cause harm or fail to comply with regulatory standards. Deployers of a high-risk AI system must adhere to the obligations set forth in Article 26 AI Act, which require taking appropriate technical and organisational measures to ensure the system is used in accordance with the provided instructions, including monitoring the system's operation based on these instructions, informing the providers when necessary and cooperating with relevant national authorities regarding any actions they take in relation to the system to implement the AI Act. Additionally, they are responsible for regularly monitoring and updating robustness and cybersecurity measures, ensuring that input data are relevant and representative of the system's intended purpose. In cases where the system influences decision-making related to people – like hiring or education, they must inform individuals that they are subject to the system, explain its purpose and decision-making process and inform them of their right to an explanation (Hadfield & Clark, 2023). If the system's use could harm health, safety or rights, they must immediately notify the provider, distributor and relevant authorities, suspend the system's use and interrupt it if necessary.

A feminist interpretation of these obligations would advocate for a monitoring framework that is particularly attuned to the ways in which AI systems may disproportionately impact women, LGBTQIA+ people and marginalised communities, particularly in contexts such as hiring algorithms, healthcare diagnostics or law enforcement. The SyRI (Systematic Risk Identification Method) case in the Netherlands offers a significant lens through which to examine the *intersectionality* of

technology, law and social justice (van Bekkum & Borgesius, 2021). SyRI was an AI-driven system used by the Dutch government to predict and identify individuals at risk of committing fraud in social welfare programs. The case, however, became controversial and raised concerns about racial profiling, social exclusion and discrimination, particularly affecting marginalised communities. A feminist and intersectional analysis of this case reveals the ways in which technology-specifically predictive algorithms can perpetuate inequalities based on multiple axes of identity, such as race, class and gender (Bekker, 2021). The system's reliance on historical data meant that individuals from racially marginalised communities, particularly those of Moroccan or Turkish descent, were disproportionately affected by its predictions (van Bekkum & Borgesius, 2021). This raised concerns about racial profiling, where the system reinforced stereotypes and disproportionately targeted people based on their racial or ethnic background. In an intersectional sense, this bias was compounded by socio-economic factors, as people in lower income brackets, who are often racial minorities, were more likely to be flagged by SyRI for welfare fraud investigations (Bekker, 2021).

To this extent, a feminist reading emphasises the necessity of conducting impact assessments that examine how an AI system may affect different genders and whether it addresses the needs of marginalised groups. Under Article 26 of the AI Act, deployers are required to perform risk assessments both prior to and following deployment to ensure that AI systems do not cause harm. A feminist interpretation of this obligation calls for these risk assessments to be explicitly gender-aware. Deployers should assess whether their AI systems contribute to or exacerbate gender inequalities, ensuring that these systems are designed to promote gender justice. This includes addressing issues such as gender-based violence in generative AI technology (Karagianni, 2025), ensuring fairness in recruitment processes and preventing discriminatory practices in healthcare.

4.1. A gender-impact assessment under the fundamental rights impact assessment

Among the solutions proposed in the AI Act to safeguard fundamental rights at risk from high-risk AI systems are a Risk Management System (RMS), outlined in Article 9, and a Fundamental Rights Impact Assessment (FRIA), as stipulated in Article 27(1). While the introduction of the RMS and FRIA for high-risk AI systems represents a novel regulatory approach, the concepts of risk management and impact assessment are well-established in technology regulation. These mechanisms have historically emerged in response to the uncertainties associated with technological advancement across multiple fields (Demetzou, 2019a).

In essence, risk management is concerned with identifying and addressing risks, understood as potential negative events (Macenaite, 2017). By contrast, impact assessments evaluate both the positive and negative consequences of an initiative on societal concerns, such as fundamental rights, though they do not necessarily prescribe measures for addressing identified risks (Demetzou, 2019b; Macenaite, 2017). However, questions persist regarding their operationalisation in the AI context. For instance, what constitutes a risk to a fundamental right – such as gender equality and non-discrimination – remains open to multiple conceptualisations (Baldwin & Black, 2016; Golpayegani, Pandit & Lewis, 2023; Van Dijk, Gellert & Rommetveit, 2016). Similarly, measuring such risks is inherently subjective (Luhmann, 1991; Slupska, 2019) and can be influenced by gendered assumptions (European Institute for Gender Equality (EIGE), 2017; Stachowitsch & Sachseder, 2019). Yet, it is essential to consider the limitations of these approaches in achieving gender equality, particularly given the AI Act's normative framework, which reflects a narrow understanding of gender and prioritises product safety over broader fundamental rights protections (Veale & Zuiderveen Borgesius, 2021).

While the AI Act introduces important safeguards, it risks falling short in addressing gender-related harms due to its narrow focus on product safety and lack of a robust gender perspective. Embedding Gender Impact Assessment (GIA) into AI governance can help bridge this gap by ensuring AI systems are designed, assessed and deployed in a way that promotes gender equality

(Karagianni & Calvi, 2025). To effectively address gender-related biases in AI systems, a comprehensive approach is required. First, it is essential to detect and mitigate algorithmic biases that disproportionately disadvantage women and marginalised gender groups. This entails scrutinising training datasets, refining model architectures and implementing bias detection techniques to prevent the reinforcement of historical inequalities. Second, AI systems should be developed through a gender-equitable design process that actively integrates feminist and intersectional perspectives. This involves embedding gender-sensitive methodologies in AI development, ensuring that systems account for diverse experiences and do not perpetuate discriminatory outcomes. Third, participatory governance mechanisms should be established to enhance transparency and accountability in AI policy decisions (Taylor, Floridi & van der Sloot, 2017). In particular, the involvement of gender experts and affected communities is crucial to ensuring that AI governance frameworks reflect lived experiences and address structural inequalities. By incorporating these measures, AI regulation can move towards a more inclusive and equitable technological landscape. However, for GIA to be effective, it must be legally mandated, supported by comprehensive gender-disaggregated data and applied *intersectionally*.

4.2. Feminist critiques of GPAI systems

GPAI systems, such as large language models, foundation models and generative AI, are increasingly shaping decision-making in critical domains, from hiring and healthcare to law enforcement. However, feminist scholars critique these systems for reinforcing gendered, racialised and class-based inequalities while failing to ensure accountability for their societal harms. Article 51 AI Act enshrines obligations for deployers of GPAI – whether corporations, governments or institutions – to mitigate harm and promote justice-oriented AI governance.

GPAI systems learn from vast datasets that often reflect historical inequalities (Shrestha & Das, 2022). For instance, language models trained on internet data may internalise sexist stereotypes, like Google Translator – which is a narrow/specialised AI system – which translates the word “nurse” in English into Greek with a female pronoun, while the word “lawyer” or “engineer” with a male, replicating in this way the gender stereotypes. To this extent, an inclusive language in their code/programming language¹⁰ should take into account gender and demographic characteristics, which is highly needed in Natural Language Processes (Bozkurt, 2023; Foulidi, 2019; Weatherall, 2002).

In a complementary manner, Article 95 of the AI Act focuses on voluntary codes of conduct, urging the AI community to go beyond the regulatory requirements by adopting self-regulatory ethical standards. This article invites key stakeholders, including industry associations and organisations, to create voluntary codes of conduct that foster high standards of trustworthiness, transparency, fairness and respect for fundamental rights in AI systems (European Union, 2025). Although these codes are not legally binding, they offer a framework for establishing aspirational norms for AI developers and deployers, promoting ethical and responsible AI development practices.

Additionally, Recital 4 AI Act emphasises the necessity of a human-centric approach to AI development. It asserts that AI should be designed to enhance human capabilities and societal well-being. The recital underscores that diverse perspectives are essential for achieving this goal, as they contribute to the creation of AI systems that are more inclusive and considerate of the varied needs and experiences of individuals across different demographics. In these terms, Recital 27 AI Act highlights the importance of incorporating diverse datasets in the training of AI systems to mitigate the risk of bias. By ensuring that AI technologies are developed using data that reflect a wide range of experiences and perspectives, the recital advocates for a more equitable outcome in the applications of AI.

¹⁰ According to Georgallidou, Gasouka and Lambropoulou, language and how it refers to the entities of the world interact with how this world is perceived. See Foulidi X., “Gender in Sociolinguistics: A concise review on linguistic sexism,” *International Journal of Multidisciplinary Research and Analysis*, 2019. See also A. Weatherall, *Gender, Language and Discourse*, London: Routledge, 2002.

This commitment to diversity is seen as essential for fostering fairness and avoiding discriminatory practices. Both Recitals 80 and 165 AI Act advocate for AI systems to respect human dignity and promote individual autonomy and equality. By fostering a human-centric approach that prioritises inclusivity, these recitals aim to prevent biased outcomes that can arise from inadequate consideration of diversity in AI design and implementation.

The Act mandates ongoing monitoring to detect evolving biases, a crucial step in mitigating algorithmic discrimination. However, its reliance on self-regulation assumes that deployers will voluntarily report biases, despite strong incentives to do otherwise. This is particularly problematic given that gender bias in AI disproportionately harms marginalised communities, who often lack institutional power to demand accountability. Furthermore, the Act lacks robust redress mechanisms, offering no clear pathways for individuals affected by algorithmic discrimination – such as hiring AI systems that disproportionately reject women – to seek justice. To address these gaps, feminist scholars advocate for the establishment of independent AI auditing bodies with expertise in gender and racial justice, alongside strengthened complaint mechanisms that empower affected users to challenge biased AI decisions effectively (O’Neil, Sargeant & Appel, 2024).

5. Concluding remarks

The AI Act, while a significant step towards regulating high-risk AI systems, falls short in addressing gendered biases and the deeper social and structural inequalities embedded in AI technologies, as was extensively explained above. Although the AI Act acknowledges the importance of non-discrimination, it lacks a comprehensive gender-sensitive approach, particularly regarding gender inclusivity for marginalised groups such as transgender, non-binary and intersex individuals. A feminist and intersectional analysis reveals that the AI Act treats gender bias primarily as a technical issue, rather than recognising it as a systemic challenge rooted in historical power imbalances, while it perpetuates a binary distinction of gender.

Moreover, the Act’s limited provisions on gender-related protections, such as the exclusion of gender from the list of sensitive data categories and its failure to mandate intersectional gender audits, highlight the need for a more inclusive and robust regulatory framework. To truly address the risks and harms posed by AI, particularly in high-risk domains like recruitment, healthcare and generative AI, the AI Act should integrate feminist legal principles that prioritise gender equality, accountability, *intersectionality* and the dismantling of structural biases. Without such critical interventions, the AI Act risks reinforcing existing inequalities rather than mitigating them, ultimately leaving marginalised communities vulnerable to the discriminatory impacts of AI technologies.

AI Act presents a regulatory framework aimed at ensuring the safety, transparency and accountability of AI systems, with a particular focus on non-discrimination and mitigation of bias. The harmonisation process is central to this effort, providing a unified approach across Member States while recognising the importance of intersectionality is missing. A feminist perspective highlights the need for a stronger intersectional approach, addressing not only gender equality but also accounting for race, class, disability and other social factors that influence individuals’ experiences within AI. Ensuring that the AI Act aligns with the principles of gender equality and human rights requires a careful, critical examination of its various processes, from conformity assessments to standardisation.

Conformity assessments, while essential in guaranteeing compliance with the AI Act, must go beyond traditional evaluations to include a gender-sensitive and intersectional lens. This ensures that AI systems do not perpetuate existing biases or exacerbate inequalities. The emphasis on the inclusion of diverse voices and perspectives, especially those of marginalised groups, is crucial in making AI systems truly fair and equitable. Standardisation processes, when infused with feminist principles, can significantly contribute to the creation of AI systems that are not only technically compliant but also socially responsible, addressing gendered harms and promoting inclusivity.

Ultimately, the AI Act has the potential to promote a fairer digital future, but this depends on the continuous and active involvement of diverse stakeholders, particularly marginalised communities, in shaping AI development and regulation. By embedding feminist principles – such as inclusivity, accountability and *intersectionality* – into the core of AI governance, the EU can pave the way for AI technologies that serve the interests of all, rather than reinforcing existing power structures and inequalities. While this is mostly for the safeguards and oversight mechanisms adopted for high-risk AI systems, the AI Act risks overlooking the gendered and intersectional impacts of these technologies. A feminist and intersectional approach to AI regulation is essential to ensure that AI systems do not perpetuate existing inequalities, especially in sensitive areas like hiring, healthcare and law enforcement. This requires incorporating gender-aware risk assessments, embedding GIA and promoting inclusive and participatory design processes. Additionally, strengthening accountability through independent auditing bodies and enhancing redress mechanisms will help ensure that AI systems are not only safe and effective but also fair and just for marginalised communities. By integrating these measures, the AI Act can move towards a more inclusive and equitable regulatory framework that upholds the dignity, autonomy and rights of all individuals, particularly those most vulnerable to the harms of biased AI systems.

Funding statement. This research was supported by FARI-AI for common good.

Competing interests. None.

References

- Ahmed, S. (1996). Moving spaces: Black feminism and post-colonial theory. *Theory, Culture & Society*, 13(1), 139–146.
- Ajunwa, I. (2019). The paradox of automation as anti-bias intervention. *Cardozo Law Review*, 41, 1671.
- Anagnostou, D., & Millns, S. (2013). Gender equality, legal mobilization, and feminism in a multilevel European system. *Canadian Journal of Law and Society/La Revue Canadienne Droit Et Société*, 28(2), 115–131.
- Andrews, L., & Bucher, H. (2022). Automating discrimination: AI hiring practices and gender inequality. *Cardozo Law Review*, 44, 145.
- Balahur, A., Jenet, A., Hupont, I. T., Charisi, V., Ganesh, A., Griesinger, C. B., & Tolan, S. (2022). Data quality requirements for inclusive, non-biased and trustworthy AI.
- Baldwin, R., & Black, J. (2016). Driving priorities in risk-based regulation: What's the problem? *Journal of Law and Society*, 43(4), 565–595. <https://doi.org/10.1111/jols.12003>.
- Bekker, S. (2021). Fundamental rights in digital welfare states: The case of SyRI in the Netherlands. In O. Spijkers, W. G. Werner, & R. A. Wessel (Eds.), *Netherlands yearbook of international law 2019. Netherlands yearbook of international law* (Vol. 50). T.M.C. Asser Press, The Hague.
- Bird-Pollan, S. (2020). The place of the unconscious in critiques of systematic prejudice: Lessons from MacKinnon and Critical Race Theory. *The Philosophical Forum*, 51(4), 377–398.
- Biswas, S., Jung, J. Y., Unnam, A., Yadav, K., Gupta, S., & Gadiraju, U. (2024, October). “Hi. I’m Molly, Your Virtual Interviewer!” Exploring the impact of race and gender in AI-powered virtual interview experiences. In *Proceedings of the AAAI Conference on Human Computation and Crowdsourcing* (Vol. 12, pp. 12–22).
- Bozkurt, A. (2023). Biased binaries. *Post Digital Science and Education*, 5(3), 544–546.
- Butler, J. (1990). *Gender trouble: Feminism and the subversion of identity*. Routledge, New York.
- Butler, J. (2024). *Who's afraid of gender?* Knopf Canada, New York.
- Calvi, A., & Kotzinos, D. (2023, June). Enhancing AI fairness through impact assessment in the European Union: A legal and computer science perspective. In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency* (pp. 1229–1245).
- Cooper, A. J. (1988). *A voice from the South*. Oxford University Press, New York.
- Costanza-Chock, S. (2020). *Design justice: Community-led practices to build the worlds we need*. The MIT Press, Cambridge, Massachusetts, London, England.
- Crenshaw, K. (1991). Mapping the margins: Intersectionality, identity politics, and violence against women of color. *Stanford Law Review*, 43(6), 1241–1299.
- Delmar, R. (2018). What is feminism? In *Theorizing feminism* (pp. 5–28). Routledge, London.
- Demetzou, K. (2019a). GDPR and the concept of risk: The role of risk, the scope of risk and the technology involved. In E. Kosta (Ed.), *Privacy and identity* (pp. 137–154). Springer International Publishing. https://doi.org/10.1007/978-3-030-16744-8_10

- Demetzou, K.** (2019b). Data protection impact assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 35(6), 105342. <https://doi.org/10.1016/j.clsr.2019.105342>.
- de Sousa Santos, B.** (2024). AI and the epistemologies of the South. *Journal of World-Systems Research*, 30(2), 635–645.
- D'Ignazio, C.** (2020). *Data feminism*. The MIT Press, Cambridge, Massachusetts, London, England.
- Di Stasio, V., & Larsen, E. N.** (2020). The racialized and gendered workplace: Applying an intersectional lens to a field experiment on hiring discrimination in five European labor markets. *Social Psychology Quarterly*, 83(3), 229–250.
- Doh, M., Canali, C., & Karagianni, A.** (2024). Pixels of perfection and self-perception: Deconstructing AR beauty filters and their challenge to unbiased body image. In *Proceedings of the 2024 ACM International Conference on Interactive Media Experiences (IMX '24)*. Association for Computing Machinery (pp. 349–353). New York, NY, USA. <https://doi.org/10.1145/3639701.3663636>.
- Drage, E.** (2024). Engineers on responsibility: Feminist approaches to who's responsible for ethical AI, *Ethics and Information Technology*, 26.
- European Commission.** (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>, accessed 14 May 2025.
- European Commission.** (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)*. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>, accessed 14 May 2025.
- European Data Protection Supervisor (EDPS) & European Data Protection Board (EDPB).** (2021). *Joint opinion 5/2021 on the European Commission's proposal for a regulation on artificial intelligence (AI)*. https://edpb.europa.eu/sites/default/files/files/file1/edpb-joint-opinion_5_2021_on_the_european_commissions_proposal_for_a_regulation_on_ai_en.pdf, accessed 14 May 2025.
- European Institute for Gender Equality (EIGE).** (2017). *Gender Impact Assessment. Gender Mainstreaming Toolkit*. Retrieved from <https://eige.europa.eu/publications/gender-impact-assessment-gender-mainstreaming-toolkit>, accessed 14 May 2025.
- European Parliament and Council.** (2024). *Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence*. Official Journal of the European Union, accessed 14 May 2025.
- European Parliament & Council of the European Union.** (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Official Journal of the European Union, L 119, 1–88. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>, accessed 14 May 2025.
- European Parliament & Council of the European Union.** (2022a). *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services (Digital Services Act) and amending Directive 2000/31/EC [Digital Services Act]*. Official Journal of the European Union, L 277, 1–101. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065>, accessed 14 May 2025.
- European Parliament & Council of the European Union.** (2022b). *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 23 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act)*. Official Journal of the European Union, L 265, 1–30. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925>, accessed 14 May 2025.
- European Union,** Charter of Fundamental Rights of the European Union (2000/C 364/01).
- European Union.** (2025). First draft general-purpose AI code of practice. <https://digital-strategy.ec.europa.eu/en/library/first-draft-general-purpose-ai-code-practice-published-written-independent-experts>, accessed 14 May 2025.
- Foulidi, X.** (2019). Gender in sociolinguistics: A concise review on linguistic sexism. *International Journal of Multidisciplinary Research and Analysis*.
- Fricker, M.** (2007). Hermeneutical injustice, epistemic injustice: Power and the ethics of knowing. Oxford Academic. <https://doi.org/10.1093/acprof:oso/9780198237907.003.0008>, accessed 3 March 2025.
- Frischhut, M.** (2022). General introduction (De Lege Lata). *The ethical spirit of EU values*. Cham: Springer. https://doi.org/10.1007/978-3-031-12714-4_2.
- Galli, F., & Novelli, C.** (2024). The many meanings of vulnerability in the AI Act and the one missing. Available at SSRN.
- Golpayegani, D., Pandit, H., & Lewis, D.** (2023). To be high-risk, or not to be—Semantic specifications and implications of the AI act's high-risk AI applications and harmonised standards. In *ACM Conference on Fairness, Accountability, and Transparency* (pp. 905–915). <https://doi.org/10.1145/3593013.3594050>.
- Guyan, K.** (2022). *Queer data*. Bloomsbury Publishing, London.
- Hadfield, G. K., & Clark, J.** (2023). Regulatory markets: The future of AI governance. *arXiv preprint arXiv:2304.04914*.

- Halberstam, J.** (1991). Automating gender: Postmodern feminism in the age of the intelligent machine. *Feminist Studies*, 17(3), 439–460.
- Haraway, D.** (2014). Chapter 27 – Situated knowledges: The science question in feminism and the privilege of partial perspective. In *Women, science, and technology: A reader in feminist science studies*. Routledge.
- Henriksen, A., Enni, S., & Bechmann, A.** (2021, July). Situated accountability: Ethical principles, certification standards, and explanation methods in applied AI. In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 574–585).
- Hill Collins, P.** (2009). *Black feminist thought: Knowledge, consciousness, and the politics of empowerment*. Routledge, New York and London.
- Holliday, C.** (2021). Rewriting the stars: Surface tensions and gender troubles in the online media production of digital deepfakes. *Convergence*, 27(4), 899–918.
- Huang L, T.-L.** (2022). Ameliorating algorithmic bias, or why explainable AI needs feminist philosophy. *Feminism, social justice, and artificial intelligence*, 8, 3–4.
- Karagianni, A.** (2025). *Shadows of selfies: How generative AI fuels GBV – An analysis of non-consensual sexualised deepfakes through abolitionism and intersectionality*. IFIP Summer School: Springer Publications.
- Karagianni, A., & Calvi, A.** (2025). Exploring gender dimensions in high-risk AI systems: Moving towards a Gender Impact Assessment within the EU AI Act. In *Privacy Law Scholars Conference 2025*.
- Karagianni, A., & Doh, M.** (2024). A feminist legal analysis of non-consensual sexualized deepfakes: Contextualizing its impact as AI-generated image-based violence under EU law. *Porn Studies*, 1–18. <https://doi.org/10.1080/23268743.2024.2408277>
- Keyes, O.** (2018). The misgendering machines: Trans/HCI implications of automatic gender recognition. *Proceedings of the ACM on Human-computer Interaction*, 2(CSCW), 1–22.
- Klamert, M.** (2015). What we talk about when we talk about harmonisation. *Cambridge yearbook of European legal studies*, 17, 360–379.
- Klumblyte, G.** (2023). Towards feminist intersectional XAI: From explainability to response-ability. *arXiv Cornell University*, 9.
- Kobayashi, K., & Nakao, Y.** (2020). One-vs.-one mitigation of intersectional bias: A general method to extend fairness-aware binary classification. *arXiv preprint* 2010.13494. <https://arxiv.org/abs/2010.13494>
- Levine, P.** (2008). States of undress: Nakedness and the colonial imagination. *Victorian Studies*, 50(2), 189–219.
- Lewis, S.** (2025). *Enemy feminisms – TERFs, policewomen, and girlbosses against liberation*. Haymarket Books, Chicago.
- Longo, M.** (2023). “Vulnerability. From the paradigmatic subject to a new paradigm of the human condition? An introduction. *International Journal for the Semiotics of Law – Revue Internationale de Sémiotique Juridique*, 36, 1359–1369.
- Luhmann, N.** (1991). *Risk: A sociological theory*. <https://doi.org/10.5860/choice.31-2392>
- Lütz, F.** (2023). Gender equality and algorithmic discrimination: The contribution of the EU standardisation request on AI. *Ex/ante*, 2023(2), 4–15.
- Macenaite, M.** (2017). The “riskification” of European data protection law through a two-fold shift. *European Journal of Risk Regulation*, 8(3), 506–540.
- MacKinnon, C. A.** (2013). From practice to theory, or what is a white woman anyway? In *Feminist legal theories* (pp. 191–200). Routledge, Michigan.
- Magee, L., Ghahremanlou, L., Soldatic, K., & Robertson, S.** (2021). Intersectional bias in causal language models. *arXiv preprint* 2107.07691. <https://arxiv.org/abs/2107.07691>
- Malgieri, G., & Fuster, G. G.** (2022). The vulnerable data subject: A gendered data subject? *European Journal of Law and Technology*, 13(2).
- Megarry, J.** (2020). ‘It doesn’t feel as transparent and accountable’: Social media and feminist ethics. *The Limitations of Social Media Feminism*, 229–279.
- Mignolo, W.** (2012). Decolonizing western epistemology/building decolonial epistemologies. *Decolonizing Epistemologies: Latina/o Theology and Philosophy*, 19–43.
- Murris, K.** (2022). *In conversation with Karen Barad: Doings of agential realism*. Taylor & Francis.
- Nativi, S., & Nigris, D.** (2021). AI watch: AI standardisation landscape. *European Commission*
- O’Connor, S., & Liu, H.** (2024). Gender bias perpetuation and mitigation in AI technologies: Challenges and opportunities. *AI and Society*, 39(4), 2045–2057.
- O’Neil, C., Sargeant, H., & Appel, J.** (2024). Explainable fairness in regulatory algorithmic auditing. *West Virginia Law Review*, 127, 79.
- Praveen Kumar, E.** (2022). A review on vulnerabilities to modern processors and its mitigation for various variants. *Procedia Computer Science*, 215, 91–97.
- Quijano, A.** (2000). Coloniality of power and eurocentrism in Latin America. *International Sociology*, 15(2), 215–232. <https://doi.org/10.1177/0268580900015002005>
- Rachel, A.** (2021, April). Can artificial intelligence be decolonized? *Interdisciplinary Science Reviews*, 46, 176–197.
- Rafanelli, L. M.** (2022). Justice, injustice, and artificial intelligence: Lessons from political theory and philosophy. *Big Data and Society*, 9(1), 20539517221080676.

- Ricaurte, P., & Zasso, M. (2023). AI, ethics and coloniality: A feminist critique. In M. Cebal-Loureda (Ed.), *What AI can do*. Milton Park (pp. 53–72).
- Rigotti, C., & McGlynn, C. (2022). Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission's proposal to criminalise image-based sexual abuse. *New Journal of European Criminal Law*, 13(4), 452–477.
- Salzberg, D. A. G. (2019). *Sexuality and transsexuality under the European Convention on Human Rights: A queer reading of human rights law*. Bloomsbury Publishing, Sheffield, UK.
- Schwartz, R., Schwartz, R., Vassilev, A., Greene, K., Perine, L., Burt, A., & Hall, P. (2022). *Towards a standard for identifying and managing bias in artificial intelligence* (Vol. 3, pp. 00). Gaithersburg, MD: US Department of Commerce, National Institute of Standards and Technology.
- Scientific Research Committee-European Parliament. (2024). Artificial intelligence act. European parliament. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI\(2021\)698792_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf), accessed 14 May 2025.
- Scientific Research Committee of the European Parliament. (2025). Algorithmic discrimination under the AI Act and the GDPR. European Parliament. [https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/769509/EPRS_ATA\(2025\)769509_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/769509/EPRS_ATA(2025)769509_EN.pdf), accessed 14 May 2025.
- Shakir, M. (2020). *Decolonial AI: Decolonial theory as sociotechnical foresight in artificial intelligence*. Philosophy & Technology Springer. 659–684.
- Shrestha, S., & Das, S. (2022). Exploring gender biases in ML and AI academic research through systematic literature review. *Frontiers in Artificial Intelligence*, 5, 976838.
- Siapera, E. (2022). AI content moderation, racism and (de)coloniality. *International Journal of Bullying Prevention*, 55–65.
- Sinders, C. (2020). Feminist data set. *Clinic for Open Source Arts*. <https://carolinesinders.com/wp-content/uploads/2020/05/Feminist-Data-Set-Final-Draft-2020-0517.pdf>, accessed 14 May 2025.
- Slupska, J. (2019). Safe at home: Towards a feminist critique of cybersecurity. *St Antony's International Review*, 15(1), 83–100.
- Sovacool, B., Furszyfer-Del Rio, D. D., & Martiskainen, M. (2021). Can prosuming become perilous? Exploring systems of control and domestic abuse in the smart homes of the future. *Frontiers in Energy Research*, 9, 765817.
- Stachowitsch, S., & Sachseder, J. (2019). The gendered and racialized politics of risk analysis. The case of Frontex. *Critical Studies on Security*, 7(2), 107–123. <https://doi.org/10.1080/21624887.2019.1644050>.
- Stierle, M. (2021). A de lege ferenda perspective on artificial intelligence systems designated as inventors in the European Patent System. *GRUR International*, 70(2), 115–133.
- Stolton, S. (2020). Poland rejects presidency conclusions on artificial intelligence, rights. Euractiv. <https://www.euractiv.com/section/digital/news/poland-rejects-presidency-conclusions-on-artificial-intelligence-rights/>, accessed 14 May 2025.
- Szczekocka, E., Tarnec, C., & Pieczera, J. (2022, December). Standardization on bias in artificial intelligence as industry support. In *2022 IEEE International Conference on Big Data (Big Data)* (pp. 5090–5099). IEEE.
- Tan, M. J. T., & Benos, P. V. (2025). Addressing intersectionality, explainability, and ethics in AI-driven diagnostics: A rebuttal and call for transdisciplinary action. *arXiv preprint* 2501.08497. <https://arxiv.org/abs/2501.08497>
- Taylor, E. T., & Bryson, M. K. (2016). Cancer's margins: Trans* and gender nonconforming people's access to knowledge, experiences of cancer health, and decision-making. *LGBT Health*, 3(1), 79–89.
- Taylor, L., Floridi, L., & van der Sloot, B. (2017). *Group privacy: New challenges of data technologies*. Dordrecht: Springer.
- Tzimas, T. (2021). *Legal and ethical challenges of artificial intelligence from an international law perspective* (Vol. 46). Springer Nature.
- van Bekkum, M., & Borgesius, F. Z. (2021). Digital welfare fraud detection and the Dutch SyRI judgment. *European Journal of Social Security*, 23(4), 323–340. <https://doi.org/10.1177/13882627211031257>
- Van Dijk, N., Gellert, R., & Rommetveit, K. (2016). A risk to a right? Beyond data protection risk assessments. *Computer Law & Security Review*, 32(2), 286–306. <https://doi.org/10.1016/j.clsr.2015.12.017>.
- Varon, J. (2021). Artificial intelligence and consent: A feminist anti-colonial critique. *Internet Policy Review*, 10(4).
- Veale, M., & Zuiderveen Borgesius, F. (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. <https://doi.org/10.9785/crl-2021-220402>.
- Weatherall, A. (2002). *Gender, language and discourse*. London: Routledge.
- Xenidis, R. (2018). *Multiple discrimination in EU anti-discrimination law: Towards redressing complex inequality? In EU anti-discrimination law beyond gender*. Oxford: European University Institute.
- Yoder, J. D. (1991). Rethinking tokenism: Looking beyond numbers. *Gender and Society*, 5(2), 178–192.

Anastasia Karagianni is a Doctoral Researcher at the Law Science Technology and Society (LSTS) research group of the Law and Criminology Faculty of Vrije Universiteit Brussels (VUB) and former FARI Scholar. Her academic background is mainly based on International and European Human Rights Law, as she holds an LL.M. from the Department of International Studies of Aristotle University of Thessaloniki. During her Master's studies, she was an exchange student for one year at the Faculty of International Law at KU Leuven. She has been also a Visiting Researcher at the iCourts research team of the University of

Copenhagen. Her thesis is titled “Divergencies of Gender Discrimination in the EU AI Act Through Feminist Epistemologies and Epistemic Controversies.”

Besides her academic interests, Anastasia is a digital rights activist, since she is a co-founder of DATAWO, a civil society organisation based in Greece advocating on gender equality in the digital era, and founder of @femme_group_BrusselsGR. Anastasia Karagianni was MozFest Ambassador 2023 and Mozilla Awardee for the project “A Feminist Dictionary in AI” – of the Trustworthy Artificial Intelligence working group.