Digital Rights in the Age of Artificial Intelligence: Challenges and Perspectives

Lecturer **Aurel Octavian PASAT**[1]

Abstract

As AI technologies become deeply embedded in society, new legal challenges related to the collection and use of personal data arise, as well as risks associated with mass surveillance and digital censorship. The article explores the growing impact of artificial intelligence (AI) on digital rights, emphasising issues such as privacy, data access and freedom of expression. It also emphasises the need to strike a balance between technological innovation and the protection of citizens' fundamental rights, through a comparative analysis of different legal systems. It takes a look at the data protection legislative framework in the European Union (GDPR) versus that in the United States, examining emerging challenges and opportunities. Relevant case studies are used to illustrate where regulations can be implemented effectively or where they are insufficient, suggesting possible solutions and future directions.

Keywords: *digital rights, artificial intelligence, fundamental rights, legal systems.*

JEL Classification: K24, K38

DOI: https://doi.org/10.62768/ADJURIS/2025/3/08

Please cite this article as:
Pasat, Aurel Octavian, „Digital Rights in the Age of Artificial Intelligence: Challenges and Perspectives", in Devetzis, Dimitrios, Dana Volosevici & Leonidas Sotiropoulos (eds.), *Digital Lawscapes: Artificial Intelligence, Cybersecurity and the New European Order*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2025, p. 144-161.

1. Introduction

Digital rights are a set of fundamental rights and freedoms that are applicable in the digital environment. They are derivatives of human rights, adapted to protect individuals in the face of the technological challenges and risks of the digital age. In the context of Artificial Intelligence, digital rights take on new dimensions, requiring a complex and dynamic approach to keep pace with rapid developments in technology.

The main digital rights in the era of Artificial Intelligence are:

[1] Aurel Octavian Pasat - Cross-border Faculty, „Dunarea de Jos" University of Galati, Romania, ORCID: 0000-0002-7239-0808, aurel.pasat@uagl.ro.

- *Right to privacy and personal data protection.* This right protects individuals' personal information from unauthorised collection, processing and sharing. In the age of AI, the emphasis is on user control over their data and transparency of automated data processing. AI algorithms can analyse and predict users' behaviour based on personal data, raising issues of surveillance and privacy violations. Facial recognition technologies and targeted advertising use personal information, often without clear consent or full understanding from the user.

- *Right to information and algorithmic transparency.* Users have the right to understand how their data is collected, used and processed by AI systems. Algorithmic transparency refers to the ability of individuals to know the principles and methods by which AI arrives at certain decisions or recommendations. Opaque algorithms or so-called 'black *boxes*' are difficult to understand even for experts, which complicates monitoring and ensuring fairness. Social media platforms and search engines use complex algorithms to monitor content, but users are often unaware of the criteria or data used for these decisions.

- *Right to freedom of expression and avoiding algorithmic censorship.* Freedom of expression is also protected in the digital environment, but AI used to moderate content can create risks of unwarranted censorship or manipulation of information. Algorithms that moderate content can have biases that lead to incorrect removal of content or the promotion of biased opinions. This can affect a plurality of opinions and access to information. Automated decisions by moderation algorithms on social platforms can lead to the removal of content that is deemed '*dangerous*' or '*offensive*' but which does not clearly violate community rules.

- *Right to justice and protection against automated decisions.* This right ensures that individuals are protected from automated decisions that affect their lives, without human intervention or the ability to challenge those decisions. It also covers the right to be informed and to understand the impact of AI algorithms on personal rights. Automated AI decisions are already being used in critical sectors such as finance, the judiciary or in the employment process, and the lack of human intervention or the possibility of challenging these decisions can have serious consequences. Credit scores automatically calculated by AI can influence a person's ability to obtain a loan, and users may not have effective means to challenge or understand the decision.

- *Right to digital security and protection against abuse.* This right protects users from cyber attacks, data breaches and misuse of digital information. AI can be used to identify and prevent such threats, but it can also facilitate advanced attacks. As AI technologies become more advanced, cybersecurity risks become more complex, requiring advanced protection and response measures. AI can be used to launch sophisticated phishing attacks or analyse vulnerabilities in security networks.

2. The Importance of Protecting Digital Rights in the AI Era

Digital rights are becoming essential in an increasingly interconnected and automated world. Everyone leaves a digital data trail on a daily basis; perhaps by buying a coffee using a reward account or by using an electronic toll collection system[2]. AI technologies, while beneficial in many ways, have the potential to profoundly affect users' digital lives and privacy. Thus, it is important that laws constantly evolve to protect these fundamental rights and to ensure a balance between innovation and respect for democratic principles. This emphasises the importance of proactive regulation and global collaboration between lawyers, technology experts, ethicists and policy-makers. Digital rights are thus at the centre of contemporary debates on technology and society, even if Peacock[3] points out, there is still debate over whether 'access to the Internet is a human right in and of itself, part of already-existing freedom of expression guarantees, or not a right at all'.

2.1. Privacy and Data Protection: the Impact of AI on Privacy

In the digital age, AI plays a significant role in transforming the way personal data is collected, processed and used. Advanced AI algorithms are capable of analysing massive volumes of data with unparalleled speed and accuracy, and this has major implications for users' privacy. While AI brings benefits, such as personalising digital experiences and improving service efficiency, these technological capabilities also create serious privacy risks. However, the privacy paradox states that the information disclosure of Internet users is problematic; although many people are concerned about their privacy online, they still share plenty of personal information on the web.[4]

Personal data is collected and processed by AI as follows:

- *Personalisation of content*: AI algorithms are widely used by digital platforms to personalise the content delivered to users, such as recommendations of movies, articles or advertisements. To do this, AI collects and analyses detailed

[2] Chih-Liang Yeh (2018), „Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers", *Telecommunications Policy*, Vol. 42, Issue 4, pp. 282–292, https://doi.org/10.1016/j.telpol.2017.12.001.

[3] Anne Peacock (2019). *Human rights and the digital divide*. London, Routledge, p. 4, https://doi.org/10.4324/9781351046794.

[4] Tobias Dienlin, Philipp K. Masur, Sabine Trepte (2023). „A longitudinal analysis of the privacy paradox". *New Media & Society*, 25(5), 1043-1064. https://doi.org/10.1177/14614448211016316; Alessandro Acquisti, Jens Grossklags (2003), *Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior*, UC Berkeley 2nd Annual Workshop on "Economics and Information Security", available at: https://infosecon.net/workshop/downloads/2003/pdf/Final_session6_acquisti.pdf, accessed on 07.05.2025.

data about user preferences and behaviours, including browsing history, geographic location, social interactions and more. This intensive data collection raises concerns about the constant surveillance of users and the lack of transparency about how their data is used.

- *Targeted advertising*: The advertising industry uses AI to analyse and predict users' consumer preferences. Algorithms can identify behavioural patterns and create detailed profiles for each user to deliver the most relevant ads. This targeting capability may seem harmless at first glance, but it can reveal intimate aspects of personal lives, for example health, political or religious beliefs, and can be considered invasive.

- *Digital surveillance*: AI technologies are used by governments and private organisations to monitor people's online and offline activities. For example, facial recognition and real-time video stream analysis are used for mass surveillance. These technologies can violate the right to privacy, especially when there is no solid legal framework regulating the limits of their use. In some cases, surveillance technologies are used to monitor citizens without their consent, raising serious human rights concerns.

Major privacy challenges in the AI era are:

- *Lack of transparency*: One of the biggest obstacles to protecting privacy is the opacity of AI algorithms. Most users are unaware of how their data is collected and used and who has access to it. Moreover, the complex nature of AI algorithms makes it difficult to understand decision-making processes, complicating the ability to trace accountability and ensure fair data processing.

- *Profiling and discrimination*: Using personal data to create predictive profiles can lead to discrimination, exclusion and may affect freedom of thought[5]. For example, AI may exclude individuals from employment or credit opportunities on the basis of criteria that are not obvious and may be profoundly unfair. The data collected and processed may reveal sensitive information, exposing users to risks of discrimination based on gender, race, religion or sexual orientation.

- *Government surveillance*: Some countries use AI to monitor citizens for national security or law enforcement purposes. This surveillance can be highly intrusive and can have a negative impact on individual liberty, especially in the absence of strict regulations to limit abuses. Privacy thus becomes increasingly vulnerable in a context of pervasive digital surveillance.

Case study: The impact of facial recognition on privacy. A notable example of how AI can affect privacy is the widespread use of facial recognition technology. In cities such as London and San Francisco, AI-enabled surveillance cameras are being used to monitor public spaces. While this technology is being touted as a means to improve public safety, it raises serious questions about the sanctity of privacy. For example, there are cases where citizens' biometric data

[5] Simon McCarthy-Jones (2019) „The Autonomous Mind: The Right to Freedom of Thought in the Twenty-First Century", *Frontiers in Artificial Intelligence, Vol. 2,* https://doi.org/10.3389/frai.2019.00019.

has been stored without consent or used to track political activists, undermining freedom of association and expression.

3. Legal Framework in the EU: GDPR

The General Data Protection Regulation (GDPR) is one of the world's most comprehensive and stringent regulations on the protection of personal data. Adopted by the European Union in 2018, the GDPR provides a robust legal framework aimed at protecting the privacy and personal data of European citizens. The regulation sets high standards for how organisations collect, manage and use personal data, imposing clear user rights and severe penalties for violating those rights.

3.1. Fundamental Rights Guaranteed by GDPR

GDPR provides a number of fundamental rights to EU citizens, designed to protect their privacy and give them control over their personal data. These rights include:

- *Right to information*: Organisations are obliged to provide users with clear and understandable information about how their data is collected and used. Users must be informed about the purposes of processing, the duration of data storage and the rights they have under the GDPR.
- *Right of access*: Citizens have the right to access the personal data an organisation holds about them. This includes obtaining information about the categories of data processed, the purpose of the processing and any third parties to whom the data has been disclosed.
- *Right to rectification*: Users may request the correction of inaccurate or incomplete personal data. Organisations must comply with such requests without undue delay.
- *Right to erasure* ('Right to be forgotten'): Citizens can request deletion of personal data in certain circumstances, such as when the data is no longer necessary for the purposes for which it was collected or when users withdraw their consent.
- *Right to restriction of processing*: Users can ask to restrict the processing of their personal data in certain circumstances, for example, if the accuracy of the data is contested.
- *Right to data portability*: the GDPR allows users to receive the personal data they have provided to an organisation in a structured, commonly used and machine-readable format. They can also request the transfer of this data to another organisation.
- *Right to object*: Citizens have the right to object to the processing of their personal data for direct marketing, scientific research or statistical purposes, depending on the circumstances.

- *Rights related to automated decisions and profiling*: the GDPR guarantees protection against decisions based solely on automated processing (including profiling) that have a significant impact on users. Citizens have the right not to be subject to such automated decisions if they have not consented to them or if they are not necessary for the performance of a contract.

The GDPR includes severe penalties for companies that fail to comply with its requirements, and EU regulators have imposed significant fines to ensure compliance. These fines can reach up to €20 million or 4% of a company's annual global turnover, whichever is higher. Here are some important examples:

- *Google*: In 2019, Google was fined €50 million by the French data protection authority, CNIL (Commission Nationale de l'Informatique et des Libertés), for breaching GDPR. The CNIL found that Google failed to provide users with clear and transparent information about its data processing policy and failed to obtain valid consent for the personalisation of ads. This sanction emphasised the importance of transparency and consent in the management of personal data.

- *Facebook (Meta Platforms Inc.)*: In 2021, Facebook was fined €265 million by Ireland's Data Protection Commission (DPC) for a massive data breach that exposed the personal information of more than 533 million users worldwide. The leaked data included phone numbers, email addresses and other sensitive information, and the investigation found that Facebook failed to comply with GDPR data security requirements.

- *British Airways:* In 2020, British Airways was fined £20 million for a data breach that affected the personal information of around 400,000 customers. The investigation found that the company failed to take adequate measures to protect personal data in breach of GDPR regulations.

H&M: In 2020, H&M was fined €35m for unlawfully collecting and storing excessively detailed information about its employees. The investigation found that H&M managers in Germany recorded details about employees' personal lives, such as health issues and religious beliefs, violating their privacy and fundamental rights.

The implementation of the GDPR has forced companies to become more accountable and transparent in their handling of personal data, leading to better protection of the fundamental rights of European citizens. However, significant challenges remain, such as ensuring compliance among global companies and striking a balance between privacy protection and technological innovation.

The GDPR is a gold standard example of data protection, inspiring other countries to adopt similar laws, and is a benchmark for regulating AI and its impact on privacy.

4. US and Data Protection

In the United States, the protection of personal data is regulated in a fragmented manner, with no homogenous federal legislation similar to the General

Data Protection Regulation (GDPR) in the European Union. The US approach to data privacy and security is mainly influenced by state-specific regulations and a number of sector-specific laws at the federal level. This complex structure creates a number of challenges and criticisms, especially compared to the strict standards imposed by GDPR in Europe.

Lack of Homogeneous Federal Legislation. One of the key features of data protection regulation in the US is the lack of a single, comprehensive and uniform federal legislative framework covering all aspects of personal data privacy. Instead, data protection is ensured through a combination of federal laws, state regulations and industry-specific rules. This decentralised approach can lead to inconsistencies and gaps in protecting citizens' privacy.

State laws. A notable example of state-level regulation is the California Consumer Privacy Act (CCPA), which is one of the strictest and most comprehensive data privacy laws in the US. Passed in 2018 and implemented in 2020, it has been called the US equivalent of GDPR[6]. The US corporations then promptly put resources to lobby against the California law, as the industry was concerning that the CCPA would become a de facto national standard.[7]

The CCPA gives California citizens extensive rights over their personal data, including the right to know what information is being collected, to request deletion of data, and to refuse the sale of personal data. The CCPA is seen as a benchmark for other states looking to introduce similar regulations.

Federal sectoral laws. Instead of a single federal data protection law, the US relies on laws regulating privacy in specific sectors. For example:

- *Health Insurance Portability and Accountability Act (HIPAA): protects the privacy of patient health data.*

- *Children's Online Privacy Protection Act (COPPA):* Protects children under 13 online.

- *The Gramm-Leach-Bliley Act (GLBA)*: Regulates the privacy of consumer financial information.

This sector-specific approach may leave certain categories of personal data unprotected or weakly protected, depending on the nature of the activities or the jurisdiction of the application.

Criticisms of Weaker Data Protection Compared to the EU. The US regulatory model is often criticised for offering weaker protection of personal data compared to the rigorous standards imposed by the GDPR in the EU. There are several issues underlying these criticisms:

---

[6] Jeeyun (Sophia) Baik (2020), „Data privacy against innovation or against discrimination?: The Case of the California Consumer Privacy Act (CCPA)", *Telematics and Informatics*, Vol. 52, 101431, https://doi.org/10.1016/j.tele.2020.101431.

[7] Matti Minkkinen, (2019). „Making the future by using the future: A study on influencing privacy protection rules through anticipatory storylines". *New Media & Society*, 21(4), 984-1005. https://doi.org/10.1177/1461444818817519.

- *Lack of general protection*. Unlike the GDPR, which provides protection for all EU citizens' personal data, regardless of sector, US law is fragmented and only applies in certain contexts. For example, many of the rights offered by the GDPR, such as the right to erasure ('Right to be forgotten') or the right to data portability, are not universally recognised in the US.

- *Consent and transparency*: the GDPR imposes strict requirements to obtain informed consent from users before collecting and processing personal data. In the US, many companies may collect data without explicit consent, using general privacy clauses that are often difficult to understand or ambiguous. This has led to abuses and use of data without the full knowledge of users.

- *Selling and monetising data*: Another major criticism is the permissiveness of the US system in selling and sharing personal data for commercial purposes. In the US, user data is a valuable resource for companies, and many regulations do not provide sufficient restrictions to prevent unethical or abusive use.

- *The power of tech companies*: Some of the world's biggest tech companies, such as Google, Facebook (Meta), Amazon and Microsoft, are based in the US. These companies hold huge amounts of personal data and are often accused of invasive data collection and use practices. The lack of strict federal regulation in the US allows them to operate with greater freedom than would be allowed in the EU.

- *Government surveillance*: Another issue criticised is the access of government authorities to citizens' personal data in the name of national security. US legislation, such as the Patriot Act, allows the government to collect and use data for security purposes, which raises serious concerns about privacy violations. For example, the mass surveillance programme revealed by Edward Snowden has shed light on the extent of personal data collection by US government agencies.

US law compared with EU GDPR:

User access to data: the GDPR guarantees citizens' right of access to their data and gives them control over how it is used. In the US, this level of control and transparency is not widely available, with the exception of some state regulations, such as the CCPA.

Fines and penalties: the GDPR provides significant penalties for breaches, incentivising companies to comply with strict data protection rules. In the US, fines are rarer and often lower, except in cases of blatant violation of sector-specific laws.

User consent: the GDPR requires explicit and informed consent for the collection of personal data, whereas in the US, the consent policy is more relaxed and often tilted in favour of companies.

The lack of uniform federal legislation in the US creates a less predictable and less protective system for personal data privacy than the GDPR in the EU. Criticisms of insufficient data protection, combined with the influence of technology companies and concerns about government oversight, suggest an urgent

need for reform and a more rigorous federal legislative framework. However, despite these challenges, there is a growing movement in the US to improve data protection and bring standards in line with European ones.

5. Challenges in Implementing AI and Data Regulation

Artificial Intelligence (AI) has radically transformed the digital landscape and modern society, but applying data protection and privacy regulations in this context presents significant challenges. The complexity of AI technologies and their global nature have created major difficulties for regulators and organisations to comply.

Enforcement of privacy regulations in the AI era faces several obstacles that complicate the effectiveness and consistency of these laws, such as:

a. Opaque algorithms and regulatory difficulty. One of the biggest obstacles in regulatory enforcement is the opaque nature of AI algorithms**.** Many algorithms, especially those based on machine learning and neural networks, operate as 'black boxes'. Roughly speaking, that an AI system is opaque means that it is difficult for users to know how it works, as well as to interpret its decisions at various levels and evaluate its behaviour against scientific and ethical norms.[8]

For example, algorithms can make decisions that have a significant impact on individuals, such as credit assessment, hiring or surveillance. The problem is that when automated decisions are challenged, companies are unable to provide clear explanations of how these decisions were made, in violation of the transparency and explainability requirements stipulated by modern regulations such as GDPR.

b. National and transnational borders. AI operates on a global scale, which makes enforcement of regulations extremely complicated, especially when collecting and transferring personal data between jurisdictions with different legal standards.

For example, in the European Union, the GDPR imposes strict rules for data protection, but other countries, such as the US, have a more relaxed approach and a fragment. This discrepancy creates a situation where a company operating globally has to comply with multiple conflicting regulations, which can be logistically difficult and costly.

For international data transfers, many companies use data infrastructure located in several countries. In this context, the transfer of personal data from the

[8] Carlos Zednik (2021), "Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence." *Philosophy & Technology* 34, no. 2 (2021): 265+. *Gale Academic OneFile* (accessed July 20, 2025). https://link.gale.com/apps/doc/A666288938/AONE?u=anon~35db595a&sid=googleScholar&xid=374b64c2; Alessandro Facchini, Alberto Termine (2021), "Towards a taxonomy for the opacity of AI systems," in Vincent C. Müller (ed.), *Philosophy and Theory of Artificial Intelligence (PTAI),* Ed. Cham, CH: Springer International Publishing, 2022, pp. 73–89.

EU to countries that do not offer an adequate level of protection becomes an issue. Despite international agreements such as the Privacy Shield (replaced by the Transatlantic Data Privacy Framework), there is a risk that citizens' personal data could be exposed to government surveillance or unauthorised uses.

c. Emerging technologies and delayed regulation. The rapid pace of AI development means that legislation often lags behind. Emerging technologies such as natural language processing, facial recognition, and autonomous vehicles present unique challenges that have not yet been fully addressed by existing regulations.

Current laws, such as GDPR, were written with a specific type of data processing in mind and do not fully cover the complexity of AI. For example, GDPR does not explicitly provide rules for how AI must be programmed or audited to prevent discrimination.

Regulators often find it difficult to react quickly to new challenges posed by AI due to lengthy and complex legislative processes. In addition, the lack of technical expertise of some regulators complicates the assessment of new technologies and their impact on privacy.

Although the implementation issues are complex, there are some directions and proposals that could contribute to better regulation of AI:

1. *Algorithmic transparency and auditability*: one suggested solution is the imposition of clear auditing standards for algorithms, which would allow verification of how AI processes data and makes decisions. This would require collaboration between authorities and technology experts to develop effective evaluation methods.

2. *Global regulatory standardisation*: The development of an international regulatory framework for AI could reduce differences across jurisdictions. Organisations such as the UN and the Council of Europe have already started discussing the creation of global principles for the ethical and responsible use of AI.

3. *Education and training of regulatory experts*: Regulators could benefit from better training and technology education to better understand and manage AI challenges.

The challenges of implementing AI and data regulation are complex and varied, involving algorithm transparency, international legal differences, and the rapid pace of technological innovation. In order to effectively protect citizens' privacy and maintain trust in AI technologies, there is a need for close collaboration between lawyers, engineers and regulators, as well as constant adaptation of regulations to new technological realities.

6. Algorithmic Bias and Discrimination

Algorithmic bias (or algorithmic bias) occurs when Artificial Intelligence algorithms make decisions that disproportionately disadvantage certain groups of

people, either because of the data used for training or because of the way these algorithms are designed. Because AI learns from large sets of data that may reflect existing inequalities and biases in society, there is a risk that these biases will be amplified, which can lead to significant discrimination in various domains.

AI has often led to discrimination, emphasising the importance of auditing and transparency of algorithms.

Examples of discrimination cases:

Criminal Risk Assessment Algorithm (COMPAS). The COMPAS algorithm has been used in several US states to assess a defendant's risk of recidivism and to help judges make bail or parole decisions.

An investigation by *ProPublica* in 2016 found that the algorithm was biased against people of colour. Although it was similarly accurate in predicting recidivism among different racial groups, COMPAS disproportionately classified people of colour as having a higher risk of committing future crimes, even when they did not reoffend. Instead, the algorithm tended to underestimate the risk for white people. This algorithmic bias raised major concerns about the fairness of the criminal justice system.[9]

The COMPAS case has emphasised the need for transparency and auditing of algorithms used in criminal justice systems, especially when they have a direct impact on people's lives. It also demonstrated the risk of using AI without understanding and correcting implicit biases in training data.

Hiring algorithms (Amazon). Amazon has developed an AI-based recruitment algorithm to evaluate candidates for technical positions. The algorithm was trained on CV data from the last 10 years of company employees.

The algorithm was found to discriminate against women, as the historical data on which it was trained reflected male dominance in technical positions. As a result, the AI learned to penalise CVs that contained words associated with women, such as 'women's chess club captain' or the names of women's universities. Even though these penalty criteria were not explicitly programmed, the algorithm absorbed biases from the training data.[10]

Amazon was forced to stop using the algorithm, but the case showed how easily discrimination can occur when biased data is used to train AI. Continuous auditing and assessing the fairness of algorithms are essential to prevent such negative effects.

Facial recognition and racial bias. Facial recognition technologies developed by companies such as IBM, Microsoft and Amazon have been tested for

[9] Jeff Larson, Surya Mattu, Lauren Kirchner and Julia Angwin (2016), *How We Analysed the COMPAS Recidivism Algorithm*, https://www.propublica.org/article/how-we-analyzed-the-comp as-recidivism-algorithm.

[10] Maude Lavanchy (2018), *Amazon's sexist hiring algorithm could still be better than a human expecting algorithms to perform perfectly might be asking too much of ourselves*, The Conversation, Lausanne, Switzerland, https://imd.widen.net/view/pdf/z7itobahi6/tc061-18-print.pdf.

their accuracy in recognising the facial features of people from different ethnic groups.

Studies, such as the one conducted by the *MIT Media Lab*, showed that these algorithms had significantly higher error rates in correctly identifying people of colour, particularly women of colour. For example, a black woman had up to a 34% probability of being misclassified, while the error rate for white men was less than 1%. This bias can lead to serious results when technology is used by law enforcement agencies to identify suspects.[11]

In response to these findings, some companies have suspended the sale of facial recognition technologies to police, emphasising the importance of ensuring the fairness of algorithms and testing them on diverse datasets.

Lending schemes and financial discrimination. Some financial technology companies are using AI to assess customer creditworthiness and decide whether to approve loans or credit cards. Algorithms analyse various data, including financial history, location, occupation and other behavioural variables.

One example is where lending algorithms gave lower scores to women compared to men, even when both groups had similar financial profiles. A high-profile case was that of Apple Card's lending programme, where several users reported that women were given lower credit limits than men, despite having comparable financial histories.[12]

This type of discrimination emphasises the need for regulation and oversight of the algorithms used for financial decisions. AI needs to be scrutinised to ensure that it does not introduce biases that affect access to financial resources.

Audit and transparency of algorithms are important for the following reasons:

1. Bias detection and correction: auditing algorithms may reveal biases that are not obvious at first glance. Continuous testing on diverse datasets can help to identify and eliminate bias.

2. Building trust: algorithmic transparency enables users and authorities to understand how automated decisions are made, thus helping to build trust in the use of AI. This is especially essential in sensitive sectors, such as justice, healthcare and finance.

3. Ethical and legal compliance: algorithms used by organisations must comply with data protection regulations and fairness principles. Without transparency and auditing, it is difficult to demonstrate that AI is acting in a fair and ethical way.

Algorithmic bias and discrimination caused by AI represent significant challenges that emphasise the urgent need to develop robust audit mechanisms and impose transparency requirements. Algorithms are not neutral; they are a

[11] https://www.media.mit.edu/articles/study-finds-gender-and-skin-type-bias-in-commercial-artificial-intelligence-systems/, accessed on 07.05.2025.

[12] https://www.technologyreview.com/2019/11/11/131983/apple-card-is-being-investigated-over-claims-it-gives-women-lower-credit-limits/, accessed on 07.05.2025.

product of the data they learn and the people who develop them. Without appropriate measures, AI risks perpetuating and even amplifying social inequalities, which requires an ethical and well-regulated approach.

7. Sources of Conflict Between Regulation and Innovation

In the age of Artificial Intelligence, strict data protection and privacy regulations play a crucial role in protecting users' rights and maintaining public trust in digital technologies. However, regulations can conflict with the rapid pace of technological innovation, creating a dilemma between user safety and technological progress. Let us analyse how these two issues interact and what sources of conflict arise.

a) Strict regulations can inhibit innovation. Stringent data protection regulations, such as GDPR in the European Union, impose complex requirements on companies developing AI technologies, which can lead to significant barriers to innovation.

We exemplify some ways in which these regulations can inhibit progress:

Compliance costs: Complying with strict regulations requires large investments in infrastructure and skilled staff to manage data privacy. For example, companies must hire data protection experts and implement complex security, auditing and reporting mechanisms. These requirements can be a heavy burden for startups and small companies that lack the resources to meet these standards. As a result, many startups may be discouraged from innovating in AI.

Slowing product development: Companies developing AI solutions need to conduct privacy impact assessments and implement preventive measures to minimise risks. These processes can delay new product launches and reduce the ability to compete in a dynamic global marketplace where rapid innovation is the key to success.

Limiting the use of data: Many regulations restrict how companies can collect and use users' personal data, which can hinder the development of advanced AI algorithms. AI depends on large amounts of data to learn and improve. When access to this data is restricted, AI innovation can suffer. For example, the GDPR's limitations on international data transfer can make it difficult to collect the diverse data needed to build efficient and fair AI systems.

b) Need for Regulation to Protect Users. Despite the impact on innovation, strict regulation is essential to protect users from the inherent risks of AI technologies. Some reasons for this need include:

Preventing abuse: AI has the ability to invade people's privacy in unprecedented ways by collecting and analysing personal data. Without clear regulations, companies could use this data in a way that jeopardises users' privacy and safety. Strict regulations ensure that data is processed transparently, fairly and only for well-defined purposes.

Reducing algorithmic discrimination: As discussed above, AI can reproduce or even amplify existing biases in the data it processes. Regulations require measures to prevent discrimination and ensure transparency of algorithms, thus protecting vulnerable groups from unfair or biased decisions.

Increased accountability: Without strict regulations, companies may avoid taking responsibility for errors or abuses of their algorithms. Clear rules, such as the right to explainability and the right to challenge automated decisions, force companies to be more transparent and accountable in their use of AI.

8. Relevant Cases of Conflict Between Regulation and Innovation

Healthcare industry and personal data: Companies developing AI technologies for the diagnosis and treatment of diseases rely on access to large sets of medical data to train and refine algorithms. However, GDPR and other medical privacy regulations limit access to patient data, slowing the pace of medical innovation. While these regulations protect patient privacy, they create a conflict with the urgent need to develop advanced AI solutions to save lives.

Autonomous vehicles and legal liability: Developers of autonomous vehicles face strict regulations on safety and legal liability. The algorithms that drive these vehicles need to be highly sophisticated and well tested before widespread deployment. However, strict regulations can delay testing on public roads and limit progress, although they are necessary to ensure public safety. This delicate balance between innovation and regulation continues to be a major challenge for the transport industry.

Financial technology (FinTech) and user data: FinTech companies are using AI to analyse financial behaviours and offer personalised credit solutions. However, data protection regulations sometimes prevent the efficient use of financial information, which limits AI's ability to personalise and improve services. Thus, innovation in FinTech can be hampered, even though these regulations are meant to protect users from financial abuse and privacy breaches.

Examples and the perspective of tech companies:

- *Google and Privacy Sandbox*: Google has announced initiatives such as Privacy Sandbox, to limit the use of third-party cookies and better protect user privacy[13]. But tech developers and advertisers have criticised the measure, arguing that it could inhibit innovation in the digital advertising industry and hurt the revenue streams of many online companies.

- *Facial recognition companies*: Some US cities, such as San Francisco, have banned the use of facial recognition technologies by government agencies because of privacy and civil rights risks. Companies that develop such technologies argue that such bans may limit innovation in public safety, though

[13] https://usercentrics.com/knowledge-hub/what-is-google-privacy-sandbox/, accessed on 07.05. 2025.

critics argue that the measures are necessary to prevent abuse.

While strict regulations may inhibit innovation in some areas, they are essential to protect users from potential AI abuse. One solution could be to adopt a flexible regulatory framework that encourages innovation while maintaining a high level of protection of personal data. Collaboration between regulators and the technology industry could also facilitate the development of solutions that respect both users' rights and the need for technological progress.

9. Conclusions

A global regulatory framework is becoming increasingly necessary as artificial intelligence advances and becomes a critical component in various economic and social sectors. The development and use of AI bring both significant opportunities and considerable risks, particularly in terms of data protection, ethics, and labour market impacts.

Regulating AI globally is important for several reasons:

Harmonisation of standards: as AI technology is used on a global scale, there is a risk that divergent regulations between countries could lead to legal issues, compliance difficulties and data protection vulnerabilities. A global framework could harmonise these regulations, ensuring effective protection for users regardless of region.

Cross-border risk management: AI can have effects that transcend national borders, such as information manipulation, cyber-attacks or influencing financial markets. A coordinated approach would help minimise these risks.

Data protection: Personal data is widely used by AI algorithms. A global framework could ensure clear rights for users and limits on data collection and processing.

Some key proposals for such a global framework include:

International co-operation and common standards:

- Creating an international platform for cooperation between governments, international organisations and private actors to establish common standards on AI and data protection.

- Building on existing initiatives, such as the European Union's General Data Protection Regulation (GDPR), which has set a precedent for the protection of personal data.

Algorithm transparency and accountability:

- A global requirement for companies developing AI to provide transparency about how their algorithms work and how personal data is used.

- Create independent audits to verify the impartiality and fairness of AI systems, thus preventing discrimination or systematic errors.

Ethical rules and user rights:

- Establish ethical principles such as respecting human dignity and ensuring that AI is used for the common good.

- The right of users to be informed when interacting with an AI system, as well as the option to refuse automation that significantly affects their lives.

Investment in education and workforce adaptation:

- International programmes to support the retraining of employees affected by automation to minimise the social and economic impact.

- Promote technology education and digital literacy to prepare new generations to operate with and around AI.

Cyber security and critical infrastructure:

- Implement cybersecurity policies to protect critical infrastructure from possible coordinated attacks involving AI.

- Information sharing between states to quickly and effectively manage potential threats.

Thoughtful global regulation could facilitate responsible innovation in AI, minimising risks and ensure benefits for society as a whole. The need for international coordination is evident to prevent a fragmented regulatory landscape that could disadvantage some states or groups of citizens.

Education and public awareness also play a key role in managing the impact of digital technologies, especially in the rapidly developing context of artificial intelligence and personal data protection. Informing citizens about their digital rights not only empowers them to protect their personal information, but also contributes to the empowerment of actors developing and using advanced technologies.

This requires the implementation of policies for education and awareness-raising, such as:

Educational programmes in schools and universities:

- Introduction of mandatory modules on digital rights and cybersecurity in school and university curricula.

- Organise practical workshops in schools to teach young people how to manage their digital footprint and how to recognise potential online threats.

*National awareness campaigns**:***

- Governments and international organisations can initiate information campaigns through media, social media and public events to educate citizens about data protection.

- Develop partnerships with NGOs and technology companies to share relevant resources and information.

Easily accessible information platforms:

- Create online platforms where citizens can learn about their digital rights, how to protect their information, and how to report abuses or security breaches.

- Publish clear guides, translated into different languages, to ensure that information is accessible to the widest possible audience.

Workshops and courses for adults:

- Organising workshops for adults in local communities so that people of

all age groups learn how to navigate the digital environment safely.

- Free or subsidised courses to teach the public about data protection, such as using passwords correctly, recognising phishing attempts and securing personal devices.

So a well-informed population is less susceptible to manipulation, fraud and cyber attacks. Education increases digital resilience, protecting both individuals and society's critical infrastructure. When citizens are informed about their rights, they are more likely to actively participate in digital policy discussions and demand better protection and regulation. Understanding the ethical implications of technology and how personal data is used helps citizens to make more informed decisions and support the responsible use of AI. An educated public can also more effectively advocate for policies and regulations that promote data protection and ethics in the use of technology.

Bibliography

1. Acquisti, Alessandro & Jens Grossklags (2003), *Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior*, UC Berkeley 2nd Annual Workshop on "Economics and Information Security", available at: https://infosecon.net/workshop/downloads/2003/pdf/Final_session6_acquisti.pdf, accessed on 07.05.2025.
2. Baik, Jeeyun (Sophia) (2020), „Data privacy against innovation or against discrimination?: The Case of the California Consumer Privacy Act (CCPA)", *Telematics and Informatics*, Vol. 52, 101431, https://doi.org/10.1016/j.tele.2020.101431.
3. Dienlin, Tobias & Philipp K. Masur, Sabine Trepte (2023). „A longitudinal analysis of the privacy paradox". *New Media & Society*, 25(5), 1043-1064. https://doi.org/10.1177/14614448211016316.
4. Facchini, Alessandro & Alberto Termine (2021), "Towards a taxonomy for the opacity of AI systems," in Vincent C. Müller (ed.), *Philosophy and Theory of Artificial Intelligence (PTAI),* Ed. Cham, CH: Springer International Publishing, 2022, pp. 73–89.
5. Larson, Jeff, Surya Mattu, Lauren Kirchner and Julia Angwin (2016), *How We Analysed the COMPAS Recidivism Algorithm*, https://www.propublica.org/article/how-we-analyzed-the-comp as-recidivism-algorithm.
6. Lavanchy, Maude (2018), *Amazon's sexist hiring algorithm could still be better than a human expecting algorithms to perform perfectly might be asking too much of ourselves*, The Conversation, Lausanne, Switzerland, https://imd.widen.net/view/pdf/z7itobahi6/tc061-18-print.pdf.
7. McCarthy-Jones, Simon (2019) „The Autonomous Mind: The Right to Freedom of Thought in the Twenty-First Century", *Frontiers in Artificial Intelligence,* Vol. 2, https://doi.org/10.3389/frai. 2019.00019.
8. Minkkinen, Matti (2019). „Making the future by using the future: A study on influencing privacy protection rules through anticipatory storylines". *New Media & Society*, 21(4), 984-1005. https://doi.org/10.1177/1461444818817519.
9. Peacock, Anne (2019). *Human rights and the digital divide*. London, Routledge,

https:// doi.org/10.4324/9781351046794.

10. Yeh, Chih-Liang (2018), „Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers", *Telecommunications Policy*, Vol. 42, Issue 4, pp. 282–292, https://doi.org/10.1016/j.telpol.2017.12.001.
11. Zednik, Carlos (2021), "Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence." *Philosophy & Technology* 34, no. 2 (2021): 265+. *Gale Academic OneFile* (accessed July 20, 2025). https://link.gale.com/apps/doc/A666288938/AONE?u=anon~35db595a&sid=googleScholar&xid=374b64c2.