Bincang Sains dan Teknologi (BST) **E-ISSN 2961-8746**
DOI: 10.56741/bst.v4i03.1117 **P-ISSN 2961-8932**



The Dark Side of Bot Farms in the Business World: An Ethical and Economic Threat in the Digital Era

[1]Ari Fajar Santoso*, [2]Zafar Khan
Corresponding Author: * arifajar@telkomuniversity.ac.id
[1] Telkom University, Bandung, Indonesia
[2] Abasyn University, Peshawar, Pakistan

Article submitted: 15 June 2025 **Revised:** 3 August 2025 **Accepted:** 25 August 2025

Abstract

In the digital economy, bot farms have emerged as a controversial tool businesses use to manipulate online visibility and influence consumer perception. While automation offers efficiency, bots' misuse, primarily through coordinated bot farms, poses serious ethical, legal, and economic challenges. This article critically examines the negative impact of bot farms in business practices, focusing on deceptive marketing, unfair competition, consumer misinformation, and the distortion of digital ecosystems. Using qualitative analysis and literature review, this study highlights the urgent need for regulatory frameworks and ethical digital governance to combat the rise of bot-driven manipulation. The findings show that bot farms undermine trust, disrupt market fairness, and erode the integrity of online platforms, calling for cross-sector efforts to mitigate their spread.

Keywords: *bot farm, consumer deception, digital governance, digital manipulation, unethical business practices*

Introduction

The proliferation of digital technologies has transformed the business landscape, offering new ways to engage customers and analyze markets. Bots (automated programs capable of performing repetitive tasks efficiently) are among the tools used. While bots can enhance customer experience and streamline services, their misuse in the form of bot farms introduces a darker dimension to digital business operations [1], [2].

A bot farm is a coordinated network of automated accounts designed to mimic human behavior at scale. These systems are often deployed to manipulate digital metrics, inflate social media engagement, or propagate disinformation. The growing sophistication of bot farms makes them harder to detect and increasingly attractive for unethical business strategies [3].

Recent reports and studies have shown how bot farms can distort online ratings, generate fake product reviews, and manipulate consumer perception, ultimately damaging market integrity and trust [4], [5]. These artificial engagements harm ethical businesses and compromise the accuracy of algorithms that govern digital visibility on platforms like Google, Amazon, and Facebook.

This paper explores the dark side of bot farms in the business world, focusing on the ethical, legal, and economic consequences. Through a structured literature review and critical analysis, we investigate how these tools compromise the fairness and transparency of digital commerce. By

highlighting current challenges and the regulatory gap, this research calls for urgent governance mechanisms and collaborative responses from multiple stakeholders in the digital ecosystem.

Literature Review

Previous studies have extensively discussed the role of bots in digital ecosystems. Ferrara et al. [1] explored the behavioral patterns of bots on Twitter, showing how they can amplify false narratives. Meanwhile, Cresci et al. [2] emphasized the evolution of bots into sophisticated "social spambots" capable of influencing real users. From a marketing perspective, bots are used for astroturfing, creating a false impression of popularity or grassroots support [3]. In business, such tactics can mislead consumers, investors, and competitors. Allcott and Gentzkow [4] argue that bot farms distort online ratings, undermining the reliability of e-commerce platforms.

Ethically, bot farms violate the principles of transparency, authenticity, and fair competition. According to Barbado et al. [5], digital persuasion must adhere to moral boundaries, which bot farms frequently transgress. Furthermore, legal scholars have highlighted the regulatory vacuum surrounding bots, especially in cross-border operations [6]. These findings suggest an urgent need to investigate bot farms' technical, ethical, and socio-economic implications in business.

Analysis and Discussion

A. Manipulation and Consumer Deception

Bot farms are commonly used to fabricate social proof (likes, followers, reviews) on social media and e-commerce platforms. These inflated metrics deceive consumers into believing a product is popular or trustworthy [7], [8], [9], [10]. For instance, fake reviews can significantly influence purchase decisions, misallocating consumer resources. Moreover, bots can simulate engagement in real time, making it difficult for algorithms to differentiate genuine interest from automation. This manipulation erodes user trust, a critical currency in digital marketplaces.



Source: https://www.bankinfosecurity.com/ukrainian-police-shutter-propaganda-spreading-bot-farm-a-22592

B. Unfair Competition and Market Distortion

Businesses using bot farms gain an unfair advantage by undermining organic marketing efforts. Competitors adhering to ethical standards are disadvantaged, skewing market dynamics [11], [12], [13],

[14]. Additionally, bot attacks in the form of fake negative reviews or click fraud can directly harm competitors' revenue and reputation. Platforms like Amazon and Google have struggled to mitigate such abuses, revealing systemic vulnerabilities in current digital governance models.



Source: https://assets-prd.ignimgs.com/2021/07/18/6cf3d8104a192be2bb2380c6e3ce466c-1626584797403.jpeg

C. Impact on Digital Ecosystems

Beyond individual cases, bot farms affect broader digital ecosystems. Algorithms that rely on user behavior to rank content are easily manipulated by automated activity [15], [16], [17], [18]. As a result, low-quality or even harmful content can gain visibility, while genuine voices are buried. This dynamic leads to a degradation of content quality and user experience. It also challenges the credibility of recommendation systems, search engines, and social platforms.



Source: https://sundayguardianlive.com/business/phone-farms-and-modern-day-exploitation

D. Legal and Ethical Implications

While some jurisdictions have started to regulate bots (e.g., California's Bot Disclosure Law), most legal systems lack explicit provisions for dealing with bot farms, especially those operated transnationally [19], [20], [21], [22]. The anonymity and scale of bot operations complicate accountability.

Ethically, deploying bot farms contravenes principles of integrity, transparency, and respect for consumer autonomy. Yet, the incentive structure of digital markets, driven by visibility and engagement metrics, continues to fuel their proliferation.

Conclusion

Bot farms represent a growing threat to ethical business practices in the digital age. Their ability to manipulate perception, distort competition, and degrade trust presents challenges that extend beyond individual firms to entire digital ecosystems. As businesses increasingly operate in data-driven environments, the misuse of automated tools like bot farms must be critically addressed. This paper underscores the need for:

- Stronger regulatory frameworks across jurisdictions,
- Ethical guidelines for digital marketing and data use,
- Platform accountability in detecting and curbing bot activity,
- Greater public awareness and digital literacy among consumers.

Tackling the dark side of bot farms requires a multidisciplinary approach, involving policymakers, technologists, businesses, and civil society to preserve the integrity of digital commerce.

References

[1] E. Ferrara, O. Varol, C. Davis, F. Menczer, and A. Flammini, 'The rise of social bots', *Commun. ACM*, vol. 59, no. 7, pp. 96–104, June 2016, doi: 10.1145/2818717.
[2] S. Cresci, R. Di Pietro, M. Petrocchi, A. Spognardi, and M. Tesconi, 'Fame for sale: Efficient detection of fake Twitter followers', *Decis. Support Syst.*, vol. 80, pp. 56–71, Dec. 2015, doi: 10.1016/j.dss.2015.09.003.
[3] F. Mazzella, A. Sundararajan, V. Butt d'Espous, and M. Möhlmann, 'How Digital Trust Powers the Sharing Economy: The Digitization of Trust', *IESE Insight*, no. 30, pp. 24–31, Sept. 2016, doi: 10.15581/002.art-2887.
[4] H. Allcott and M. Gentzkow, 'Social Media and Fake News in the 2016 Election', *J. Econ. Perspect.*, vol. 31, no. 2, pp. 211–236, May 2017, doi: 10.1257/jep.31.2.211.
[5] R. Barbado, O. Araque, and C. A. Iglesias, 'A framework for fake review detection in online consumer electronics retailers', *Inf. Process. Manag.*, vol. 56, no. 4, pp. 1234–1244, July 2019, doi: 10.1016/j.ipm.2019.03.002.
[6] N. P. Suzor, *Lawless*. Cambridge University Press, 2019. doi: 10.1017/9781108666428.
[7] G. D. Domenico, J. Sit, A. Ishizaka, and D. Nunan, 'Fake news, social media and marketing: A systematic review', *J. Bus. Res.*, vol. 124, pp. 329–341, Jan. 2021, doi: 10.1016/j.jbusres.2020.11.037.
[8] B. Horne and S. Adali, 'This Just In: Fake News Packs A Lot In Title, Uses Simpler, Repetitive Content in Text Body, More Similar To Satire Than Real News', *Proc. Int. AAAI Conf. Web Soc. Media*, vol. 11, no. 1, pp. 759–766, May 2017, doi: 10.1609/icwsm.v11i1.14976.
[9] Y. Li, F. Wang, S. Zhang, and X. Niu, 'Detection of Fake Reviews Using Group Model', *Mob. Netw. Appl.*, vol. 26, no. 1, pp. 91–103, Nov. 2020, doi: 10.1007/s11036-020-01688-z.
[10] M. Luca and G. Zervas, 'Fake It Till You Make It: Reputation, Competition, and Yelp Review Fraud', *Manag. Sci.*, vol. 62, no. 12, pp. 3412–3427, Dec. 2016, doi: 10.1287/mnsc.2015.2304.
[11] B. Edelman, M. Luca, and D. Svirsky, 'Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment', *Am. Econ. J. Appl. Econ.*, vol. 9, no. 2, pp. 1–22, Apr. 2017, doi: 10.1257/app.20160213.
[12] R. Gorwa and D. Guilbeault, 'Unpacking the Social Media Bot: A Typology to Guide Research and Policy', *Policy Internet*, vol. 12, no. 2, pp. 225–248, Aug. 2018, doi: 10.1002/poi3.184.
[13] J. Ratkiewicz, M. Conover, M. Meiss, B. Goncalves, A. Flammini, and F. Menczer, 'Detecting and Tracking Political Abuse in Social Media', *Proc. Int. AAAI Conf. Web Soc. Media*, vol. 5, no. 1, pp. 297–304, Aug. 2021, doi: 10.1609/icwsm.v5i1.14127.

[14] D. Freelon and C. Wells, 'Disinformation as Political Communication', *Polit. Commun.*, vol. 37, no. 2, pp. 145–156, Feb. 2020, doi: 10.1080/10584609.2020.1723755.
[15] X. Liu, 'A big data approach to examining social bots on Twitter', *J. Serv. Mark.*, vol. 33, no. 4, pp. 369–379, Apr. 2019, doi: 10.1108/jsm-02-2018-0049.
[16] N. Chavoshi, H. Hamooni, and A. Mueen, 'DeBot: Twitter Bot Detection via Warped Correlation', presented at the 2016 IEEE 16th International Conference on Data Mining (ICDM), IEEE, Dec. 2016. doi: 10.1109/icdm.2016.0096.
[17] K. Shu, A. Sliva, S. Wang, J. Tang, and H. Liu, 'Fake News Detection on Social Media', *ACM SIGKDD Explor. Newsl.*, vol. 19, no. 1, pp. 22–36, Sept. 2017, doi: 10.1145/3137597.3137600.
[18] C. Shao *et al.*, 'Anatomy of an online misinformation network', *PLOS ONE*, vol. 13, no. 4, p. e0196087, Apr. 2018, doi: 10.1371/journal.pone.0196087.
[19] U. Khairatun Hisan and M. Miftahul Amri, 'Artificial Intelligence for Human Life: A Critical Opinion from Medical Bioethics Perspective – Part I', *J. Pub. Heal. Sci.*, vol. 1, no. 02, pp. 100–111, Dec. 2022.
[20] U. Khairatun Hisan and M. Miftahul Amri, 'Artificial Intelligence for Human Life: A Critical Opinion from Medical Bioethics Perspective – Part II', *J. Pub. Heal. Sci.*, vol. 1, no. 02, pp. 112–130, Dec. 2022.
[21] P. Popiel, 'Regulating datafication and platformization: Policy silos and tradeoffs in international platform inquiries', *Policy Internet*, vol. 14, no. 1, pp. 28–46, Mar. 2022, doi: 10.1002/poi3.283.
[22] A. Iliopoulou-Penot, 'Governing the "Governors" of online speech: a review of the Digital Services Act's first steps in regulating social media platforms', *Yearb. Eur. Law*, Oct. 2025, doi: 10.1093/yel/yeaf006.

Authors



Ari Fajar Santoso is a lecturer at Telkom University, Indonesia's Information Systems study program. He has research interests in enterprise architecture, semantic networks, and the TOGAF Framework. In addition, he has also published the results of his research in national and international journals. (email: arifajar@telkomuniversity.ac.id).



Dr. Zafar Khan is a scholar at Abasyn University, Peshawar, Pakistan. He is an Assistant Director, Human Resources, Government of Khyber Pakhtunkhwa Food Safety and Halal Food Authority. His core skills include, but are not limited to, human resource management and talent onboarding, conducting interviews, payroll section handling, ERP management, and HR information system handling. (email: adzafarkhan@outlook.com).