Balancing AI Advancements and Data Privacy in Digital Marketing: A Conceptual Exploration of Ethical Considerations and Consumer Rights

Ghaleb El Refae
Department of Business Administration, College of Business
Al Ain Campus, Al Ain University
P.O. Box: 64141, Al Ain, UAE
ghaleb.elrefae@aau.ac.ae

Ahmad Ibrahim Aljumah
College of Communication and Media
Al Ain University, Abu Dhabi Campus
P.O. Box 112612, Abu Dhabi, UAE
ahmad.aljumah@aau.ac.ae

Mohammed T. Nuseir
Department of Business Administration
College of Business
Al Ain University, Abu Dhabi Campus,
P.O. Box 112612, Abu Dhabi, UAE
mohammed.nuseir@aau.ac.ae

***Abstract*—Artificial intelligence (AI) and digital marketing have become increasingly intertwined in recent years. While AI has the potential to revolutionize digital marketing by automating many of the processes involved in advertising, it also presents several challenges and potential problems. The most rising issue is the data privacy issues that marketers might face when practicing AI for digital marketing strategies. Data privacy is a crucial issue when it comes to AI-based digital marketing strategies. Marketers are gathering many data about their clients/customers and prospects thanks to the spread of AI technology to tailor their marketing efforts and offer a better customer experience. Yet, this data may be delicate and may include sensitive or private information that must be secured. As we know, AI relies heavily on data to generate insights and make decisions. However, collecting and analyzing customer data can raise privacy concerns. Marketers need to ensure that they are collecting and using data in a transparent and ethical way to avoid potential legal and reputational risks. This paper aims to ponder conceptually the data privacy issues using artificial intelligence for all aspects of digital marketing. In addition, this paper will also look at the customers' rights to share their information.**

Keywords—data privacy, artificial intelligence, digital marketing, customer rights.

I. Introduction To Data Privacy

In the current digital era, customers are becoming more concerned about data privacy (25). The term data privacy is explained as "The protection of personal information or data, such as a person's name, address, phone number, financial information, or any other information that may be used to identify or link a person, is referred to as data privacy. It entails having control over how this information is gathered, used, stored, and shared. Data privacy aims to protect people's right to control over what information is gathered about them, how it is used, and who has access to it. In the era of digital technology, where personal data may be easily gathered and shared across several platforms without users' awareness or consent, this is especially crucial." Consumers are becoming more aware of the possible hazards related to data breaches, identity theft, and illegal access to their personal information as information that is more personal is shared and kept online. Customers' top worries regarding data privacy include data breaches, lack of transparency, regulation and enforcement, and lack of control (15). Figure 1 shows the data privacy barrier to AI for digital marketing.

In this paper, these concepts are discussed in detail with possible solutions for companies towards AI implementation in digital marketing (20).

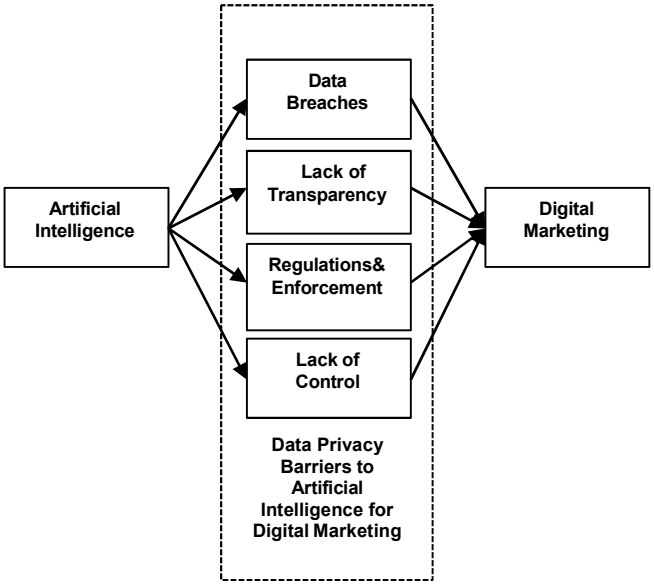

Fig. 1. Data Privacy Barriers

II. Data Breaches

Consumers are concerned about the protection of their personal information, including their name, address, social security number, and financial data. They worry that hackers may access or steal personal information, resulting in identity theft or financial crime. When using artificial intelligence for digital marketing, data breaches might be a serious concern (19; 27). This is since AI systems need access to many client data, including private data like names, email addresses, and credit card numbers. Identity theft, financial fraud, and other types of cybercrime may result if this data gets into the wrong hands (8).

There could be several causes of data breaches in AI for digital marketing such as weak security measures. Companies may safeguard consumer data and make sure that their AI systems are secure and dependable by addressing inadequate security measures in AI for digital

979-8-3503-5469-0/24/$31.00 ©2024 IEEE

marketing (8). To maintain a high degree of security and secure client data, it is critical for businesses to keep current on the most recent security measures and best practices. In addition, companies with insufficient data protection measures may not have firewalls, access restrictions, or encryption in place to safeguard client data (23).

Moreover, companies with Vulnerable Infrastructure may have old or improperly maintained servers, routers, or firewalls, which can increase their susceptibility to online assaults. On the other hand, employees or other insider threats may purposefully or accidentally breach security measures by disclosing passwords or other sensitive information to unauthorized people, among other actions (14). Third party suppliers pose a threat to data breaches, and businesses frequently deal with these vendors to handle their consumer data, such as marketing firms (30). The fact that various suppliers might not be using the same security procedures might make data breaches more likely. Additionally, assaults such as poisoning, adversarial, or backdoor attacks may be possible against artificial intelligence algorithms. To obtain unauthorized access to client data, attackers might modify the data or algorithms (31).

A. How Companies can prevent data breaches?

There are various researchers (9); (18), who have recommended strong security methods like encryption, multi-factor authentication, and regular security audits are some ways that businesses may protect themselves. In addition, businesses should regularly review their risks to spot weaknesses and take preventative measures to address them. The staff, however, must be regularly trained in data privacy and security best practices (23). This includes using secure passwords, seeing, reporting irregularities, and avoiding phishing frauds. Companies should thoroughly investigate third-party providers to make sure they adhere to data protection laws and have robust security measures in place to prevent data breaches. Moreover, explainable AI may aid businesses in better understanding the operation of their AI algorithms and locating any weaknesses or possible points of vulnerability (2). By following these guidelines, international companies who use artificial intelligence for digital marketing may help prevent data breaches. This can help safeguard client data and increase customer trust.

III. LACK OF TRANSPARENCY

The lack of transparency in how companies manage customer data frustrates customers. They are interested in the kind of data being gathered, how they are being utilized, and who has access to them. When using artificial intelligence for digital marketing, a major difficulty might be a lack of transparency (33). This is due to the complexity of AI systems, which makes it challenging for users to comprehend how their data is being utilized and what decisions are being made considering it.

Lack of transparency in AI for digital marketing can be attributed to several factors, such as the fact that certain AI systems are referred to be "black boxes," meaning that people find it difficult to comprehend how they make decisions. Because of this, it could be challenging for customers to comprehend why particular advertisements or product recommendations are made to them (11).

Apart from social media platforms, websites, and mobile applications, companies might also get information from other sources. Consumers might not be aware of all the information being gathered or its intended uses. Moreover, biased data may be utilized to train AI systems, which can lead to biased results (33). Customers could find it challenging to grasp or recognize the unfair or discriminating effects this can have. Finally, customers may find it challenging to comprehend their rights and how their data is safeguarded due to a lack of defined legislation around the use of AI in digital marketing (32).

A. How companies can increase transparency in AI for digital marketing?

Companies should be transparent about how their AI systems operate, how data is gathered, and how it is use. There are various marketing researchers (29); (11); (21), who have recommended that customers may thus better comprehend why particular advertisements or product recommendations are made to them. Moreover, companies may utilize explainable AI systems, which are created to be clearer and easier for people to grasp. Customers that use these technologies may be able to better understand how decisions are made using their data. Companies should be open and honest about the information they get, how they gather it, and how they utilize it. Customers may benefit from knowing how their data is being utilized and the choices being made as a result (24).

In addition, Companies must take action to eliminate prejudice in AI systems, including checking their data and algorithms for bias and employing a variety of data sets to train their algorithms. Companies should adhere to data protection standards to guarantee that customer data is secured and that consumers are aware of their rights to promote transparency (31). Companies may gain consumers' trust and guarantee that their data is being utilized in a responsible and ethical manner by enhancing transparency in AI for digital marketing.

IV. REGULATIONS AND ENFORCEMENT

Customers demand stricter laws and enforcement to safeguard their privacy. They want firms to be held liable for data breaches and illicit use of their personal information (13) ;(1). Moreover, (12) informed that when using artificial intelligence in digital marketing, there are several laws and enforcement policies in place to safeguard user data. Some of the key regulations and enforcement measures include:

a) General Data Protection Regulation (GDPR)
b) California Consumer Privacy Act (CCPA)
c) Federal Trade Commission (FTC)

d) European Data Protection Board (EDPB)
e) National Data Protection Authorities (DPAs)
f) International Standards Organizations

All businesses that process the personal information of EU individuals must comply with the GDPR, which is thorough data privacy legislation (28). Companies are required to employ stringent data privacy procedures and get express consent before collecting and utilizing personal data. Consumers in California have the right to know what personal information is being collected about them and how it is being used according to the CCPA, state-level data privacy legislation (26). Moreover, it allows customers the option to ask for the deletion of their information. For enforcing data privacy laws in the United States and the other part of the world, the FTC is the principal federal agency in charge. It has the jurisdiction to investigate and punish companies that disobey data privacy rules, especially those pertaining to artificial intelligence and digital marketing. An organization in charge of enforcing and monitoring the GDPR in Europe is called the EDPB (12).

In addition to having the power to levy fines and other sanctions for non-compliance, it also offers firms information and recommendations on how to comply with the GDPR. Each national DPA of an EU member state oversees applying the GDPR domestically. They are empowered to investigate and punish businesses that breach the GDPR, particularly those engaged in digital marketing and artificial intelligence. For data privacy and security, several international standards organizations, including ISO and IEEE, offer recommendations and standards (4,49).

These guidelines can aid companies in putting best practices for data privacy into practice and safeguarding against data breaches. Companies may secure client data and guarantee that their use of artificial intelligence in digital marketing is open and ethical by adhering to certain rules and enforcement mechanisms (5). To be compliant and maintain a high degree of data privacy and security, it is crucial for businesses to keep up with the most recent laws and best practices.

V. LACK OF CONTROL

Customers believe that once their personal information is released online, they no longer have much control over it. They are concerned that their data may be used for purposes for which they did not provide consent or that they might not be able to erase their data if they so want. When using artificial intelligence in digital marketing, a big worry is the lack of control over data privacy (6). Consumers want to feel in control of their personal information and how it is utilized.

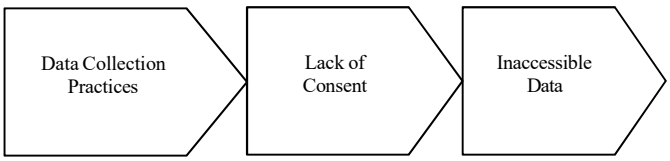

Fig.2. Causes of lack of control in AI for Digital Marketing

Figure 1 shows that Companies may collect data from a variety of sources, including social media platforms, websites, and mobile apps. Customers may not be aware of all the data being collected or how it is, being used (22). On the other hand, customers may not have given explicit consent for their data to be used in certain ways, or they may not be aware of how their data is being used. Lastly, the customers may not have access to their own data or may not be able to control how companies are using it.

A. How companies could address lack of control in AI for digital marketing?

International companies, which are willing to initiate AI in digital marketing, should be transparent about how their AI systems operate, how data is gathered, and how it is put to use. Customers may find this useful in understanding the types of data being gathered and their intended uses (10). Prior to collecting and utilizing consumers' personal information, businesses should have their express consent. Consumers should be provided with clear and detailed information about the types of data being collected, their intended uses, and the individuals who will have access to them. (47).

In addition, companies should provide customers with the choice to refuse the gathering and usage of their data. Customers may have more control over their personal data because of this. Furthermore, Customers should have access to their own personal data from businesses so they can understand what data is being gathered and how it is being utilized. To safeguard client data from data breaches or illegal access, effective data security measures must be put in place. Customers will feel like they have greater control over how their personal information is handled as a result. Companies may increase consumer trust and make sure that their customers' data is being utilized in a fair and ethical way by addressing lack of control in AI for digital marketing (16,50).

VI. RECOMMENDED SOLUTION FOR DATA PRIVACY

International companies can take several steps to solve data privacy issues for digital marketing while using artificial intelligence. Here are some potential solutions:

A. Adhere to local data protection laws:

Previous researchers (5); (26), suggested that international companies should be aware of the data privacy laws in each jurisdiction where they conduct business and make sure they are following them. For instance, the General Data Protection Regulation (GDPR) of the European Union, which is applicable to all businesses operating inside the EU, contains stringent data protection obligations.

Businesses should make sure that their methods for collecting and processing data adhere to all applicable laws.

B. Employ data reduction

By limiting the quantity of data, they gather and analyze, businesses may lower the risk of data privacy breaches. Companies should just gather the data required for their marketing activities and employ artificial intelligence to evaluate it, not retaining personal information unless essential (3).

C. Put in place robust security measures:

To secure client data, businesses should put strong security measures in place. To secure data from unwanted access, this involves implementing encryption, access limits, and frequent security audits (23).

D. Provide transparent and unambiguous privacy policies:

Businesses must offer consumers privacy policies that are upfront and explicit, outlining the data they gather, how they use it, and how customers may manage it. By doing this, you may increase consumer trust and make sure they are aware of how their data is being utilized (4).

E. Get express approval:

Before collecting consumers' personal data, businesses should have their express consent. Customers may be given the option to voluntarily consent to the collection and processing of their data as part of this (11).

F. Hire data privacy experts:

Multinational companies and corporations may require employing data privacy experts to counsel them on the best procedures for data security and privacy. These professionals can guarantee that the business is following local laws and putting the best data protection practices into place. International businesses may assist in resolving data privacy challenges for digital marketing while utilizing artificial intelligence by putting these strategies into practice. Customers will be more likely to trust a company if their personal information is managed responsibly and securely (17).

VII. DISCUSSION

Data privacy is a top issue for businesses using artificial intelligence for digital marketing and market research. Even while artificial intelligence (AI) has the potential to be a great tool for customer data analysis and understanding consumer behavior, it also needs access to sensitive personal data. From surfing habits and purchasing patterns to personally identifiable data like names and addresses, this information may cover it all. It makes sense that businesses do not want to divulge their information (46). Confidential information is at danger of being stolen or disclosed, which might be bad for the business and its clients. The acquisition and use of personal data is also surrounded by legal and ethical issues, which businesses must carefully negotiate.

Companies must take action to safeguard the security and privacy of client data to satisfy these concerns. To prevent unwanted access, this includes putting robust data protection measures in place, such as encryption and access limits. Also, businesses should be open and honest about how they gather and utilize customer data, clearly stating what information is being gathered, why, and for what purposes. The General Data Protection Regulation (GDPR) of the European Union (EU) and the California Consumer Privacy Act (CCPA), which place tight restrictions on the gathering, using, and sharing of personal data, are only two examples of rules and regulations that businesses must abide with (48).

VIII. CONCLUSION

Consumers' worries about data privacy are major, and companies must act to allay them and guarantee the security of the personal data of their clients. In conclusion, while concerns about data privacy may prevent companies from implementing artificial intelligence for digital marketing and investigating virtual markets, these issues can be allayed using effective data protection measures, openness about data collection and use procedures, and adherence to relevant laws and regulations. They can accomplish this while safeguarding the security and privacy of their customers' private information and utilizing the power of AI to get insightful knowledge into consumer behavior. Companies may secure client data and guarantee that their use of artificial intelligence in digital marketing is open and ethical by adhering to rules and enforcement mechanisms. To be compliant and maintain a high degree of data privacy and security, it is crucial for businesses to keep up with the most recent laws and best practices.

REFERENCES

[1] Alkhayyat, A. M., & Ahmed, A. M. (2022). “The impact of artificial intelligence in digital marketing administration Supervisor: Stylianos Papaioannou.”

[2] Bandari, V. (2019). “The Impact of Artificial Intelligence on the Revenue Growth of Small Businesses in Developing Countries: An Empirical Study.” Reviews of Contemporary Business Analytics, vol. 2(1), pp. 33-44.

[3] Biega, A. J., & Finck, M. (2021). “Reviving purpose limitation and data minimisation in data-driven systems.” arXiv preprint arXiv:2101.06203.

[4] Chander, A., Abraham, M., Chandy, S., Fang, Y., Park, D., & Yu, I. (2021). “Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation.” Policy Research Working Paper, 9594.

[5] Clifford, D., Richardson, M., & Witzleb, N. (2022). “Artificial intelligence and sensitive inferences: new challenges for data protection laws. In Regulatory Insights on Artificial Intelligence” (pp. 19-45). Edward Elgar Publishing.

[6] Colleoni, E., & Corsaro, D. (2022). “Critical issues in artificial intelligence algorithms and their implications for digital marketing.” In The Routledge Handbook of Digital Consumption (pp. 166-177). Routledge.

[7] De Capitani Di Vimercati, S., Foresti, S., Livraga, G., & Samarati, P. (2012). “Data privacy: Definitions and techniques.” International

Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 20(06), pp. 793-817.

[8] Dewani, P. P., & Bains, K. (2020). WEBACCESSPRO: "An Artificial Intelligence Start Up in Crowded Market." Academy of Marketing Studies Journal, vol. 24(4), pp. 1-17.

[9] Dimitrieska, S., Stankovska, A., & Efremova, T. (2018). "Artificial intelligence and marketing." Entrepreneurship, 6(2), pp. 298-304.

[10] Estrada-Jiménez, J., Parra-Arnau, J., Rodríguez-Hoyos, A., & Forné, J. (2019). "On the regulation of personal data distribution in online advertising platforms." Engineering Applications of Artificial Intelligence, vol.82, pp. 13-29.

[11] Aljumah, A.I.2022. Exploring nexus among big data analytic capability and organizational performance through mediation of supply chain agility. *Uncertain Supply Chain Management, 2022, 10(3), pp. 999–1008*

[12] Felzmann, H., Villaronga, E. F., Lutz, C., & Tamò-Larrieux, A. (2019). "Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns." Big Data & Society, vol. 6(1), 2053951719860542.

[13] Fiero, A. W., & Beier, E. (2022). "New Global Developments in Data Protection and Privacy Regulations: Comparative Analysis of European Union, United States, and Russian Legislation." Stan. J. Int'l L., vol. 58, pp. 151.

[14] Hörnle, J., Schmidt-Kessen, M., Littler, A., & Padumadasa, E. (2019). "Regulating online advertising for gambling–once the genie is out of the bottle…". Information & Communications Technology Law, vol. 28(3), pp. 311-334.

[15] Aljumah, A. I., Shahroor, H., Nuseir, M., & El Refae, G. A. (2022). "The effects of employee commitment and environment uncertainty on product quality: The mediating role of supply chain integration." Uncertain Supply Chain Management, vol. 10(4), pp. 1379–1386

[16] Jin, G. Z. (2018). "Artificial intelligence and consumer privacy. In The Economics of Artificial Intelligence: An Agenda" (pp. 439-462). University of Chicago Press.

[17] Limna, P. (2022). "Artificial Intelligence (AI) in the hospitality industry: A review article." International Journal of Computer Science Research, vol. 6, 1-12.

[18] Mogaji, E., & Nguyen, N. P. (2022). "Managers' understanding of artificial intelligence in relation to marketing financial services: insights from a cross-country study." International Journal of Bank Marketing, vol. 40(6), pp. 1272-1298.

[19] Aljumah, A.I., Nuseir, M.T., El Refae, G.A.2023. Examining the effect of social media interaction, E-WOM, and public relations: Assessing the mediating role of brand awareness. International Journal of Data and Network Science, 2023, 7(1), pp. 467–476

[20] Murgai, A. (2018). "Transforming digital marketing with artificial intelligence." International Journal of Latest Technology in Engineering, Management & Applied Science, vol. 7(4), pp. 259-262.

[21] Ribeiro, T., & Reis, J. L. (2020). "Artificial intelligence applied to digital marketing." In Trends and Innovations in Information Systems and Technologies, vol. 2 8 (pp. 158-169). Springer International Publishing.

[22] Robinson, S. C. (2020). "Trust, transparency, and openness: How inclusion of cultural values shapes Nordic national public policy strategies for artificial intelligence (AI)." Technology in Society, vol. 63, 101421.

[23] Rodgers, S. (2021). "Themed issue introduction: Promises and perils of artificial intelligence and advertising." Journal of Advertising, vol. 50(1), pp. 1-10.

[24] Sachdev, R. (2020, April). "Towards security and privacy for edge AI in IoT/IoE based digital marketing environments." In 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC) (pp. 341-346). IEEE.

[25] Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2021). "Setting B2B digital marketing in artificial intelligence-based CRMs: A review and directions for future research." Industrial Marketing Management, vol. 98, pp. 161-178.

[26] Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2022). "Assessing behavioral data science privacy issues in government artificial intelligence deployment." Government Information Quarterly, vol. 39(4), 101679.

[27] Nuseir, M.T., Aljumah, A.2020. Digital marketing adoption influenced by relative advantage and competitive industry: A UAE tourism case study. *International Journal of Innovation, Creativity and Change, 2020, 11(2), pp. 617–631*

[28] Shi, P., Winter, J. S., & Zhang, B. (2021). "Governance of privacy protection: How laws will be adopted to address new technologies?"

[29] Sposit, N. (2019). "Adapting to digital marketing regulations: The impact of the General Data Protection Regulation on individualized, behavior-based marketing techniques." Journal of Digital & Social Media Marketing, vol. 6(4), pp. 341-348.

[30] Sylvain, O. (2018). The Market for User Data. Fordham Intell. Prop. Media & Ent. LJ, vol. 29, 1087.

[31] Topol, E. J. (2019). "High-performance medicine: the convergence of human and artificial intelligence." Nature medicine, vol. 25(1), pp. 44-56.

[32] Tschider, C. A. (2018). "Regulating the internet of things: discrimination, privacy, and cybersecurity in the artificial intelligence age." Denv. L. Rev., pp. 96, 87.

[33] Tucker, C. (2018). "Privacy, algorithms, and artificial intelligence." In The economics of artificial intelligence: An agenda (pp. 423-437). University of Chicago Press.

[34] Wang, R., Bush-Evans, R., Arden-Close, E., Bolat, E., McAlaney, J., Hodge, S., ... & Phalp, K. (2022). "Transparency in persuasive technology, immersive technology, and online marketing: Facilitating users' informed decision making and practical implications." Computers in Human Behavior, 107545.

[35] Wang, Y., Xiong, M., & Olya, H. (2020, January). "Toward an understanding of responsible artificial intelligence practices." In Proceedings of the 53rd hawaii international conference on system sciences (pp. 4962-4971). Hawaii International Conference on System Sciences (HICSS).

[36] Saboune, F. M. F. (2022, November). "Virtual Reality in Social media marketing will be the new model of advertising and monetization." In 2022 Ninth International Conference on Social Networks Analysis, Management and Security (SNAMS) (pp. 1-7). IEEE.

[37] Nuseir, M.T., Aljumah, A.I., El Refae, G.A.2022. The Influence of E-learning, M-learning, and D-learning on the Student Performance: Moderating Role of Institutional Support. Proceedings - 2022 23rd International Arab Conference on Information Technology, ACIT 2022, 2022

[38] Moradi, M. (2021). "Importance of internet of things (IoT) in marketing research and its ethical and data privacy challenges."

[39] Tabash, M. I., Farooq, U., El Refae, G. A., & Qasim, A. (2023). Exploring the carbon footprints of economic growth, foreign investment, energy dependency and financial development: does EKC work in GCC region?. *Management of Environmental Quality: An International Journal*, *34*(2), 273-289.

[40] Yasmin, T., El Refae, G. A., & Eletter, S. (2020). Oil price and urgency towards economic diversification through effective reforms and policies in Caspian Basin. *Journal of Eastern European and Central Asian Research (JEECAR)*, *7*(3), 305-315.

[41] Awawdeh, A. E., Shahroor, H. G. N., Alajlani, S., Nuseir, M. T., & Aljumah, A. I. (2022). Assessing mechanism of financial institutions' role in managing environmental vulnerabilities. *Environmental Science and Pollution Research*, *29*(56), 84773-84786.

[42] Farhi, F., Jeljeli, R., Aburezeq, I., Dweikat, F. F., Al-shami, S. A., & Slamene, R. (2023). Analyzing the students' views, concerns, and perceived ethics about chat GPT usage. In *Computers and Education: Artificial Intelligence* (Vol. 5). Elsevier B.V. https://doi.org/10.1016/j.caeai.2023.100180

[43] Jeljeli, R., Farhi, F., Hamdi, M. E., & Saidani, S. (2022). The Impact of Technology on Audiovisual Production in the Social Media Space. *Academic Journal of Interdisciplinary Studies*, *11*(6), 48–58. https://doi.org/10.36941/ajis-2022-0148

[44] Al-Chahadah, A. R., Refae, G. A. E., & Qasim, A. (2020). The impact of financial inclusion on bank performance: the case of Jordan. *International Journal of Economics and Business Research*, *20*(4), 483-496.