The Intersection of Artificial Intelligence and Employment Legal Relations: Balacing Employer Interests with Fundamental Rights in AI-Driven Employment Practices

Agnese Reine
Faculty of Social Sciences
Riga Stradiņš university
Riga, Latvia
agnese.reine@rsu.lv

***Abstract*— In the era of rapid technological advancement, artificial intelligence (hereinafter "AI") has profoundly transformed various sectors, notably employment. The integration of AI in employment practices represents a significant paradigm shift, enhancing efficiencies but also introducing substantial challenges. This integration poses complex legal issues, particularly in balancing employer interests with employees' fundamental rights, in particular to privacy. As of August 1, 2024, the European Artificial Intelligence Act (hereinafter "AI Act") was enacted. This legislation introduces a risk-based framework that mandates specific responsibilities for both providers and deployers of AI systems. Within the context of employment legal relationships and the integration of various AI systems therein, it is crucial to conduct a thorough analysis of the interplay between the General Data Protection Regulation and the stipulations of the AI Act. This article examines the legal frameworks that regulate rights to privacy and AI-driven employment practices, emphasizing the imperative to reconcile employer objectives—such as productivity and cost-efficiency—with employees' rights to privacy, non-discrimination, and equitable treatment. Through a detailed comparative analysis of extant legislation and case law, this study identifies deficiencies in current legal protections and advocates for a framework that ensures AI systems in employment conform to fairness and human rights principles. The article argues for a proactive legislative approach that not only addresses current challenges but also anticipates future ethical and legal issues arising from advancements in AI technology.**

Keywords*— *Artificial Intelligence, Business Objectives in Employment, Non-discrimination, Rights to Privacy

I. Introduction

In the century marked by rapid technological development, AI has assumed a significant role. Every day, the use of AI significantly increases across various sectors, including employment, providing opportunities to enhance employee efficiency, facilitate daily tasks, and monitor task performance etc. The use of AI must be analyzed in connection with its potential impacts on individuals, in particular in ensuring protection of privacy.

The European Council of October 2017 stated that to successfully build a Digital Europe, the EU needs in particular: [..] a sense of urgency to address emerging trends: this includes issues such as artificial intelligence and blockchain technologies, while at the same time ensuring a high level of data protection, digital rights and ethical standards. Also, the European Council invited the Commission to put forward a "European approach to artificial intelligence"[1]. Following this, European Commision stated: "The EU's approach to artificial intelligence centers on excellence and trust, aiming to boost research and industrial capacity while ensuring safety and fundamental rights. The way we approach AI will define the world we live in the future. To help build a resilient Europe for the Digital Decade, people and businesses should be able to enjoy the benefits of AI while feeling safe and protected [2]." Therefore, it is clearly stated, that artificial intelligence solutions should be implemented and used in processes around different areas, however it should be managed in a way, that ensures fundamental rights and freedoms.

The aim of this article is to analyze the interaction between legal framework of employment, artificial

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol2.8571

intelligence and privacy protection, define the impact on the provision of fundamental rights and suggestions how to ensure balance between employers interests and employees rights to privacy in the rapid development of the artificial intelligence.

II. Materials and methods

This article utilizes interdisciplinary methods, such as analytical, descriptive, deductive and inductive methods, as well as following interpretative methods of legal acts: grammatical, historical, systemic, teleological. The mentioned methods will be used to analyse the legal regulations of employment relations and artificial intelligence, case law, scientific and other sources, to identify issues and their impact on the protection of fundamental rights.

III. Results and Discussions

As of August 1, 2024, the European AI Act was enacted. This legislation introduces a risk-based framework that mandates specific responsibilities for both providers and users of AI systems, which are tailored according to the risk level associated with their deployment. Recital 1 of the AI Act states: “The purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of AI systems in the Union, in accordance with Union values, to promote the uptake of human centric and trustworthy AI while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (the ‘Charter’)[..] [3].” Also recital 2 states: “This Regulation should be applied in accordance with the values of the Union enshrined as in the Charter, facilitating the protection of natural persons, undertakings, democracy, the rule of law and environmental protection, while boosting innovation and employment and making the Union a leader in the uptake of trustworthy AI [3].” Thus, the above clearly points to the main EU objective, i.e., boost innovation and employment while ensuring the fundamental rights and freedoms established in the Charter of Fundamental Rights of the European Union (hereinafter “the Charter”). Article 7 “Respect for private and family life” of the Charter states, that everyone has the right to respect for his or her private and family life, home and communications and Article 8 “Protection of personal data “ states, that everyone has the right to the protection of personal data concerning him or her [4]. Therefore, the Charter states, that protection of privacy inlcuding data protection is one of the fundamental rights of individuals. Taking into account what is stated in Recitals 1 and 2 of the AI Act, it is clear that the implementation and use of AI must be aligned with the protection of fundamental rights, particularly data protection.

In addition to the previously mentioned scope of the Charter, it's also worth mentioning the European Convention on Human Rights, which in Article 8 stipulates the right to respect for private life[5]. In interpreting this Article 8 of the European Convention on Human Rights, the European Court of Human Rights (hereinafter “ECtHR”) has recognized that the concept of "private life" has a broad scope. The acquisition and storage of personal data fall within the ambit of the right to respect for private life. In analyzing the interplay between employment legal relations and personal data protection, it should be noted that as early as December 16, 1992, in the case of “Niemietz v. Germany”, the ECtHR clarified that it would be overly restrictive to apply the concept of private life only to the "inner circle" in which an individual can live his personal life as he chooses, and to completely exclude the outside world, which does not fall within this circle. Respect for private life also includes the rights to a certain extent to form and develop relationships with other people. Moreover, it seems there is no fundamental reason why this understanding of "private life" should exclude professional or business activities, as it is precisely in work life that most people have significant, if not the greatest, opportunities to develop relationships with the outside world. This observation by the ECtHR indicates a broad interpretation of the concept of private life, including its applicability to employment legal relations[6]. The regulation of personal data protection has evolved over the years into what is now known as the General Data Protection Regulation (hereinafter "GDPR").

Thus, the use of AI systems must be interpreted in conjunction with the GDPR [7], which has been applicable since May 25, 2018, regulating aspects of personal data protection in the EU.

Furthermore, it is necessary to analyze requirements set out in the AI Act and GDPR and assess their impact to the employment legal relationship.

The use of AI systems in recruitment and already established employment legal relationship, offers a significant opportunity to enhance employee performance, improve overall company performance and efficiency, and simplify and streamline various processes. Such use of AI is also in line with the EU's aforementioned position on AI development. However, it is essential to analyze, the risks associated with the use of AI systems in employment legal relationship, particulartly focusing on data protection as one of the fundamental rights, as well as analyze how to ensure a balance between the employer's interests and the employee's right to privacy.

Initially, it is essential to analyze the requirements governing the use of AI systems in employment relationships and subsequently examine these conditions in the context of GDPR compliance.

According to the Article 6 (2) of the AI Act and respective Annex III (4): “(a) AI systems intended to be used for the recruitment or selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates; (b) AI systems intended to be used to make decisions affecting terms of work-related relationships, the promotion or termination of work-related contractual relationships, to allocate tasks based on individual behaviour or personal traits or characteristics or to monitor and evaluate the performance and behaviour of persons in such relationships [3]", are considered as high-risk AI systems. Also Recital 57 of the AI Act explains, that: "AI systems used in employment, workers management and access to self-employment, in particular for the recruitment and selection of persons, for making decisions affecting terms of the work-related relationship, promotion and termination of work-related contractual relationships, for allocating tasks on the basis of individual behaviour, personal traits or characteristics and for monitoring or evaluation of persons in work-related contractual relationships, should also be classified as high-risk, since those systems may have an appreciable impact on future career prospects, livelihoods of those persons and workers' rights [3]. Therefore, in scope of this article, risks will be analyzed from the high-risk AI system perspective.

This article analyzes the use of AI systems, therefore the analyses is made from the *'deployer'* perspective in scope of definitions set out in the AI Act, i.e., from the perspective of the employer who uses AI systems under its authority. Requuirements towards the 'providers' are set out in the Section 2 of the Ai Act.

Article 26 of the AI Act sets out the obligations of deployers of high-risk AI systems, i.e. sets the requirements for the users of the AI systems. Deployers of high-risk AI systems shall 1) take appropriate technical and organisational measures to ensure they use such systems in accordance with the instructions for use accompanying the systems; 2) ensure that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system; 3) keep the logs automatically generated by that high-risk AI system to the extent such logs are under their control; 4) monitor the operation of the high-risk AI system on the basis of the instructions for use and, where relevant, inform providers (icl. In case of a high risk identified, incident and other situations defined in Article 16 (5)) [3]. Also, obligations include specific requirements towards the emploers, stating, that before putting into service or using a high-risk AI system at the workplace, deployers who are employers shall inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system. Also Article 26 (11) states, that deployers of high-risk AI systems referred to in Annex III that make decisions or assist in making decisions related to natural persons shall inform the natural persons that they are subject to the use of the high-risk AI system [3]. Thus, this requirement is relevant for AI systems used in recruitment and employment as it is stated in Annex III of the AI Act.

In addition to the aforementioned obligations, Article 27 of the AI Act requires deployer to do the Fundamentas rights impact assessment for high-risk AI systems.

The aim of the fundamental rights impact assessment is for the deployer to identify the specific risks to the rights of individuals or groups of individuals likely to be affected, identify measures to be taken in the case of a materialisation of those risks [3].

However these requirements are not applicable to all high-risk AI systems, but only to those specified in Article 27 (1) of AI Act [3], that does not include high-risk employment, workers' management and access to self-employment systems. Respectively, if AI systems are used in recruitment or employment relationships, there is no requirement to conduct a Fundamental Rights Impact Assessment. However, it is important to note that according to the AI Act, EU member states are allowed to impose stricter requirements through national laws related to the governance of high-risk AI systems, therefore, the regulatory framework may differ in each EU country.

When analyzing high-risk AI systems in scope of employment, it is important to remember, that it is acknowledged that the employee is in a position of subordination to the employer, therefore, the incorrect use of AI systems can have significant consequences for the employee. Considering that an employee in a less protected position may not be able to fully defend their rights, there is a substantial risk that the employee's fundamental rights could be compromised. Therefore, it is crucial to conduct a thorough risk assessment of AI systems used in recruitment and employment to ensure compliance with fundamental rights such as data protection. While a Fundamental Rights Impact Assessment is not mandatory unless specified by national laws, all requisite measures related to the processing of personal data, such as the Data Protection Impact Assessment (DPIA), must be adhered to. Even though the Data Protection Impact Assessment (DPIA) is broadly focused on assessing all potential impacts on data subjects, it is the author's opinion that with the implementation of AI systems in daily operations, the DPIA should also be further developed to specifically address and assess the detailed risks of infringing fundamental rights.

Continuing to analyze the risks associated with the use of AI, particularly in ensuring the protection of personal data, this article will examine some of the most significant risk factors.

A significant amount of personal data is processed even before an employment legal relationship is established, notably during the recruitment process. With the advancement of AI technologies, companies are seeking to make recruitment more efficient and are therefore eager to exploit the opportunities provided by AI systems. Recruitment is a complex process that demands significant time and effort to evaluate and select the most suitable candidate for a position. Employers are keen on streamlining this process to make it as quick and efficient as possible, thereby conserving the resources of HR personnel.

Artificial Intelligence (AI) significantly enhances recruitment efficiency by automating routine tasks, including screening resumes, parsing extensive data sets, and conducting preliminary candidate assessments. These systems are adept at analyzing large volumes of data to identify optimal candidates for specific roles. More than merely evaluating skills and experiences listed on resumes, AI can infer potential cultural fit by analyzing various data points that might be overlooked by human recruiters. Additionally, AI leverages historical data to predict outcomes such as job performance and candidate-job fit, offering a predictive approach to hiring decisions. AI systems also excel in managing large volumes of applications, which enables large organizations to scale their recruitment efforts effectively without the need for additional human resources. Furthermore, AI-driven chatbots and automated systems are able enhance the candidate experience by providing timely updates, feedback, and guidance throughout the recruitment process. These capabilities demonstrate AI's pivotal role in transforming recruitment processes, and explains the interests of the employer in using this kind of systems, however it is crucial to evaluate possibilities provided by the AI recruitment systems versus the GDPR requirements. The benefits of AI in recruitment, as outlined above, are indeed attractive to many company managements seeking efficiency and scalability. However, the implementation of these AI systems must be navigated carefully due to strict data protection regulations, notably the GDPR. GDPR imposes several key requirements that could limit the use of AI.

When analyzing the utilization of AI systems in established employment legal relationships, several objectives for deploying AI systems emerge. AI systems enable comprehensive monitoring of employee performance, analyzing data over time to discern trends, strengths, and areas needing improvement. Moreover, AI-driven platforms regularly assess employee satisfaction and engagement, utilizing data analytics to pinpoint potential issues or patterns throughout the organization. AI also enhances HR operations by processing extensive data from various activities, offering insights into workforce dynamics, productivity levels, and the overall effectiveness of HR policies. Additionally, AI automates routine administrative tasks such as timekeeping, scheduling, and compliance reporting. In certain cases, AI can even monitor the health and well-being of employees by analyzing metrics like work hours, physical activity levels, and self-reported mood scores. Each of these applications demonstrates AI's potential to transform traditional employment practices by providing more in-depth, data-driven insights and automating administrative processes, thereby optimizing workforce management and operational efficiency.

Taking into account various possibilities of using AI systems in recruitment and established employment relationships, it is crucial to address several aspects of the GDPR that are particularly pertinent. By highlighting these regulatory considerations, the article aims to balance the legal boundaries necessary to foster both technological advancement and privacy protection in employment practices.

Within the scope of this article, two crucial aspects from the data protection perspective will be analyzed: 1) the use of consent as a legal ground for processing personal data in AI systems; 2) automated decision-making, including potential biases and the ability for data subjects to exercise their rights.:

1) Consent – consent is one of the legal grounds stated in the GDPR that can be used as a legal basis for processing personal data. In scope of employment legal relationships, consent is not commonly used as a legal basis for processing personal data due to the dependent nature of the employee-employer relationship. This dependency may lead to consent that is not fully compliant with GDPR requirements. Conversely, in the recruitment process, consent is frequently utilized as a legal ground for processing data collected from the candidates. According to the GDPR, consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement [7]. This includes, that clear and understandable information needs to be provided to the data subject, in this case employee about the consent that is beeing collected, i.e., what amount of personal data will be collected, for what exact purposes, etc. Therefore, when analyzing the requirements set out in the GDPR regarding consent, and in the AI Act, particularly the obligations for employers to inform affected workers of their exposure to high-risk AI systems, it can be concluded that this information should be provided at the very beginning of the recruitment process. This includes before collecting personal data and prior to its use in AI systems. Consequently, the information required for consent to be lawful and the information about the use of AI systems could be provided simultaneously.

However, prior to implementing such solutions for recruitment, employers should assess the impact of the solution on potential candidates, taking into account the data subjects' right to object at any time to the processing of personal data concerning them which is based on automated decision-making. This assessment should include the evaluation of possible alternatives, for example, ensuring the possibility for candidates to opt out of the use of the AI system and proceed through the recruitment process in another manner. The aspects of the automated decision-making in scope of using AI systems are analyzed in the next section of the article.

2) Automated decision-making – if AI systems are used in recruitment process to screen resumes and to eliminate candidates, or in employment relationships – e.g., to analyze employee work efficiency in employment leading to termination of legal relationship, this is considered as automated decision-making according to the GDPR. Decisions made by automated means, in this case AI systems, without human envolvement grant employees ('data subjects' under GDPR) specific rights. These rights include requesting a manual review of the decision, involving human oversight. Article 22 (1) of the GDPR states, that the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her [7], thus, employers in scope of implementing use of AI systems in their processes need to ensure, that the candidates and employees are able to excersise their rights according to the GDPR and ask for human envolvement into the decisions made by the AI system.

However, the use of AI systems in automated decision-making is further complicated by the GDPR requirements for transparently defining the logic embedded within the decision-making process. GDPR states, that meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing that involved automated decision-making should be provided. Unlike other types of automated decision-making, where specific logic and criteria are clearly established to guide decisions, ensuring full compliance with these GDPR requirements is challenging with AI systems. To effectively utilize AI systems in such contexts, a common understanding of how information about the decision-making process should be communicated is necessary. In the author's opinion, the European Data Protection Board (hereinafter "EDPB") should establish guidelines or specific provisions to clarify the explanation of the logic used in automated decision-making involving AI systems. This would facilitate unifyed application and adherence to GDPR requirements. Otherwise, the lack of specific guidance from the EDPB might lead to varying interpretations of the requirements across the EU, potentially resulting in non-compliance with GDPR mandates.

Also, similarly, when utilizing AI systems in decision-making, it is crucial to ensure that these systems do not perpetuate discrimination in any aspect of decision-making. As stated in Recital 75 of the GDPR the risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination [..] [7]. Also as set out in the AI Act, it is necessary to analyze and prevent any biases using AI system, however due to different type of AI systems, processes how the AI is trained and how the information provided to the AI system is analyzed, it is still a risk, that AI systems could be biass in their decision making, that might lead to discrimination.

AI Act states, that diversity, non-discrimination and fairness means that AI systems are developed and used in a way that includes diverse actors and promotes equal access, gender equality and cultural diversity, while avoiding discriminatory impacts and unfair biases that are prohibited by Union or national law. Biases can for example be inherent in underlying data sets, especially when historical data is being used, or generated when the systems are implemented in real world settings. Results provided by AI systems could be influenced by such inherent biases that are inclined to gradually increase and thereby perpetuate and amplify existing discrimination, in particular for persons belonging to certain vulnerable groups, including racial or ethnic groups [3].

As research from the EU Agency for Fundamental Rights highlights, users of predictive algorithms need to assess the quality of training data and other sources that influence bias and may lead to discrimination. Such bias and potential discrimination may be developed or amplified over time, when data based on outputs of algorithmic systems become the basis for updated algorithms. Consequently, algorithms that are used to make or support decisions about people, such as predictive policing, need to be assessed before and regularly after deployment. Special attention needs to be paid to the use of machine learning algorithms and automated decision-making [8].

Analyzing different scientific researh papers, it is clear, that it remains a debatable issue whether a human or an AI system can exhibit more bias in decision-making processes. Human and AI biases can consequently create a feedback loop, with small initial biases increasing the risk of human error, according to the findings published in Nature Human Behaviour [9], [10]. Co-lead author Professor Tali Sharot (UCL Psychology & Language Sciences, Max Planck UCL Centre for Computational Psychiatry and Ageing Research, and Massachusetts Institute of Technology) said: "People are inherently biased, so when we train AI systems on sets of data that have been produced by people, the AI algorithms learn the human biases that are embedded in the data. AI then tends to exploit and amplify these biases to improve its prediction accuracy. Professor Sharot added: “Algorithm developers have a great responsibility in designing AI systems; the influence of AI biases could have profound implications as AI becomes increasingly prevalent in many aspects of our lives.” [9], [10]. Thus, even the responsibility for training an AI system—including ensuring that decisions made by it are unbiased —falls under the provider responsibility, the deployer should also analyze the decisions made by the AI system to ensure there is no discrimination.

IV. Conclusions

Overall, this article has highlighted several important aspects to consider when integrating AI systems into employee recruitment and employment relationships. While it addresses key points such as non-discrimination, transparency in automated decision-making, and the division of responsibilities between AI providers and deployers, it also acknowledges the limitations of its scope. There are many more aspects of AI system usage in employment contexts that merit attention but are beyond the breadth of this article.

Main conclusions:

1. **Alignment with EU Values:** The European Union aims to foster innovation and employment while safeguarding fundamental rights and freedoms. This entails that the development, marketing, implementation, and usage of AI systems within the Union must adhere to Union values. This approach ensures the promotion of human-centric and trustworthy AI, alongside a robust protection of fundamental rights.
2. **High-Risk AI Systems in Employment:** AI systems used for recruitment or employee management—such as those deployed to analyze and filter job applications, assess candidates, make decisions affecting employment terms, or monitor employee performance—are categorized as high-risk. This designation underscores the significant implications these systems can have on personal and professional aspects of individuals' lives.
3. **Duty to Inform:** Before deploying high-risk AI systems within the workplace, it is mandatory for employers (deployers) to inform both workers' representatives and the affected workers about the implementation of these systems. This transparency is crucial in maintaining trust and adherence to ethical standards in the deployment of AI technologies.
4. **Impact Assessments:** Although specific requirements for Fundamental Rights Impact Assessments are not mandated in the employment sector under current regulations, the importance of conducting thorough and high-quality assessments remains critical. This includes the utilization of Data Protection Impact Assessments (DPIAs) which should be expanded to also thoroughly evaluate the risks AI systems might pose to fundamental rights.
5. **Consent in Recruitment:** When using consent as the legal ground for processing personal data in the recruitment process, information about the use of AI systems should be provided simultaneously. There is no need for separate consent specifically for the use of AI systems, as long as the information provided covers all aspects of personal data processing, including the deployment of AI.
6. **Right to Object:** In scenarios where AI systems are utilized in recruitment and/or employment that result in automated decision-making, it is imperative to ensure that candidates or employees can exercise their right to object to such processing. This right is crucial in cases where decisions could significantly affect their professional life, ensuring compliance with GDPR provisions on automated decision-making.
7. **Challenges with Automated Decision-Making:** The use of AI in automated decision-making complicates compliance with GDPR requirements, which demand transparency in the logic used within the decision-making process. Unlike other automated systems where the decision-making criteria are clear, AI systems often involve complex algorithms that are not transparent. To effectively deploy AI in such contexts, there must be a common understanding of how details about the decision-making process are communicated.
8. **Non-Discrimination in AI Decision-Making:** When utilizing AI systems in decision-making processes, it is imperative to ensure that these systems do not perpetuate discrimination in any form. This involves rigorous testing and monitoring of AI algorithms to detect and mitigate any biases that may exist within the decision-making framework. Ensuring fairness and equity in automated decisions is not only a technical requirement but also a legal and ethical imperative to uphold the standards of justice and non-discrimination enshrined in both EU law and broader international human rights norms.

Acknowledgments

This study was funded by the project "RSU internal and RSU with LSPA external consolidation”, No. 5.2.1.1.i.0/2/24/I/CFLA/005

References

[1] European Council, General Secretariat of the Council, “European Council meeting (19 October 2017) – Conclusions,” EUCO 14/17, October 19, 2017. [Online]. Available: https://data.consilium.europa.eu/doc/document/ST-14-2017-INIT/en/pdf . [Accessed: Feb. 1, 2025].

[2] “European approach to artificial intelligence,” Apr. 9, 2025. [Online]. Available: https://digital-

strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence. [Accessed: Apr. 17, 2025].

[3] "Regulation (EU) 2024/1689 of the European Parlianment 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)," Jul. 12, 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689. [Accessed: Feb. 1, 2025].

[4] "Charter of Fundamental Rights of the European Union, (2000/C 364/01), Official Journal of the European Communities," C364/1, Dec. 18, 2000. [Online]. Available: https://www.europarl.europa.eu/charter/pdf/text_en.pdf. [Accessed: Feb. 1, 2025].

[5] "European Convention on Human Rights, Council of Europe," Sep. 3, 1953. [Online]. Available: https://www.echr.coe.int/documents/d/echr/convention_ENG [Accessed: Feb. 20, 2025]

[6] European Court of Human Rights judgement, "Niemietz v. Germany," 13710/88, Dec. 16, 1992. [Online]. Available: https://hudoc.echr.coe.int/eng?i=001-57887. [Accessed: Feb.21, 2025]

[7] "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, and repealing Directive 95/46/EC (General Data Protection Regulation)," OJ L 119, May 4, 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. [Accessed: Feb.21, 2025]

[8] European Union Agency on Fundamental Rights, "Bias in Algorithms – Artificial Intellligence and Discrimination," 2022. [Online]. Available: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2022-bias-in-algorithms_en.pdf. [Accessed: Feb. 20, 2025].

[9] "Bias in AI amplifies our own biases," Dec. 18, 2024. [Online]. Available: https://www.ucl.ac.uk/news/2024/dec/bias-ai-amplifies-our-own-biases#:~:text=Artificial%20intelligence%20(AI)%20systems%20tend,new%20study%20by%20UCL%20researchers. [Accessed: Feb. 23, 2025].

[10] M. Glickman and T. Sharot, "How human–AI feedback loops alter human perceptual, emotional and social judgements," Nature Humane Behaviour, vol. 9, no.2, p. 345, February 2025. Available: Nature Human Behaviour, https://www.nature.com/articles/s41562-024-02077-2 [Accessed: Feb. 23, 2025], https://doi.org/10.1038/s41562-024-02077-2