Research Report - 7th Annual Session

General Assembly

Digital privacy and data protection with AI

Forum: General Assembly

Issue: Digital privacy and data protection with AI

Student Officer: Diya Kuriakose

Position: Deputy Chair

Introduction

In today's increasingly modernised and technologized world, digital privacy and data protection have become topics of great concern, especially due to the rise of artificial intelligence (AI) systems which are being used globally. From personalised ads to computerised decision making, AI systems use a large amount of personal data to perform various tasks. These details of personal data are often collected without the users' complete knowledge or consent. While AI continues to develop more innovatively and complexly, not only does it provide more benefits for people to utilise but also raises grave concerns of how personal data is being collected and used by these systems and for whom.

The key to understanding and finding solutions on this issue is recognising how AI systems recognise and collect data,how it is being utilised for its own development, and how that personal data can display more than what users may give consent to. Understanding how various privacy regulations on the online world work, and what they are supposed to provide users better aids countries and organisations to find more solutions and guidelines in their activities in the online world. Furthermore, developed technologies with newer features and more advanced programs are emerging offering solutions in users daily lives for all simple human tasks. The understanding of AI systems and their usage of personal data ensures that these solutions maintain a balance between being innovative, and protecting a user's personal data. With AI being so deeply ingrained in today's society, discussing data protection and digital privacy remains essential to protecting users' rights and promoting a healthy, safe online future.

Definition of Key Terms

Anonymisation

- According to the GDPR, data is anonymous if it is not identifiable in nature, meaning it cannot be identified with any person. When discussing data protection and privacy, non-personal data is often referred to as anonymous data. The term anonymisation is given to the changing of data from becoming personal to unidentifiable and non-personal (PrivacyCompany 2023).

Artificial Intelligence

- Artificial Intelligence (AI) is the term used to refer to computer systems which can perform the same complex tasks which humans can perform. Highly developed artificial intelligence is capable of accomplishing various tasks including reasoning, creating and decision making. While AI tools are capable of a range of tasks, the overarching theme is being able to perform human-like tasks under unsupervised circumstances (May 2024).

Consent

- It is the deliberate, informed and freely given permission to take part in an activity. The concept of consent is identical both online and offline. Consent in the online world includes giving/seeking permission to engage with an activity to happen. Consent in the context of AI includes for example informing individuals if and how their data will be used (Secure Redact London).

Data Protection Impact Assessment

- The Data Protection Impact Assessment (DPIA) is a process designed and used to find any risks on a users privacy or personal data when processing details for a program, such as ones used in many AI programs and bots. For AI systems, using a DPIA ensures that there is a responsible and moral use of data being put in these systems for development. (Milenkoski 2024).

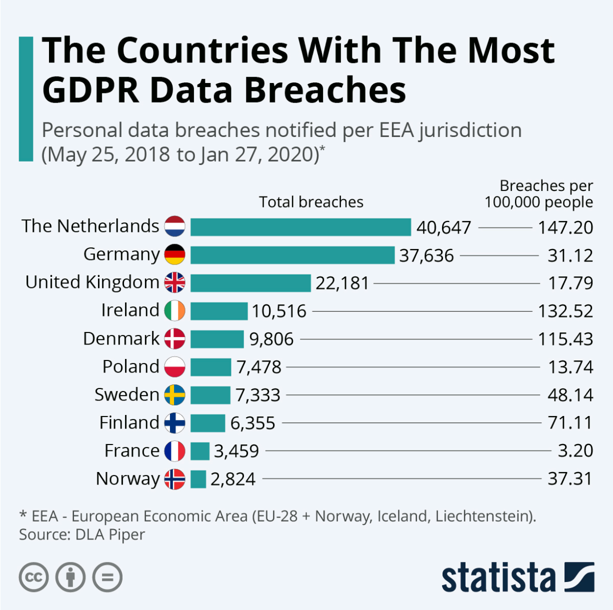
Profiling

- Profiling in the online world refers to specifically collecting details about internet users such as their likes, interests, purchases and locations to create a profile of them. This profile can then be used for various purposes, companies in marketing and AI systems can cater their responses to a user's complex needs. Online profiling has historically been most sophisticatedly used by marketers and companies seeking to inform themselves of their customers and in turn, adapting their marketing strategies (Online Profiling 2025).

General Overview

Data protection and digital privacy has become a crucial matter in question as AI becomes more complex and integrated in society, used for simplifying tasks in retail to social media platforms and digital assistants. AI systems are fed large amounts of personal data, enabling them to fulfill the supposed self-generated responses and actions (Miller 2024). Ethical handling of personal data is essential for the protection of individual's rights, building a transparent online community and confirming agreement with existing privacy laws (A/HRC/56/45: Mapping report: human rights and new and emerging digital technologies 2024).

Data privacy has always been a topic of concern, long before the latest technological advancements of AI. Some of the earliest actions done in protecting individuals digital information and data includes the US Privacy Act of 1974, which prohibited the exposing of data of an individual from a data system without the authorised written consent from the user. Other similar acts included Germany's Federal Data Protection act of 1977, which was later followed by the European Union's Data Protection Directive in 1995. The latter 2 data protection laws are what laid the foundation for the General Data Protection Regulation (GDPR) in 2018, a privacy regulation that is recognised wholly by the European Union (Voss 2025). While specific to the EU, it set global standards to be recognised, emphasising the importance of the protection of individuals rights, such as authorisation, and also highlighted the importance in transparency and responsibility in the usage of personal data.



While the European Union leads in digital privacy regulation, which can be especially seen with their various privacy acts such as the GDPR and the EU AI act which coins the term 'high risk' with AI systems due to their mass reliance on personal data, other regions such as various parts of Africa, and more developed countries such as the US are still introducing and starting to evolve their own data protection laws (Kujawski 2024). The specificity and enforcement behind these developing regulations varies regionally, for example; most less economically developed countries lack data laws specific to AI and instead rely on general data protection acts. Recent times have seen a rise in the creation of regulations surrounding AI and data protection along with more legislation around digital privacy. As mentioned, the EU AI act, passed in 2024 clearly states the requirements for non-negotiable transparency, oversight and the conduction of assessments to identify risks with AI systems, in ensuring that the personal data given is authorised and within all legal and ethical bounds. (Haller 2024.)

The regulation of AI and data protection, as well as digital privacy laws has extensive impacts on individuals, societies and organisations. The impact it has on individuals is the strong rights they will hold on personal data and the minimisation of risks in terms of profiling, discrimination and unlawful monitoring. Societies are also impacted as it forces greater accountability on them to ensure safe and transparent use of AI, and ensure the challenges which come with responsible data use are continuously worked on to prevent harms to others, especially for marginalised and at risk communities. And for the impact on organisations, while their costs will rise for strong programs on digital privacy and complying with regulations, it builds trust and better connection with their customers. As AI systems continue to develop in complexity, so do the ethical and legal regulations and frameworks which protect individuals' data and their privacy, making this a key topic of discussion.

Major Parties Involved

Brazil

Brazil has been working actively in ensuring there is a balance between AI development and data protection for its population. They have already established various acts and agencies which focus on the regulation of personal data and protecting individuals privacy as A furthermore develops. They have enabled the LGPD, General Personal Data Protection Act modelled from the EU and their National Data Protection Authority works actively to develop regulations specific to AI focussing on transparency within these AI systems in terms of personal data (ALERT 2024). Further legislative efforts also took place in 2024, with bills passed on obligations AI developers must take.

China

China has a strict control of all personal data being used both regularly and in AI systems. They have effectively added data privacy laws such as the Personal Information Privacy Law (PPIL) and have a robust overview of personal data and AI. China emphasises the importance of governments having access to this personal data, and the personal data along with AI development is closely monitored to ensure it aligns with national security beliefs (Tobin 2024).

Germany

Germany, like all members of the European Union, enforces the GDPR which is arguably one of the tightest data protection regulations which must be complied to. Germany being a highly developed technological state, focusses that all their AI systems fulfil the GDPR, including transparency regarding the processes of the AI systems and minimisation of data usage. Furthermore, Germany has been a vocal leader in promoting individuals rights and a legal usage of AI with appropriate privacy regulations.

Japan

Japan is a vocal leader of Asia in advocating for an ethical and responsible development of AI, prioritising transparency and public knowledge on the processes of AI systems while still heavily emphasising the importance of innovation and development of AI to benefit consumers. Japan has made it clear that the development of AI is crucial to today's society but in regulation of legal laws. This includes Japan's Act on the Protection of Personal Information (APPI) which focuses on the controlling of data privacy and recently had amendments made to emphasise the boundaries AI systems must hold themselves to (Tobin 2024).

New Zealand

New Zealand is one of the modern countries which have been updating its legislative frameworks in addressing the new challenges AI has been posing, with its more complex developments such as artificial decision-making and transparency. New Zealand's Privacy Act of 2020 sets out clear regulations about the collection, analysing, usage and sharing of personal data in various AI systems. This law they established emphasises their stance on protecting individuals' rights to privacy and keeping them safe digitally (Tobin 2024).

USA

The USA does not have any federal laws about digital privacy on data but it does have regulations which are for given industries and sectors. This includes privacy laws such as the California Consumer Protection Act (CCPA) and the Health Insurance Portability and Accountability

Act (HIPAA) which focuses on the protection of data and personal details of individuals under certain sectors. The regulation of AI systems is still an ongoing debate, with more action being urged for national expectations in terms of data protection under AI. The Federal Trade Commission (FTC) and other agencies continue to criticise AI systems for the protected privacy of consumers (Moskaleva 2024).

Timeline of Key Events

Timeline of events in reverse chronological order leading up to present day.

Date	**Description of Event**
UN enacts South Korean- and Dutch Resolution on AI in the military (November 2024):	**Event 5-** The first resolution regarding AI in the military has been taken into effect by the UN which was led by the Netherlands and South Korea. The resolution calls member states for international discussions and global agreements on the usage of AI responsibly, in various military contexts.
UNGA passes the first Global AI Resolution (March 2024):	**Event 4-** The UN General Assembly has adopted the first global resolution on AI which was co-sponsored by China and the USA with another 120 countries. The resolution focuses on the digital divide which has been made and also the protection of personal data and digital rights in AI systems.
UN Secretary General's Policy Brief (May 2023):	**Event 3-** A policy brief was released by the UN-Secretary General highlighting specific sectors needed to be worked on or global cooperation in the digital world. The policy brief also discussed the importance of collectively ensuring the protection of data in AI.
UNDP launch of 'Digital for Sustainable Development' act (2023)	**Event 2-** The UNDP's Bureau of Arab States launched an initiative called the Digital for Sustainable Development (D4SD) in 2023 which focussed on using various online and digital tools and also AI to further progress in reaching the Sustainable Development Goals, while emphasising the importance of a responsible and legal use of AI.
OHCHR release of reports on privacy about the online world.	**Event 1-** The Office of the United Nations High Commissioner for Human Rights (OHCHR) worked throughout the year on releasing reports in further understanding the difficulty of keeping the protection of individuals rights. The reports provided possible solutions which

could be done providing various suggestions of legal structures to uphold people's rights while developing and consuming AI systems.

Previous Attempts to Resolve the Issue

- Adopting the first official resolution in March 2024, the United Nations General Assembly unanimously agreed upon the first global resolution which called to protect personal data and control AI systems usage and collecting of AI systems.

- Releasing the EU's GDPR, which is the official proactive stance of how AI should be responsible and the personal data should be kept and worked with careful ethical consideration.

- The G7's adoption of the Guiding Principles on AI and a Code of Conduct regarding AI, which was signed optionally by all nations who were willing, emphasising the importance of transparency and ethicalness in the development of AI.

- The Data Free Flow with Trust (DFFT) initiative mentioned at the G20 summit in Osaka in 209, which was further explored by the G20 nations, looked for finding a fair border between allowing data to be worked with but still having strong privacy protections and rules set.

- The OECD's AI principles, which was last updated in 2024, was signed by 46 countries and highlighted the need of global aid and digital privacy being protected in the various AI systems being used.

Possible Solutions

- Developing through international cooperation, more mandatory principles for all AI systems to follow in terms of privacy and ensure all ethical aspects are integrated in those principles ensuring no violation of digital privacy.

- Making it obligatory for all organisations to establish their own policies and regulations in terms of data privacy, with different organisations choosing to limit or expand how they use the data within all legal bounds.

- Strongly encouraging the utilisation of Data Protection Impact Assessments (DPIAs) when using and developing AI systems which are at high risk of violating privacy risks, to ensure only authorised and legal AI systems become available to users.

- Minimising the collection and amount of personal data which is being used for AI systems and using exactly the necessary data required for AI systems which help it function.

- A routine review of AI systems and the personal data that is being collected, along with removing any unwanted or extra personal data. The review could also lead to more adaptations of the AI systems to ensure that no malicious activity occurs.

Appendices

Appendix A: World Map of Regions Focussing on AI Privacy Regulations

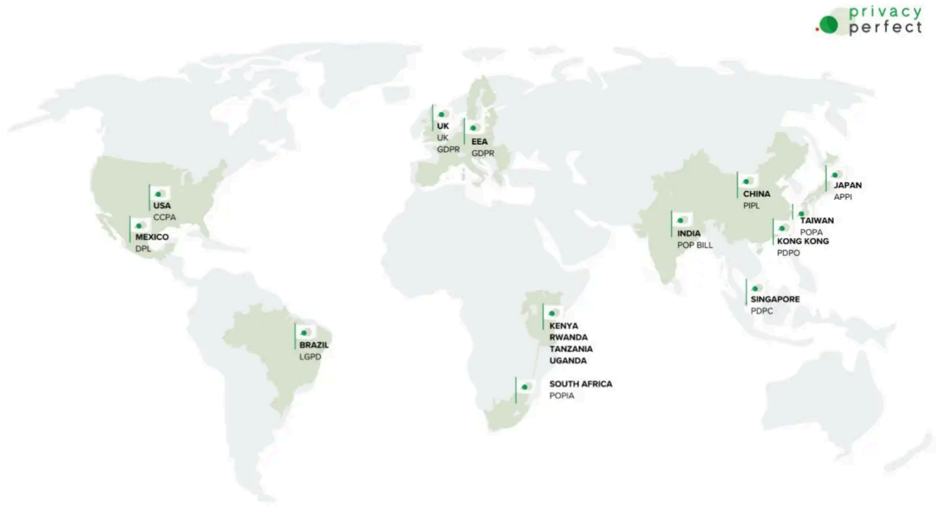


Diagram 1, shows nations in the world where orders are being passed for stronger AI Privacy regulations.

Bibliography

"A/HRC/56/45: Mapping report: human rights and new and emerging digital technologies - Report of the Office of the United Nations High Commissioner for Human Rights." *United Nations Human Rights Office of the High Commissions*, 20 Aug. 2024, www.ohchr.org/en/documents/thematic-reports/ahrc5645-mapping-report-human-rights-and-new-and-emerging-digital. Accessed 30 Apr. 2025.

ALERT. "Brazil's Digital Policy in 2025: AI, Cloud, Cyber, Data Centers, and Social Media." *COVINGTON*, 18 Feb. 2025, www.cov.com/en/news-and-insights/insights/2025/02/brazils-digital-policy-in-2025-ai-cloud-cyber-data-centers-and-social-media. Accessed 30 Apr. 2025.

Haller, Drew. "Furthering a rights-based digital agenda at the United Nations General Assembly and the Summit of the Future." *Research ICT Africa*, 19 Sept. 2024, researchictafrica.net/2024/09/19/furthering-a-rights-based-digital-agenda-at-the-united-nations-general-assembly-and-the-summit-of-the-future/. Accessed 30 Apr. 2025.

Kujawski, Fabio. "Brazilian Data Protection Authority opens public consultation on data protection and AI." *mattosfilho.com*, 13 Nov. 2024, www.mattosfilho.com.br/en/unico/consultation-data-protection-ai/. Accessed 30 Apr. 2025.

May, Kelley. "What is Artificial Intelligence?" *NASA*, 13 May 2024, www.nasa.gov/what-is-artificial-intelligence/. Accessed 30 Apr. 2025.

Milenkoski, Marin. "Conducting a DPIA: Best Practices for AI Systems." *GDPRLocal*, 17 Oct. 2024, gdprlocal.com/conducting-a-dpia-best-practices-for-ai-systems/#:~:text=It%27s%20a%20process%20that%20helps,and%20ethical%20use%20of%20data. Accessed 30 Apr. 2025.

Miller, Katharine. "Privacy in an AI Era: How Do We Protect Our Personal Information?" *HAI Stanford*, Stanford, 18 Mar. 2024, hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information. Accessed 14 Apr. 2025.

Moskaleva, Natalia. "A Brief History of Privacy." *criipto.com*, CRIIPTO, 18 Dec. 2024, www.criipto.com/blog/history-of-privacy. Accessed 30 Apr. 2025.

"Online Profiling." *Gale E-Commerce Sourcebook*, Encyclopedia.com, 26 Mar. 2025, www.encyclopedia.com/books/educational-magazines/online-profiling. Accessed 30 Apr. 2025.

PrivacyCompany. "What are the Differences Between Anonymisation and Pseudonymisation." *Privacy Company EU*, 6 Mar. 2023, www.privacycompany.eu/blog/what-are-the-differences-between-anonymisation-and-pseudonymisation. Accessed 30 Apr. 2025.

Secure Redact London. "Is consent being prioritized in AI training?" *SecureRedact*, Pimloc, www.secureredact.ai/articles/is-consent-being-prioritized-in-ai-training. Accessed 30 Apr. 2025.

Tobin, Donal. "What is Data Privacy—and Why Is It Important?" *Integrate.io*, 21 Dec. 2024, www.integrate.io/blog/what-is-data-privacy-why-is-it-important/. Accessed 30 Apr. 2025.

Voss, Gregory. "Europe and cyberspace – Data protection." *Ehne.fr*, ehne.fr/en/encyclopedia/themes/material-civilization/digital-europe/europe-and-cyberspace—-data-protection. Accessed 30 Apr. 2025.