International Journal for Scientific Research (IJSR)

IJSR

المجلة الدولية للبحوث العلمية

Vol. (3), No. (3)

March 2024

الإصدار (3)، العدد (3)

An Overview of AI Data Protection in the Context of Saudi Arabia

Reema Bakheet Alzahrani

Master of Commercial Law, Prince Sultan University, Riyadh, Kingdom of Saudi Arabia

reemafz7@hotmail.com

Abstract

The Personal Data Protection Law in Saudi Arabia aims to protect individuals' data and regulate businesses that collect, retain, analyze, process, and share it across borders around the globe. Artificial intelligence and data protection are interconnected concepts since AI uses data sets to make decisions and perform activities. However, ethical questions about personal data use and potential bias in AI persist in the present AI environment. Therefore, while AI has led to digital transformation in sectors like transportation, healthcare, and finance, the technology has privacy implications that limit its usage by many organizations.

In the country's journey to reduce its oil dependency and become modernized, it is significant for Saudi Arabia to have a sufficient set of regulations and laws to deal with AI-related legal challenges. In this regard, the authorities have initiated programs to streamline the KSA's data protection laws with European AI regulations and data safety laws after recognizing the need to preserve data sets. This paper examines the present laws and legal regulatory framework for AI and data protection in Saudi Arabia and the legal challenges to protecting data in AI. The paper also discusses legal issues related to AI data protection and the barriers that restrict data protection law reform in light of the available literature on AI data protection. After examining the present data protection measures in the KSA, the paper gives recommendations for improving the overall AI data protection laws and regulations in the kingdom.

Keywords: Artificial Intelligence, Data Protection, Saudi Arabia, Legal Challenges, Regulations.

1. Introduction

The world has transformed with the rapid advancements in digital technologies, particularly AI. Artificial intelligence has created unimaginable and unprecedented solutions for human convenience. However, while AI has certainly eased certain aspects of human living and routine, the technology has raised ethical and legal questions about personal data use and potential bias. In this regard, organizations that adopt AI technology must ensure adequate human oversight and consider the potential impact of AI systems on individuals and corporations. AI is defined as a technology that enables computers and machines to impersonate human intelligence and problem-solving abilities (IBM, 2024). AI, often associated with machine learning, deep learning, and artificial neural networks, is a system capable of solving complex problems and achieving specific goals (Chikhaoui et al., 2022). The rapid growth of artificial intelligence is attributed to daily data production and computing power. Of note, AI applications have been adopted in different key sectors such as transportation, education, healthcare, banking, and finance (Al-Baity, 2023). The drastic emergence and spread of AI technology across the world has caused AI and data protection to become intertwined concepts as the need to regulate the technology arises.

Artificial intelligence is driving the Fourth Industrial Revolution due to the technological potential of AI systems and the vast availability of data in the globalised world thus raising concerns about data safety. AI research is now driven by economic and social demands, reaching the average user through cheap computational power and connectivity. As the technology becomes accessible to everyone, it has enabled the use of AI applications for persistent monitoring and adaptation. However, the widespread use of AI to improve user services has raised legal concerns about privacy and security implications due to the need for user data (Meurisch & Mühlhäuser, 2021). AI applications with capabilities like generating imagery, speech, text, language, and synthetic data can learn the user’s interests and goals to serve their needs. AI can also provide predictive machine learning models, reduce human bias, and augment decision making through probabilistic reasoning and data discerning (Mitrou, 2018). Therefore, the capability of AI systems to access, use, and learn from personal data necessitates the implementation of a robust regulation system to prevent data misuse (Albakjaji, & Almarzoqi, 2022). Importantly, to simplify the regulation of generative AI models, the purpose limitation principle must be applied to AI to define the purpose of the models. If the purpose of an AI model is not narrowed down, issues can arise such as the inability to explain the need for certain types of personal data. It is clear that while AI technology is bound to positively transform the world, the development of new AI tools and services should be in compliance with existing data protection and AI regulation principles to ensure that user data is protected.

In the case of AI regulation in the Kingdom of Saudi Arabia (KSA), the increasing debate surrounding intellectual property laws and the challenges faced by existing legal frameworks have caused the country to streamline the legal aspects that govern AI and related innovations. To chart a path forward in AI regulation, legislators and other stakeholders in the KSA have examined and compared national, regional, and cultural concepts of privacy and data protection to understand the similarities and differences between central, national, and international laws (Bygrave, 2010). For instance, European law such as the General Data Protection Regulation (GDPR) is increasingly recognizing data protection as a distinct set of rights from traditional privacy or private life rights (Andrews, 2024). Further, to ensure that companies use AI technology in a trustworthy manner, AI regulations in the European Union (EU) emphasize accountability and compliance with the accuracy principle. By comparing data protection regulations in Saudi Arabia with laws from other regions, the KSA can create an AI environment that provides transparency to users (Albakjaji & Almarzoqi, 2022). Of note, providing clarity, transparency, and appropriate consideration during the development and application of AI models can allow companies to build consumer trust.

Despite the ease of use and benefits of AI, the issue of data safety arises when using the technology since AI service developers rely on vast amounts of data from organizations, individuals, and states to train AI models. As expected, the rise of AI has significantly impacted privacy rights by allowing organizations to collect, store, and process vast amounts of data at unprecedented rates. From a legal perspective, the capability of AI to gather sensitive information not only raises questions about transparency, but it can also compromise privacy rights in predictive analytics (Nagar, 2023). Therefore, data protection principles, including data security, availability, and access control, are important in the present day to address the issue of rapid digital transformation. For individuals and organizations, failure to protect data can lead to financial losses, reputational damage, and legal liability. Data protection also has a crucial role for organizations to safeguard sensitive data, prevent corruption, loss or damage, and ensure accessibility, reliability, and trust in data-centric operations. Notably, as the public perception of artificial intelligence shifts from exceptional to normal with certain capabilities becoming routine technology, the government has a responsibility to reinforce data protection, safety, and privacy laws to protect its citizens.

This paper addresses the relationship between artificial intelligence and data protection since the issue has become extremely significant for organizations, individuals, and groups. The relationship between the aforementioned concepts is understood by discussing the legal challenges facing data protection efforts in the current artificial intelligence era. The core of the discussion is the regulatory framework for artificial intelligence and data protection in Saudi Arabia. Since the country is a hub for tourists from all over the world, the KSA should prioritize strengthening its regulatory framework for AI-based applications to protect the personal data of both tourists and citizens. Due to the significance of AI technology to the economy of Saudi Arabia, it is important to form and implement laws and regulations that govern the transfer of personal data and protect sensitive or important data sets.

2. Literature Review

The rapid global interconnectivity has transformed the movement and transfer of information and data. Web- or computer-based global interconnectivity has led to the creation of intimate data sets that can track movements (Saad, 1981). In the present era, artificial intelligence privacy is a fundamental right that requires ethical, jurisdictional, and sociological considerations. In this regard, communication and AI-based processing technologies have altered perceptions by necessitating further ethical, legal, and sociological responses that are majorly associated with data protection (Alsulaiman & Alrodhan, 2014). According to Bygrave (2010), the GDPR specifies that protecting personal data from unauthorised disclosure is a fundamental right that all individuals should possess. As the use of AI technology expands, it is important to develop legal measures that prevent the unauthorised disclosure of personal data since it can negatively impact the health, safety, and identity of individuals at a global level. To safeguard the data, organizations and corporations not only have to adopt a set of internal data protection measures, but they also have to comply with legislation that governs the use of AI (Hammad & Al-Mehdar Law Firm, 2024). At the state level, authorities also have to implement data protection policies since AI-based applications are equally utilized by state agencies for economic prosperity in the Saudi Kingdom. For this reason, safeguarding data in the current era of rapid information technology evolution is a fundamental issue at the individual, organizational, and state levels.

Since AI can both threaten and strengthen data protection, efforts to address the challenges posed by the technology are crucial to eliminating potential AI adoption risks. The conflict or gap between existing laws and AI can result in data safety breaches and threaten data protection. Cate and Dockery (2018) highlight that since AI technology is used by companies to fulfill sensitive roles such as monitoring data usage, developing privacy tools, and analyzing policies, data protection laws must be improved to protect privacy and avoid creating bureaucratic barriers. Notably, AI data protection pertains to two types of data: the personal data of individuals and non-personal data. Depending on the form of the data, the legal, social, and economic impact on individuals varies greatly in the case of data violation or misuse. Due to its importance, the legal challenges tied to personal data are not only more sensitive but should also be addressed with care.

With the rapid advances in the fields of IT and AI, data protection has become a mainstream approach to privacy regulation. In 2020, around 142 new laws were enforced to secure the safety and protection of data. These omnibus-style frameworks, mostly applied outside of Europe and the United States, cover a greater scope of data practices and emphasize individual dignity. However, the abstract nature of these frameworks presents challenges in defining concepts like personal data (Gstrein & Beaulieu, 2022). Despite the challenges, it is still important for courts and individual authorities to enforce data protection rules and provisions in an effective manner to strengthen the protection of personal data.

3. AI &Saudi Vision 2030

With the aim of moving away from its reliance on oil, Saudi Arabia's government has supported digital transformation through the Saudi Vision 2030 Plan which includes embracing advanced technologies and expressing the country's cultural and religious heritage through different mega projects. Of note, government services including e-government are majorly influenced by recent developments in the Saudi 2030 Vision as well as the needs of pilgrims (Alharbi et al., 2021). Regarding artificial intelligence, Saudi Arabia's Vision 2030 plans highlight the country's goal to be a regional and global leader in AI and other technologies (Radwan, 2023). The country has greatly invested in advanced technology firms that serve both citizens and the large number of foreigners entering the country. KSA aims to transform into an information society and digital economy by increasing productivity and providing IT services for all sectors.

While Saudi Arabia also plans to diversify its economy by greatly investing in AI projects to improve different sectors, the nation is grappling with legal and ethical issues regarding AI and data protection. For this reason, the KSA has embraced data protection regulations under the National Vision 2030 to enhance the government's effectiveness in controlling AI development and protecting data (Data & Authority, 2020). To achieve its technological goals, the country also created the Saudi Data and Artificial Intelligence Authority (SDAIA) in 2019 to oversee data protection laws and govern the spread of AI (Alim, 2024). The SDAIA is engaged in transforming the Saudi government into a data-driven and AI-enabled organization by implementing innovative data and AI solutions (Fotis Law, 2024). Further, the SDAIA has also established the National Data Management Office and created a national cloud infrastructure with over 45,000 trained professionals (Accenture, 2024). Creating an authority like the SDAIA to control, organize, and develop AI in the country shows that the KSA government is committed to protecting its people's data by advancing laws and regulations to match new technological developments.

The PDPL was initially implemented in 2021 and amended in 2023, with an extended grace period until 2024. As the first comprehensive law that covers data protection issues in Saudi Arabia, the PDPL will be enforced starting from 14 September 2024. The main features of the law include data subject rights, informed consent, access to data, processing restrictions, anonymization, legitimate interest, data processors, and disclosure. In addition, the PDPL covers principles like purpose limitation, data minimization, controller obligations, informed consent, processing restrictions, data subject rights, and penalties (Natasha, et, al, 2023). The PDPL not only includes extensive penalties for entities and businesses that fail to comply with the outlined rules, but its scope also extends to territories outside the Kingdom of Saudi Arabia (Data Guidance, 2024). Specifically, the scope of the PDPL not only covers Saudi Arabian businesses and citizens, but it also extends to entities in foreign countries that process the personal data of people that live in the KSA. For countries outside the KSA, the SDAIA deems them as either adequate countries or non-adequate countries depending on the level of personal data protection in these countries. Of note, the General Data Protection Regulation (GDPR) is one of the main influences that the SDAIA relied on to develop the personal data transfer rules outlined in the PDPL. Before the PDPL's enforcement date, all businesses and other entities that deal with data that belongs to subjects living in Saudi Arabia are required to initiate compliance programmes (O'Connell, 2024). Failure to comply with the law after it comes into effect will result in penalties such as warnings, fines, possible imprisonment, compensation claims, and confiscation of the infringing material or funds for violating individual data privacy rights. By enforcing the PDPL, Saudi Arabia aims to ensure that the personal data of its citizens is secure and protected in the current AI environment.

4. AI & Data Protection Reforms in Saudi Arabia

Since privacy and data protection are a global concern, countries are addressing data protection issues through constitutions, laws, and technical requirements. To address the issue of data privacy and protection, digital identity technology must adhere to international human rights treaties for data protection and privacy. Domestic laws should clearly define digital identity programs and safeguard data storage, usage, and access to ensure data protection. Non-state actors should align their practices with GDPR standards (Beduschi, 2019). Similarly, organizations that use AI technology should consider local and international data protection requirements in their technical and organizational measures. Saudi Arabia has introduced a privacy law that aligns with international privacy laws. The law allows data transfer on three grounds: adequacy decision, appropriate safeguards, and derogations. It also considers four scenarios for data transfer prohibition*:* national security, privacy risk, invalid safeguards, or inability to comply (Al-Masry, 2024). However, while the country’s law is aligned with international policies, Saudi Arabia's policymaking differs from Western information societies since it favors regional control over ICT infrastructure. Since privacy is crucial for e-government adoption and usage, Saudi Arabia needs a functional privacy act and standard terminology to encourage citizens to use e-government services (Alasem, 2015). Overall, in the case of Saudi Arabia and other countries that have adopted AI technology, the success or failure of AI-based applications depends on how data laws are developed and administered.

The AI and data protection reforms in the KSA have also emphasized the importance of consent to the processing of personal and sensitive data. Consent is defined as a legal basis for processing personal data, collecting data indirectly, using it for other purposes, and disclosures (Data Protection, 2023). According to the Implementing Regulations, there are two distinct forms of consent: ordinary consent and explicit consent (Blyth et al., 2023). Before processing personal data or Sensitive Data, an organization must receive explicit consent from the data subjects. Further, not only must consent be obtained freely, but the purpose of processing personal data should also be explained to the individuals in an open, clear, and specific manner (Blyth et. al, 2023). If the data set comes from multiple individuals, explicit consent must be obtained independently from each data subject. Notably, to avoid legal consequences, entities must not obtain any person's consent through a misleading approach. Similar to the GDPR, the Implementing Regulations not only allow consent to be withdrawn but they also require that the withdrawing process should be simpler than the process of giving consent (Blyth et al., 2023). Therefore, not only is explicit consent important to allow personal and sensitive data protection, the process of granting or withdrawing consent must be done freely in a clear and straightforward manner.

5. The Importance of Improving Data Protection Law

Data protection law must be improved due to the legal, ethical, and economic challenges posed by generative AI technology. The main concerns associated with the adoption of AI technology are bias and fairness, privacy and security, accountability and transparency, and economic impacts such as job displacement. On the subject of bias and fairness, individuals and businesses should be vigilant when using AI since the technology is trained on historical data that may contain elements of bias. For this reason, the law should improve to prevent the creation of a biased and discriminatory environment. It is also important to improve data protection law to address the privacy and security concerns associated with AI systems. Businesses that use AI should comply with government regulations such as PDPL and adopt a robust policy to safeguard the personal information of their users (Silverman & Elliot, 2024). Data protection law should also account for the opacity of AI algorithms. By improving data protection legislation, the government can demand transparency from stakeholders in the sector to ensure that the AI decisions that are made are logical and justifiable. Evidently, the widespread adoption and development of AI technology necessitates that rules and regulations evolve to address the AI-related issues that are bound to arise as the technology continues to advance. Saudi Arabia’s AI ethics principles require entities that develop or adopt AI-based systems to adopt certain ethics and standards. While the Kingdom does not have any specific penalties set out for violating the aforementioned principles, laws such as the PDPL, copyright law, anti-cybercrime law, and consumer protection law outline the relevant punishment for non-compliance. Therefore, when using the personal information of users for AI processing, it is important for businesses to avoid committing offences that violate the principles of AI ethics.

The discussion emphasizes the importance of data protection since it has the potential to create a safe technology-led society by strengthening its legal aspects. However, authorities and all the associated stakeholders need to understand that data protection laws need to be developed accordingly to match the changes brought by AI development. As AI technology transforms every day, the laws need thorough and continuous research to find the core legal challenges and deal with different concerns.

6. Need to Regulate AI Data Protection

While AI can unlock human potential, it also requires mature policy and regulatory safeguards to ensure its success. In the era of AI-based applications, the user’s trust in e-government refers to a user’s belief in government privacy practices and data security (Tech & rights, 2024). In particular, privacy refers to the right to control the use and transfer of personal information (Alasem, 2015). Since personal information is frequently spread on the internet during online activities like social networking and business transactions, the information can be used by website owners and AI systems without the user’s knowledge (Alshehri). Therefore, there is an ethical need for the government to create awareness about online security and develop the appropriate legal measures to protect personal user data.

Examining EU data protection law shows that Europe prioritises data protection and commercial privacy as fundamental human rights. The authorities in the EU have developed stronger laws than even the United States due to the absence of IT platform monopolies. For instance, Austria is leading in data protection through technological advancements and education. The country also plans to introduce a digital tax to raise funds for discrimination in data protection which is in alignment with the European Commission’s proposal for fair taxation of digital business activities (Puaschunder, 2019). Importantly, AI developers must exercise caution and care by aiming for ethical use through accepted guidelines and regulations (Joshi, 2019). In the case of Saudi Arabia, data security is a critical concern for businesses, individuals, and the government given that data breaches can pose a significant threat to citizens and government bodies (Alharbi et al., 2021). Since uncontrolled AI systems threaten the fundamental rights of people and organizations, governments have a responsibility to adopt data protection measures that uphold the human rights of data privacy and protection.

Comparing the EU AI Act to the Saudi Law reveals that the two data protection laws share similarities based on the significant effort taken to regulate artificial intelligence-based services. One of the core features of the AI Act is a debiasing exception to the GDPR’s ban on using and transferring sensitive data. Bias is an issue for AI systems since collecting and using sensitive data about ethnicity, religion, health, and other personal information can result in accidental discrimination. Article 10 of the GDPR also includes safeguards aiming to limit risks and eliminate bias when entities make use of special category data (Bekkum and Borgesius, 2024). The safeguards include limiting data access only to authorised individuals, implementing high-level of privacy and security measures, and deleting sensitive data after correcting a bias. Of note, the implementation of both the EU AI Act and Saudi Arabian AI regulations is still underway. For this reason, part of the precise text may still be subject to change or improvement to match present and upcoming changes in the AI systems industry.

7. Legal Challenges to Protect Data in AI

This section of the paper highlights the legal challenges associated with the artificial intelligence data protection. AI presents significant challenges for data protection legislation due to the conflict between fundamental data safety principles and general AI strategy (Cate & Dockery, 2018). The challenges arise when the principles of transparency, purpose limitation, and data minimization conflict with AI's strategy. Another significant legal challenge for data protection law is gaining consent and addressing consent issues in public contexts (Scassa, 2021). Of note, with global sales expected to increase by 92%, data protectionists are concerned about the use and transfer of users' personal information (Chikhaoui et al., 2022). Further, the rising popularity of digital assistants like Google Home and Amazon Echo has raised concerns about the processing of user data. Therefore, it is important to ensure transparency regarding personal data use to address privacy concerns and protect data.

Legal discussions on AI face challenges due to a lack of algorithmic transparency which is exacerbated by inadequate information about algorithm functionality. Not only do AI algorithms rely on a vast amount of data, but they must also consider sensitive data to generate accurate results. For this reason, there is a need for accountability and fair governance in the use of AI technology to ensure that sensitive data is protected. Legal scholars and data protection authorities argue that AI poses significant privacy and data protection challenges including user consent, surveillance, and infringement of individual rights (Rodrigues, 2020). Further, AI's large datasets raise privacy concerns when personal data is used without consent.

There needs to be strict adherence to data protection regulations and transparency when using AI systems (Epilogue Systems, 2024). Organisations should also comply with local data protection laws and international regulations such as the GDPR when deploying AI solutions. Therefore, data protection laws are crucial in the AI context since AI systems blur the line between personal and non-personal data sets.

Another challenge that exists in the current AI legal landscape is the lack of comprehensive, unified, and up-to-date legislation that governs AI use. Currently, there is also no AI-specific enforcement in the KSA (Hammad & Al-Mehdar Law Firm, 2024). The responsible use of generative AI systems in Saudi Arabia requires compliance with multiple legal regulations including data protection laws, ethical and fair AI principles, intellectual property laws, regulatory compliance, contractual agreements, labour laws, consumer protection laws, cybersecurity laws, liability and accountability, government approvals and licensing, anti-discrimination laws, and international data transfer regulations in the case of cross-border data transfer (Hammad & Al-Mehdar Law Firm, 2024). Therefore, it may be difficult for both businesses and legal professionals to navigate the complicated web of regulations that govern the legal and ethical use of AI.

Compliance with AI's unforeseen purposes also remains a challenge in Saudi Arabia's current environment. Since the country has opened its borders to allow people from other nations to visit the KSA for business and trading opportunities of business, the legal challenges to data protection need to be handled in a careful manner (Meenagh and Tucker, 2023). Since the KSA's data protection laws will apply to both citizens and foreign entities in the country, they should account for the data protection understanding of Saudi locals and the understanding of foreign visitors. Therefore, the authorities need to consider the perspectives of both locals and foreigners while developing laws to handle the legal challenges.

8. Conclusion

This article provides a comprehensive overview of the legal issues and challenges related to AI in Saudi Arabia. Due to rapid advances in AI technology, ethical issues regarding the use of personal data or sensitive information have emerged thus necessitating countries across the world including the Saudi Arabia to implement data protection law reforms. While ensuring that AI is compliant with ethical values and human rights is a complex issue, it can be resolved through continuous research and appropriate legislation. By addressing non-discrimination and human dignity issues, the framework of data protection laws has become more complex (Parveen, 2018). Policymakers in the KSA developed the PDPL, Saudi Arabia's first data protection law, to control AI in the country by incorporating privacy and safety principles. When creating or reforming AI data protection legislation such as the PDPL, policymakers in the KSA considered the purposes of AI regulation including safeguarding fundamental rights, mandating product disclosure, holding governments accountable, establishing an independent regulator, and enabling reporting and compensation for AI-induced harm (Tech & Rights, 2024). In the current globalised world, the government also has the responsibility to ensure strong compliance to AI data protection principles and international standards. The laws on AI data protection in the KSA need to be revised to develop a robust mechanism that serves all dimensions of legal challenges that are encountered in data protection.

9. Recommendations

Based on the discussion on the developments made by Saudi Vision 2030 and data protection reforms in the KSA several recommendations have been proposed to improve the present AI data protection in Saudi Arabia.

1. The government of Saudi Arabia should develop a regulatory framework to deal with the legal AI data protection challenges based on continuous research and

development. The framework would help the authorities to stay updated with the recent developmental challenges in AI. Based on the challenges that arise, the legal framework can be modified accordingly for a better data protection mechanism.

2. Vision 2030 authorities should form regulations that take the mega AI-based developmental projects in Saudi Arabia into consideration. The legal challenges would thus be minimized using a custom approach for each AI-based project or AI-based application. In this regard, the authorities of Vision 2030 should consider all the stakeholders that are associated with these megaprojects in any manner. Considering each of the stakeholders would help the authorities in categorising the legal needs for AI data protection.
3. Clear penalties should be considered and documented to be implemented would be in the event that a data breach occurs. The penalties can be in different forms such as monetary fines, firing from employment, or imprisonment. AI application developers or other stakeholders should be made aware about these penalties in case they violate the legal reforms regarding AI data protection.
4. Particular legal reforms should be developed for foreigners if they get involved in any data breaches. The reforms should be in compliance with the international standards or data protection laws.
5. The relevant authorities and Saudi agencies should be responsible for accessing and overseeing all the organisations that use data sets from individuals or other entities to develop or modify AI applications. The numerous megaprojects under development based on the Saudi Vision 2030 need massive support from AI technologies to reach the end goals of the Vision. Data is the crucial and core element of these projects thus it should be protected by forming laws and regulations for different industries and business sectors.
6. Along with these practices, public education on online security and data protection is crucial for raising awareness of internet usage risks and privacy

implications among the general people. Saudis should know their data protection rights in legal terms and how can they utilise laws for their individual protection.

7. There are businesses in different sectors in the KSA that are facing challenges in complying with the PDPL laws developed by the authorities. These challenges include implementing new data protection policies and training staff. Nevertheless, complying with the regulations such as the PDPL can protect data and ensure the digital safety of users. For that reason, KSA should collaborate with data protection agencies to create a framework for managing legal issues.

10. References

- Cate, F. H., & Dockery, R. (2018). Artificial Intelligence and Data Protection: Observations on a Growing Conflict: Observations on a Growing Conflict. 경제규제와법, 11(2), 107-130.
- Accenture. (2024). Reimagining Saudi Arabia's economy. Retrieved from https://www.accenture.com/pl-en/case-studies/artificial-intelligence/reimagining-saudi-arabia-economy
- Alasem, A. N. (2015). Privacy and eGovernment in Saudi Arabia. In World Congress on Engineering and Computer Science (Vol. 2, pp. 21-24).
- Al-Baity, H. H. (2023). The artificial intelligence revolution in digital finance in Saudi Arabia: a comprehensive review and proposed framework. Sustainability, 15(18), 13725.
- Albakjaji, M., & Almarzoqi, R. (2022). The Patentability of AI Invention: The Case of the Kingdom of Saudi Arabia Law. International Journal of Service Science, Management, Engineering and Technology, 13 (1), 1-22.
- Alharbi, A. S., Halikias, G., Rajarajan, M., & Yamin, M. (2021). A review of effectiveness of Saudi E-government data security management. International Journal of Information Technology, 13, 573-579.
- Alim, N. (2024). New Data Protection Law in Saudi Arabia. New Data Protection Law in Saudi Arabia. Retrieved from https://www.datenschutz-notizen.de/new-data-protection-law-in-saudi-arabia-

2245256/#:~:text=The%20legal%20reform%20on%20data,and%20executive%20regulations%20were%20added.

- Al-Masry, O. (2024). Saudi Arabia publishes final Personal Data Protection Law. Retrieved from https://iapp.org/news/a/saudi-arabia-publishes-final-personal-data-protection-law/#:~:text=On%207%20Sept.%2C%20the%20Saudi,year%20to%20prepare%20for%20compliance.
- Al-Saif. S & Yildiz, H. (2024). Saudi Arabia’s Data Protection Law and Regulations Come into Effect. Retrieved from https://www.clearycyberwatch.com/2024/01/saudi-arabias-data-protection-law-and-regulations-come-into-effect/
- Alshehri, A. M. Digital Footprint: A Data Privacy Concerns for End Users in Saudi Arabia.
- Alsulaiman, L. A., & Alrodhan, W. A. (2014). Information Privacy Status in Saudi Arabia. Comput. Inf. Sci., 7(3), 102-124.
- Andrews, C. (2024). European Parliament approves landmark AI Act, looks ahead to implementation. International Association of Privacy Professionals.
- Arab News. (2023). Saudi AI chiefs launch campaign to protect children’s personal data. Retrieved from https://www.arabnews.com/node/2412551/saudi-arabia.
- Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. Big Data & Society, 6(2), 2053951719855091.
- Bekkum, M. V. & Borgesius, F. Z. (2024). The AI Act's debiasing exception to the GDPR. International Association of Privacy Professionals. Retrieved from https://iapp.org/news/a/the-ai-acts-debiasing-exception-to-the-gdpr/.
- Blyth, K., Kesaria, J., & Christie, C. (2023). Impact of the implementing regulations to the Saudi Personal Data Protection Law. Retrieved from https://www.lexology.com/library/detail.aspx?g=dad99ae0-feed-4a2b-b470-c8434f48a573.
- Bygrave, L. A. (2010). Privacy and data protection in an international perspective. Scandinavian studies in law, 56(8), 165-200.
- Chikhaoui, E., Alajmi, A., & Larabi-Marie-Sainte, S. (2022). Artificial intelligence applications in healthcare sector: ethical and legal challenges. Emerging Science Journal, 6(4), 717-738.
- Data Guidance, (2024). Saudi Arabia. Retrieved from https://www.dataguidance.com/jurisdiction/saudi-arabia.

- Data Protection, (2023). Saudi Arabia - Data Protection Overview. Retrieved from https://www.dataguidance.com/notes/saudi-arabia-data-protection-overview.
- Data, S., & Authority, A. I. (2020). National Data Governance Interim Regulations (2020). Retrieved from https://sdaia.gov.sa/ndmo/Files/PoliciesEn.pdf.
- Epilogue Systems. (2024). 5 Key AI Legal Challenges in the Era of Generative AI. Retrieved from https://www.epiloguesystems.com/blog/5-key-ai-legal-challenges/#:~:text=Key%20Legal%20Issues%20in%20AI%20Law&text=Privacy%20and%20Data%20Protection%3A%20AI,for%20companies%20deploying%20AI%20solutions.
- Fotis Law. (2024). Changes to the Technology and Data Laws in Saudi Arabia. Retrieved from https://fotislaw.com/lawtify/technology-data-laws-saudi-arabia/
- Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. Philosophy & Technology, 35(1), 3.
- Hammad & Al-Mehdar Law Firm (2024). Artificial intelligence and ethics: Navigating the legal landscape for businesses. LexisNexis E-Journal, 1-4.
- IBM. (2024). What is artificial intelligence (AI)? Retrieved from https://www.ibm.com/topics/artificial-intelligence
- Joshi, N. (2019). Why governments need to regulate AI. Retrieved from https://www.linkedin.com/pulse/why-governments-need-regulate-ai-naveen-joshi/
- Meenagh. B, & Tucker, L. (2023). Saudi Arabia's data protection law enters into force. Retrieved from https://www.lw.com/en/offices/admin/upload/SiteAttachments/Saudi-Arabias-data-protection-law-enters-into-force.pdf
- Meurisch, C., & Mühlhäuser, M. (2021). Data protection in AI services: A survey. ACM Computing Surveys (CSUR), 54(2), 1-38.
- Nagar, R. (2023). The Impact of AI on Privacy and Data Protection Laws. Retrieved from https://www.linkedin.com/pulse/impact-ai-privacy-data-protection-laws/
- Natasha, et, al. (2023). Kingdom of Saudi Arabia's New Personal Data Protection Law and Implementing Regulations—Key Obligations, Responsibilities and Rights
- O'Connell, N. (2024). An overview of Saudi Arabia's new Personal Data Protection Law. Retrieved from https://www.tamimi.com/law-update-articles/an-overview-of-saudi-arabias-new-personal-data-protection-law/

- Parveen, R. (2018). Challenges in cloud computing adoption-an empirical study of educational sectors of Saudi Arabia. Indian Journal of Science and Technology, 11(48), 1-11.
- Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. Journal of Responsible Technology, 4, 100005.
- Saad, A. R. (1981). Information Privacy and Data Protection: A Proposed Model for the Kingdom of Saudi Arabia. Abdul Raman Saad & Associates, Malaysia.
- Scassa, T. (2021). AI and Data Protection Law. Artificial Intelligence and the Law in Canada (Toronto: LexisNexis Canada, 2021).
- Silverman, K. & Elliot B. (2024). Artificial Intelligence Law. Latham and Watkins LLP.
- Tech & Rights. (2024). AI Regulation: Present Situation and Future Possibilities. Retrieved from https://www.liberties.eu/en/stories/ai-regulation/43740.