Journal of Politics and Ethics in New Technologies and AI

Vol 2, No 1 (2023)

Journal of Politics and Ethics in New Technologies and AI

Balancing ChatGPT and Data Protection in Germany: Challenges and Opportunities for Policy Makers

Fouad Leboukh, Emmanuel Baba Aduku, Omar Ali

doi: 10.12681/jpentai.35166

Journal of Politics and Ethics in New Technologies and AI
Volume 2, Issue 1 (2023)
e-ISSN: 2944-9243

https://doi.org/10.12681/jpentai.35166

RESEARCH ARTICLE

Balancing ChatGPT and Data Protection in Germany: Challenges and Opportunities for Policy Makers

Fouad Leboukh
Willy Brandt School of Public Policy, University of Erfurt, Germany.

Emmanuel Baba Aduku
Willy Brandt School of Public Policy, University of Erfurt, Germany.

Omar Ali
Willy Brandt School of Public Policy, University of Erfurt, Germany.

Abstract

In the last few months there has been widespread discussion about the remarkable progress made in the field of artificial intelligence, specifically large language models such as "ChatGPT". The ethical implications of AI, particularly concerning data protection, have sparked discussions on the necessity of robust regulations. This article examines the intersection of data protection, ChatGPT, and the ethics of AI, it explores Germany's ongoing efforts to strike a balance between harnessing the potential of large language models as ChatGPT and ensuring responsible and transparent use of AI technology in the policy-making realm. The GDPR serves as a guiding framework, necessitating careful consideration of privacy rights and secure handling of personal data when deploying ChatGPT in Germany's policy-making processes. The study draws on analysis on the current laws and regulations of data protection in Germany while studying Germany's commitment to safeguarding personal information through the active presence of The German Federal Commissioner for Data Protection and Freedom of Information. The first section provides a context and presents the policy problem. The second section looks at the available policy options on the role of policymaking in establishing comprehensive regulations regarding the use of ChatGPT and generative AI. The third section provides recommendations on how Germany can ensure the responsible management of ChatGPT, through strengthening data protection laws and regulations, simultaneously, restricting ChatGPT usage to private users and government, also, embracing appropriate usage of generative AI while developing ethical guidelines and best practices to harness its benefits, fostering innovation and advancement.

Keywords: Artificial Intelligence, ChatGPT, Privacy, Data Protection, Germany, Ethics of AI, Regulations, GDPR, Policy Making

Introduction

In the last few months there has been widespread discussion about the remarkable progress made in the field of artificial intelligence, specifically an application known as "ChatGPT". This privately owned application is created by Open AI, a company supported by Microsoft, and has the ability to

Leboukh, F., Baba Aduku, E., & Ali, O. (2023). Balancing ChatGPT and Data Protection in Germany: Challenges and Opportunities for Policy Makers. *Journal of Politics and Ethics in New Technologies and AI*, *2*(1), e35166. https://doi.org/10.12681/jpentai.35166

generate a diverse range of content such as articles, construction topics, jokes, and poetry as per the user's request. Similar to the previous ChatGPT, the large language models (LLMs) have sparked a sophisticated academic discussion regarding their moral ramifications for years (Gordijn & Have, 2023). Technology experts, including Elon Musk, called for a temporary halt to the development of "artificial intelligence" (Chee & Supantha, 2023). EU Industry Commissioner Thierry Breton proposed new AI rules aim to address concerns about the risks of using ChatGPT and AI technology. This was the first comment issued by a senior official in Brussels regarding the application, which was classified just two months after its launch as the fastest growing consumer application in history (Chee & Supantha, 2023). The EU Commissioner for Industry stresses that there can be benefits to this development in artificial intelligence, but there is an urgent need to keep pace with this development, therefore there is a call for strong regulatory framework to ensure the protection and the privacy of data.

This policy brief examines the intersection of data protection, ChatGPT, and the ethics of AI. Focusing on Germany's commitment to data protection, the brief addresses the challenges and opportunities associated with integrating ChatGPT within the framework of ethical AI practices and existing regulations such as the General Data Protection Regulation GDPR. The ethical implications surrounding AI technologies, particularly with regard to privacy, require robust regulations to ensure the responsible and transparent use of ChatGPT.

In the wake of the ChatGPT's launch, a wave of scrutiny has swept across several European countries, prompting them to closely examine the implications of this novel technology. Italy, being at the forefront, took decisive action by imposing a ban on its utilization by its agency The Italian Data Protection Authority. As a result, experts predict that other prominent European Union nations, such as France and Germany, may follow suit in implementing comparable regulations and restrictions (Browne, 2023). As Germany emerged as a leading nation in the realm of personal data protection, showcasing active involvement in this field in recent years, through its agency The German Federal Commissioner for Data Protection and Freedom of Information. Despite Germany's well-established culture of privacy and data protection, the country has yet to take decisive action concerning ChatGPT. The impact of ChatGPT on users' privacy in Germany is currently a subject of extensive deliberation and analysis. Given Germany's commitment to safeguarding personal information, it becomes crucial for the nation to effectively navigate the challenges posed by this emerging technology. The coming section of this policy brief presents available policy options and policy relevance on the role of policymaking in establishing comprehensive regulations regarding the use of ChatGPT and generative

AI. The last section provides recommendations on how Germany can ensure the responsible management and transparency of ChatGPT.

To address these concerns, policymakers in Germany represented in The German Federal Commission for Data Protection and Freedom of Information have to actively assess the impact of ChatGPT on user's privacy and consider the development of guidelines and frameworks to promote responsible usage. Striking a balance between leveraging the benefits of AI-generated language and upholding democratic principles is a crucial aspect of shaping the future landscape of policymaking. It requires ongoing research, a collaboration between stakeholders, and the establishment of transparent standards to ensure that ChatGPT contributes positively to users' data while mitigating potential risks.

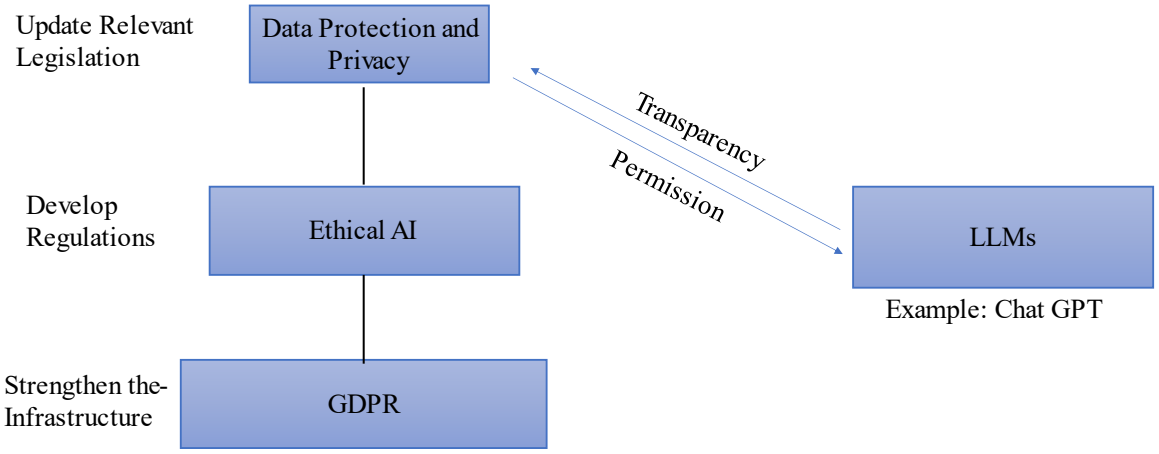
Options for Policy Makers

Having discussed the context and the policy problem in the preceding section, we present the policy option that policy makers in Germany can consider when thinking about how to balance generative artificial intelligence such as ChatGPT. These options include, but are not limited to, updating relevant legislation, restricting generative AI use for government business in the interim, and developing ethical guidelines for generative AI use. We will discuss these options in detail.

Update Relevant Legislation to Regulate Generative Artificial Intelligence

Given the uncertainty around generative artificial intelligence that has produced the likes of ChatGPT, updating the relevant European Union and German legislation becomes pertinent. Once again, the EU is at the forefront of legislation to regulate artificial intelligence (Iyengar, 2023). However, the current Artificial Intelligence (AI) Act being developed by the European Union was conceived when large language models (LLMs), such as the likes of ChatGPT and other models, had not emerged. In regulating artificial intelligence, the generative nature of large language models and the uncertainty around which trajectory these LLMs can take remains a crucial issue for protecting data and privacy in Germany. Policy makers in the European Union and Germany should view updating legislation and regulations as a continuous process rather than a static one as these policy instruments struggle to keep pace with artificial intelligence and technology in general (Iyengar, 2023). Will policymakers adopt a voluntary or binding approach to compliance in relation to artificial intelligence? Perhaps policymakers can adopt a triangulation of the three approaches even though Germany´s political economy as a corporatist market economy favors a binding approach as this is most relevant to Germany´s historical and contemporary context.

Fig. 1



Framework Explaining the Interrelationship between Data Protection and LLMs such as ChatGPT (The Authors, 2023)

The figure presented above illustrates the utilization of the General Data Protection Regulation (GDPR) framework as a key reference for policymakers. By leveraging the GDPR framework, policymakers can establish a dedicated component for ethical Artificial Intelligence (AI) and seamlessly integrate it into the process of updating legislation and regulations. This is particularly important for governing AI software that interacts with user data. This approach ensures that AI technologies namely Large Language Models like ChatGPT operate within the boundaries of data protection regulations, fostering transparency, accountability, and the responsible use of user data in the context of Artificial Intelligence.

Restrict ChatGPT Away from Government Business

As generative artificial intelligence is a novel and rapidly expanding phenomenon, one of the options policy makers in Germany can adopt is to restrict the use of generative AI for government business. The public sector, by virtue of its role in public good production and public service delivery handles a large trove of citizen data. To be sure, generative AI can enhance the public sector through it many potential uses such as chatbots for responding to citizen requests, facilitating decision making by public servants, and document or text analysis (Council of the European Union, 2023). The protection of such data is a national security issue in this age when information and communications technology has become critical infrastructure. Therefore, the need to restrict the use of generative AI for a period becomes important. This is to enable The German Federal Commissioner for Data Protection and

Freedom of Information study the phenomenon to decide how to contextualize the use of generative AI in government business, most importantly how to protect citizen data.

Develop Ethical Guidelines and Best Practices for ChatGPT Use in Germany

Large language models that give rise to the likes of ChatGPT come with immense positive and negative impacts for human society. Already, the issue of discrimination has been highlighted in the early AI tools developed. This presents policy makers in Germany with the option of developing ethical guidelines and best practices for the use of generative AI. The presence of ethical guidelines should not replace the need for legislation but can be an instrument for driving voluntary compliance (Mittelstadt, 2019). Under such an arrangement, AI companies and other stakeholders operating in Germany and the wider European Union will agree to a set of principles that shape how they develop and deploy AI tools in various sectors. It is important that such guidelines combine general and sector-specific principles to consider the contextual issues in various sectors and how they play out. These principles will set the stage for the long-term governance of generative AI in Germany.

Policy Recommendations

Strengthen data protection through updating laws and regulations

The right to privacy, which is crucial for safeguarding human dignity, independence, and self-determination, must be upheld, shielded, and advanced at every stage of AI system development. It is imperative that data collection, usage, sharing, storage, and deletion for AI systems adhere to international laws and align with ethical values and principles while respecting applicable national, regional, and global legal frameworks. To this end, a multi-stakeholder approach must be adopted to establish robust data protection frameworks and governance mechanisms at the national or international level, to ensure compliance throughout the AI system lifecycle (UNESCO, 2021). As a result, it is strongly advised that The German Federal Commissioner for Data Protection and Freedom of Information ensures the safeguarding of citizens' data by implementing laws and regulations that uphold their rights. This can be achieved by drawing on the expertise of other nations, for instance, The Canadian government has enforced the Personal Information Protection and Electronic Documents Act (PIPEDA), a national statute that governs the gathering, utilization, and revelation of personal data by privately owned companies. The responsibility of ensuring compliance with PIPEDA falls under the Office of the Privacy Commissioner (OPC), which carries out investigations into complaints, performs audits, and initiates legal proceedings under federal legislation (Walters, 2019). On the other hand, The Privacy Act of Australia governs the processing of personal information by both government and private sector organizations. The Privacy Act contains 13 Australian Privacy

Principles (APPs), which establish guidelines for acquiring, using, and disclosing personal information (Burdon & Telford, 2010).

Japan also has enacted the Protection of Personal Information (APPI) Act, which governs the processing of personal information by both government and private sector organizations. The APPI includes laws on the acquisition, use, and disclosure of personal information and provisions on persons' rights to access and amends their personal information (Hoffmann, 2022). All these rules and regulations from other countries experiences play an important part in protecting citizens' data, and it is the first step for the German authority to get out of this bind, which is data protection.

Restrict ChatGPT usage to private users, not public

To tackle worries related to safeguarding data, it might be wise to contemplate limiting the availability of ChatGPT solely to individual users instead of making it accessible to the masses. This can be accomplished by enforcing specific protocols, like mandating users to sign up and authenticate their identity, and constraining the categories of information that can be fed into the platform (Whitman & Mattord, 2022). By restricting entry using this method, it could potentially diminish the possibility of unapproved entrance to confidential individual data, whilst simultaneously permitting individual users to reap the advantages of ChatGPT's sophisticated linguistic capabilities (Nissenbaum, 2010).

Numerous instances exist where countries have enforced measures to control the usage of chatbots and language processing systems akin to ChatGPT for private users, aiming to safeguard sensitive data. For example, in Canada, the OPC has provided direction on chatbot usage, stressing the significance of honesty, agreement, and data reduction. The OPC advised that businesses restrict chatbot usage to authorized individuals and that they guarantee that private information is only obtained as required for the chatbot's purpose (Office of the Privacy Commissioner of Canada, 2021).

By enforcing strategies like mandating user registration, acquiring explicit approval, and constraining data gathering to only what is essential for the chatbot's purpose, it is feasible to strike a balance between the advantages of sophisticated language processing abilities and the requirement for data security. Therefore, it is strongly advised that The German Federal Commissioner for Data Protection and Freedom of Information take advantage of the expertise of these nations and opt for the strategy that is appropriate for safeguarding and securing the data of its citizens.

Developing ethical guidelines and best practices for development

When crafting ethical standards and optimal methodologies for the advancement of ChatGPT in Germany, it could prove beneficial to reference the insights and knowledge gained from comparable

policies and nations. Engaging a diverse group of stakeholders in the creation process is imperative, encompassing scholars from academia, professionals from industry, and members of civil society, alongside representatives from impacted communities. Several organizations have taken the initiative to formulate ethical codes and optimal methodologies for the creation of technologies such as ChatGPT. The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems has devised a series of ethical protocols for autonomous and intelligent systems. Moreover, the Partnership on AI, which is an alliance of technology corporations and advocacy groups, has also created a set of top practices for AI development (Aldinhas Ferreira et al., 2019).

The Automated Decision-Making Directive of Canada mandates that federal agencies of Canada guarantee transparency, responsibility, and adherence to Canadian privacy laws in their utilization of artificial intelligence. Additionally, the directive mandates that agencies perform evaluations of the probable effects of their AI systems on human rights, encompassing privacy and non-bias (Nalbandian, 2022). As a result, it is strongly urged that the German Federal Commissioner for Data Protection and Freedom of Information leverage the knowledge of these countries to adopt highly ethical guidelines for preserving its citizens' data.

Conclusions

In conclusion, the deployment of ChatGPT technology in Germany necessitates a strong emphasis on data security and privacy. The development of robust regulations and ethical norms and best practices are crucial steps to ensure the responsible and protective integration of this technology. By implementing and adhering to rigorous regulatory frameworks, Germany can effectively address the challenges associated with ChatGPT while safeguarding individuals' privacy rights.The potential of ChatGPT technology is undoubtedly intriguing, but its utilization must be guided by the principles of data protection and privacy. Germany's commitment to these values, coupled with the establishment of comprehensive regulations and guidelines, will play a vital role in shaping the responsible deployment of ChatGPT. Striking a balance between technological advancements and individual rights is paramount.

To navigate the complexities surrounding ChatGPT, ongoing dialogue, and collaboration among policymakers, stakeholders, and industry experts will be essential. By fostering a proactive and cooperative approach, Germany can seize the opportunities presented by ChatGPT while safeguarding personal data and ensuring that ethical considerations remain at the forefront. With a strong focus on data security and privacy, Germany can effectively harness the potential of ChatGPT technology for the benefit of its citizens while upholding their fundamental rights.

References

Aldinhas Ferreira, M. I., Silva Sequeira, J., Singh Virk, G., Tokhi, M. O., & E. Kadar, E. (Eds.). (2019). *Robotics and Well-Being* (Vol. 95). Springer International Publishing. https://doi.org/10.1007/978-3-030-12524-0

Browne, R. (2023, April 4). Italy became the first Western country to ban ChatGPT. Here's what other countries are doing. *CNBC*. https://www.cnbc.com/2023/04/04/italy-has-banned-chatgpt-heres-what-other-countries-are-doing.html

Burdon, M., & Telford, P. (2010). The Conceptual Basis of Personal Information in Australian Privacy Law. *Murdoch University Electronic Law Journal*, *17*(1), 1–27.

Chee, F. Y., & Supantha, M. (2023, March 2). ChatGPT in spotlight as EU's Breton bats for tougher AI rules. *Reuters*. https://www.reuters.com/technology/eus-breton-warns-chatgpt-risks-ai-rules-seek-tackle-concerns-2023-02-03/

Council of the European Union. (2023). *ChatGPT in the Public Sector-Overhyped or Overlooked?* Analysis and Research Team (ART). https://www.consilium.europa.eu/media/63818/art-paper-chatgpt-in-the-public-sector-overhyped-or-overlooked-24-april-2023_ext.pdf

Gordijn, B., & Have, H. ten. (2023). ChatGPT: Evolution or revolution? *Medicine, Health Care and Philosophy*, *26*(1), 1–2. https://doi.org/10.1007/s11019-023-10136-0

Hoffmann, T. (2022). Data Protection by Definition – Report on the Law of Data Disclosure in Japan. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4055510

Iyengar, R. (2023). *The Global Race to Regulate AI*. Foreign Policy. https://foreignpolicy.com/2023/05/05/eu-ai-act-us-china-regulation-artificial-intelligence-chatgpt/?utm_medium=email&_hsmi=257909296&_hsenc=p2ANqtz-_fZbx6uEwgsagflVRJWPw9EHm9oTBE1vukvI7VPXDSRApFmzUPLDJJ3kFGEptj_EqUdzefnXaW7t4P4maXdz-z130UoA&utm_content=257909296&utm_source=hs_email

Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, *1*(11), 501–507. https://doi.org/10.1038/s42256-019-0114-4

Nalbandian, L. (2022). Increasing the accountability of automated decision-making systems: An assessment of the automated decision-making system introduced in Canada's temporary resident visa immigration stream. *Journal of Responsible Technology*, *10*, 100023. https://doi.org/10.1016/j.jrt.2021.100023

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books, an imprit of Standford University Press.

Office of the Privacy Commissioner of Canada. (2021). *Guidelines for obtaining meaningful consent*. https://priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/

UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*. Unesco. https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

Walters, N. (2019). *Privacy Law Issues in Blockchains: An Analysis of PIPEDA, the GDPR, and Proposals for Compliance*. https://ssrn.com/abstract=3481701

Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (Seventh edition). Cengage.