CAUSES AND CONSEQUENCES OF DIGITAL SECURITY BREACHES IN THE AI REGIME: A FEMINIST OUTLOOK

Dr Debabrata Das, Assistant Professor, Department of English, Rabindra Bharati University, Kolkata, West Bengal
Dr Snigdha Naskar, Assistant Professor, Department of Lib. & Inf. Sc., Rabindra Bharati University, Kolkata, West Bengal

Abstract:

The proposed article is primarily focused on exploring the myriad connections between gender perspectives, digital security, identity dynamics, and global governance vis-à-vis the various types of security breaches facilitated by Artificial Intelligence (AI) in India. By thoroughly examining the interrelations between these issues, the present study intends to identify the gendered implications of AI-driven security breaches and their impact on both the process and politics of individuation in the current AI- regime. At the same time, the study plans to assess the impact of such breaches on both the national and global systems of governance. As such, contemporary socio-political realities, at the national as well as global fronts, would automatically come under the critical purview of the current study. Drawing upon academic sources and empirical evidences, the proposed paper would argue that integrating gender perspectives enriches our understanding of security challenges and governance mechanisms, which in turn helps governments frame more inclusive and gender-sensitive policies for their respective nations. Therefore, it becomes imperative on the part of the scholars to recognise the areas and mechanisms of gender vulnerabilities in the digital security system, in order to help the governments as well as individual institutions to identify the possible challenges and also to help them develop adequate measures to counter such menaces more effectively.

Key Words: Gender, Digital, Security Breaches, Identity, Governance.

1. Introduction:

The use of artificial intelligence (AI) in almost every sphere of life has become more common since the last decade. While on the one hand, it has made human life and their activities easier, on the other, the use of it has created a few non-negotiable negatives that are threatening larger damage in the future. The growing implementation of AI-based technologies has sparked serious concerns regarding its applicability across various industries, leading to acute apprehensions. These concerns are further amplified by the potential threats it poses to human rights, notably evident in the wake of gender biases in numerous AI-based applications. While the accomplishment of women's rights has been an arduous journey, still far from being complete, the struggle for gender equality persists even in the current century. The emergence of artificial intelligence technology has introduced another dimension to this ongoing societal challenge. (Chauhan & Kaur, 2022)

In the present study, the main focus has been given on the issue of gender vulnerabilities in the Artificial Intelligence (AI) regime. Artificial Intelligence (AI) refers to the development of computer systems that can perform tasks that normally require human intelligence. This includes activities like learning, reasoning, problem-solving, perception, language understanding, and decision-making. Gender vulnerabilities typically describe the unique challenges, risks, or issues that individuals or groups may face due to their gender. This encompasses a range of concerns, including: Gender-based harassment, cyberbullying, and online abuse often target individuals based on their gender. Women, in particular, might face disproportionate levels of online harassment, including threats, stalking, or derogatory comments, etc. (Hinson et.al. 2)

2. Methodology:

The present paper employs the analysis and examination of existing texts, such as conventions,

protocols, and declarations. To comprehend the issue of gender discrimination concerning AI and to seek potential solutions, the paper also considers findings from various existing studies and research papers authored by different individuals as well as various world-based organisational reports.

3. Review of Literature:

A review of related has been done on the proposed topic of concern. This strives to analyze the existing published literature in areas related to the said study area. Some of the literature pertaining to the gendered vulnerabilities in the AI-regime has been presented here for discussion.

Biswas, Arundhatie, (2023) in her research study entitled "The Great Gender Glitch: Women and Online Violence." focuses on online harassment, this research provides insights into the experiences of Indian women. It examines the role of AI in facilitating harassment and emphasizes the importance of legal and policy measures to combat it. It investigates the link between AI technologies and gender-based violence in India. It discusses the urgent need for AI regulation and ethical considerations to protect women from digital harm.

In the year 2022, Kumar, S., and Choudhury, S. in their article entitled "Gender and feminist considerations in artificial intelligence from a developing-world perspective, with India as a case study" explores the impact of Artificial Intelligence (AI) and robotics on women in developing countries, focusing on India as a case study. The study aims to uncover whether the introduction of AI worsens the challenging circumstances for women in the developing world or if it potentially acts as a force for empowerment. It highlights the lack of research on the impact of AI on women in developing nations, emphasizing the need for more exploration in this area.

Chatterjee, Sheshadri, (2019) in her article "Is Data Privacy a Fundamental Right in India? An Analysis and Recommendations from Policy and Legal Perspective." endeavours to determine whether personal data privacy constitutes a fundamental right in India. Additionally, it offers recommendations to various relevant authorities regarding safeguarding personal information on online platforms.

4. Connections among Gender Perspectives, Digital Security and Global Governance:

The interrelation between gender perspectives, digital security, and global governance is a multifaceted and complex subject. The dynamics among these elements encompass issues of inclusivity, privacy, and policy frameworks.

In the Indian context, the interrelation between gender disparity, digital security, and governance is multifaceted, impacting various aspects of societal and technological developments. These aspects may be classified in the following manner:

- **Gender Disparity in terms of Access to Technology:** There exists a significant gender gap in the access to digital technology, particularly in rural and marginalized communities. This disparity influences the effectiveness of digital security measures, as certain gender groups may be more vulnerable due to limited access. (Nikore & Uppadhayay, 2021)
- **Digital Security Concerns for Women:** Women in India often face unique digital security concerns, including online harassment and privacy infringements. Insufficient digital literacy and gender-based vulnerabilities can exacerbate risks, influencing governance policies regarding online safety. (*Cyber Security Challenges for Women*, 2023)
- **Impact on Governance Policies, Data Privacy and Gender-Specific Concerns:** Gender disparities and vulnerabilities in digital security can influence governance policies. For instance, it might prompt the government to introduce policies focused on enhancing digital literacy and ensuring safety for women in digital spaces. Governance frameworks need to address gender-specific data privacy concerns, especially in sectors like healthcare, where sensitive gender-specific information may be at risk. Policies safeguarding such data can influence governance and security measures. (*The Personal Data Protection Bill*, 2019)
- **Representation in Governance and Security Measures:** Inclusion of diverse gender perspectives in governance and security measures is crucial. Gender disparity might affect representation in

ISSN: 2278-4632
Vol-13, Issue-11, No.03, November: 2023

decision-making processes, impacting the formulation and implementation of policies related to digital security (Gurumurthy, 2014). One significant worry revolves around generative AI's contribution to the proliferation of deep-fakes convincing yet artificial videos crafted by AI algorithms trained on vast online content. These deep-fakes often appear on social media, blurring the line between fact and fiction, particularly in the realm of politics. (*Rapid AI Proliferation Is a Threat to Democracy*, 2023)

5. Impact of AI-driven Security Breaches:

AI-driven security breaches have profound impacts on both national and global systems of governance, affecting policy, geopolitics, and international relations. AI-driven security breaches have direct impact on national security, geopolitical relations, legal and regulatory changes, citizen perception, etc.

- **National Security and Policies:** Security breaches caused by AI can compromise national security, affecting critical infrastructure, defence systems, and confidential information. AI can facilitate the theft of sensitive government and military data, including classified information. State-sponsored actors and cybercriminals may exploit AI techniques to breach government databases, compromising national security. (Kello, 2016).
- **Geopolitical Relations:** Breaches affecting national or global systems can strain diplomatic relations. The attribution of cyber attacks and breaches is often complex, leading to geopolitical tensions and accusations between nations. This can influence alliances, trade relationships, and international cooperation. Global governance systems, such as international organizations and agreements, are also vulnerable to AI-driven security breaches. (Segal, 2017)
- **Legal and Regulatory Changes:** High-profile breaches often lead to changes in laws and regulations. Governments might enact new cyber security legislation, imposing stricter compliance measures on both public and private sectors to prevent future breaches. AI-powered cyber attacks can target critical national infrastructure such as power grids, water supply systems, and transportation networks. These attacks can disrupt essential services, leading to widespread chaos and economic damage. (*The General Data Protection Regulation, 2022*)
- **Trust and Citizen Perception:** Security breaches can erode public trust in governance systems. If governments fail to protect sensitive information, citizens may lose faith in their ability to govern securely. Rebuilding this trust becomes a crucial aspect of governance. AI-driven social engineering attacks can manipulate public opinion, influence elections, and spread disinformation. These tactics can destabilize the political landscape and undermine trust in the government. (Olmstead & Smith, 2017)

6. Gendered Implications of AI-Driven Security Breaches

The gendered implications of AI-driven security breaches are a multifaceted issue that has far-reaching consequences on both the process and politics of individuation in the current AI regime. Gender vulnerabilities in AI-driven digital security systems highlight how certain groups or individuals may be disproportionately affected by security flaws or biases. Some key areas of vulnerability and gendered implications of AI-driven security breaches include:

- **Impacts on Digital Autonomy:** Digital autonomy, or the ability to control one's online presence and data, is critical in the IA regime. Gendered implications arise when women are disproportionately affected by AI-driven security breaches, as it erodes their sense of digital autonomy. For example, the fear of having personal information exposed or manipulated can discourage women from fully participating in online spaces, limiting their ability to engage in political discourse and individual expression. (Kumar & Choudhury, 2022)
- **Reinforcement of Gender Stereotypes:** AI algorithms, which are often trained on biased datasets, can perpetuate harmful gender stereotypes. Security breaches involving AI can exploit these biases to target individuals based on their gender, further perpetuating discrimination and reinforcing

societal norms. This can have a profound impact on the politics of individuation, as individuals may feel under pressure to conform to these stereotypes in their online behaviour to avoid being targeted. Gender-specific needs or vulnerabilities may be inadequately represented in the design of security systems, leading to systems that don't effectively account for the risks faced by different genders. (Buolamwini & Gebru, 2018)

- **Biased Algorithms in Cyber security:** AI algorithms used in cyber security may inadvertently perpetuate gender biases. For instance, these algorithms might flag certain behaviours more frequently in one gender compared to others, leading to discriminatory outcomes in security monitoring or threat assessments. A recent study conducted by a team of psychology researchers reveals that even when internet searches are geared towards gender neutrality, the results tend to favour male-centric outcomes. These search results not only perpetuate gender bias but also hold the potential to sway hiring decisions by influencing users. Published in the journal Proceedings of the National Academy of Sciences (PNAS), this research adds to the growing body of evidence showcasing how artificial intelligence (AI) can significantly shape our perceptions and behaviours (Devitt, 2022).
- **Online Harassment and Gender-Based Violence:** AI-driven security breaches can escalate online harassment and gender-based violence, which disproportionately affect women. Perpetrators can use AI tools to amplify their attacks, making them more sophisticated and difficult to combat. This not only hinders the process of individuation but also discourages women from participating in digital spaces, limiting their political agency and voice. The use of AI in surveillance systems and data analysis can raise significant privacy concerns. Women may be disproportionately affected as they often face gender-specific privacy threats, such as non-consensual image sharing (revenge porn) or stalking facilitated by AI-powered tracking technologies. Women, especially, are more likely to face online harassment and privacy infringements. AI-driven systems that fail to adequately address or protect against such harassment can leave women vulnerable to online threats and breaches of privacy. The AI clothing remover stands as a pioneering technology employing advanced artificial intelligence algorithms to digitally strip individuals of their clothing in photos. It harnesses specialized deep-learning models that have been meticulously trained to discern and comprehend various clothing components such as shirts, pants, and dresses with precision. Through analyzing visual cues and patterns, these algorithms skilfully recognize and remove clothing while maintaining the natural body contours beneath. Originally designed to aid the fashion and entertainment sectors, this technology is now being repurposed for the creation of deep-fake nude images (Ali, 2023). When AI is exploited in security breaches, it can exacerbate these gender-based vulnerabilities, leading to more severe consequences for women. (Biswas, 2023)
- **Trust Deficit and Technological Withdrawal:** When individuals, particularly women, repeatedly experience AI-driven security breaches, it can erode their trust in digital technologies and platforms. This trust deficit can lead to technological withdrawal, where individuals disengage from online activities to protect their privacy and security. This withdrawal can have political implications, as it may lead to a reduction in civic engagement and participation.
- **Policy and Legal Gaps:** The gendered implications of AI-driven security breaches highlight policy and legal gaps in addressing these issues. Existing laws and regulations may not adequately protect individuals from these emerging threats. Policymakers must consider the gendered dimension of security breaches when developing and implementing cyber security policies.

7. Use of AI in India

Artificial intelligence (AI) has been rapidly gaining traction in India across various sectors. From healthcare and agriculture to finance and education, AI is revolutionizing processes, making them more efficient and innovative. In healthcare, AI is being utilized for diagnostics, predictive analytics, and personalized medicine. Start-ups like Practo, SigTuple are using AI to analyze medical

images, while companies like NIRAMAI are developing AI-based solutions for early breast cancer detection using thermography and machine learning. In agriculture, AgNext AI is aiding farmers in optimizing crop yields and managing resources efficiently. Companies like CropIn and RML AgTech provide AI-powered solutions for crop monitoring, disease detection, and yield prediction. Financial sectors are adopting AI for fraud detection, risk assessment, and customer service. Finance tech companies like ZestMoney, Paytm use AI algorithms to assess creditworthiness, facilitating access to credit for many who were previously underserved. In education, AI is enhancing learning experiences through personalized learning platforms. Ed-tech start-ups like BYJU'S and Unacademy use AI to create personalized learning paths for students. In customer service Haptik integrates AI in conversational chatbots, providing customer support and engagement for various businesses. GreyOrange implements AI-driven robotics and automation in warehouses, optimizing logistics and supply chain management in manufacturing sectors. Cisco and IBM have implemented AI solutions in Indian smart city projects for traffic management, waste management, and energy efficiency. (Khan, 2023)

8. Mitigating AI-Driven Security Breaches in India

The integration of gender perspectives in AI security is a crucial step towards ensuring fairness, equity, and mitigating biases in technological systems. Several strategies can be implemented to address gender perspectives in AI security. To mitigate security breaches by AI in both national and global governance systems, the Indian government may consider the following measures:

- **Strengthen Cyber Security:** Enhance cyber security measures for critical infrastructure, government agencies, and diplomatic communication. Invest in AI-powered defence systems to detect and respond to threats effectively.
- **Regulation and Oversight:** Develop robust regulatory frameworks to govern AI developments and uses, ensuring that ethical and security standards are adhered to. Collaborate with international partners to establish global norms for AI in security.
- **International Cooperation:** Engage in international cooperation on cyber security and AI governance. Participate in multilateral discussions and agreements to address global security challenges posed by AI.
- **Invest in AI Defence:** Allocate resources for the development of AI-powered security solutions that can proactively identify and mitigate threats.
- **Promote Ethical AI:** Encourage responsible development and use of AI, emphasizing ethical considerations, transparency, and accountability.
- **Diverse and Representative Data:** Ensuring diverse and representative datasets is critical in training AI systems. By including a wide range of gender identities and demographics, the systems can better recognize and represent various genders.
- **Algorithmic Fairness:** Implementing fairness metrics and techniques within AI algorithms to reduce biases. Techniques like adversarial de-biasing or re-weighting training examples can help mitigate gender-based biases in AI models.
- **Transparency and Explainability:** Developing AI systems that can explain their decision-making processes can aid in identifying and rectifying gender biases. Interpretable AI models can help ensure transparency and accountability in the outcomes they produce. Conducting gender impact assessments on AI systems, similar to environmental or societal impact assessments, can help in identifying potential gender biases and mitigating them before deployment. Such assessments could be integral to AI development processes.

By integrating gender perspectives into AI security through these strategies, the aim would be to build more ethical, fair, and inclusive AI systems that do not perpetuate or exacerbate gender-based biases.

9. Conclusion:

Thus, the gendered implications of the AI-driven security breaches constitute an extremely

crucial subject that requires immediate attention, since it is intricately linked to the question of self-fashioning and also to the process of self-actualization. These implications include privacy violations, impacts on digital autonomy, reinforcement of gender stereotypes, online harassment, trust deficits, and policy gaps. The gender perspectives of security breaches facilitated by AI in India, and also across the globe, are inevitably intertwined with broader issues of online harassment, privacy, bias, and discrimination. Therefore, the urgent need of the time is to develop appropriate regulatory measures, ensure ethical AI development, and frame gender-inclusive policies, in order to address these challenges effectively and also to promote gender equality in the ongoing AI regime.

Endnotes:

Ali, Nayem (2023, Aug 17) *AI being used to make deepfakes spark online harassment concerns. What does the law say? | The Business Standard*. (2023). Retrieved November 2, 2023, from https://www.tbsnews.net/tech/ai-being-used-make-deepfakes-spark-online-harassment-concerns-what-does-law-say-683950

Bapna, N. (2016). Draft National Policy for Women, 2016: Repeating Old Themes. *Economic and Political Weekly*, *51*(35), 22–25.

Biswas, A. (2023, Mar 8). *The Great Gender Glitch: Women and Online Violence*. ORF. Retrieved November 2, 2023, from https://www.orfonline.org/expert-speak/the-great-gender-glitch/

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 77–91. https://proceedings.mlr.press/v81/buolamwini18a.html

Chatterjee, S. (2019). Is data privacy a fundamental right in India? An analysis and recommendations from policy and legal perspective. *International Journal of Law and Management*, *61*(1), 170–190. https://doi.org/10.1108/IJLMA-01-2018-0013

Chauhan, P., & Kaur, G. (2022). Gender Bias and Artificial Intelligence: A Challenge within the Periphery of Human Rights. *Hasanuddin Law Review*, *8*, 46. https://doi.org/10.20956/halrev.v8i1.3569

Cyber Security Challenges for Women. (2023). National Law School of India University. Retrieved November 2, 2023, from https://www.nls.ac.in/projects/cyber-security-challenges-for-women/

Devitt, J. (2022). *Gender Bias in Search Algorithms Has Effect on Users, New Study Finds*. New York University Web Communications. Retrieved November 13, 2023, from http://www.nyu.edu/content/nyu/en/about/news-publications/news/2022/july/gender-bias-in-search-algorithms-has-effect-on-users--new-study-

Gurumurthy, A., & Chami, N. (2014). *Digital Technologies and Gender Justice in India -An analysis of key policy and programming concerns Input to the High Level Committee on the Status of Women in India, 1-51*.

Hinson, Laura et. al. (2018). *Technology-facilitated gender-based violence: What is it, and how do we measure it?*, Washington D.C., International Center for Research on Women, 2.

Kello, L. (2016). *Private-Sector Cyberweapons: Strategic and Other Consequences*, 1-25, (SSRN Scholarly Paper 2836196). https://doi.org/10.2139/ssrn.2836196

Khan, A. (2023, May 12). *Artificial Intelligence in India*. Intellipaat Blog. https://intellipaat.com/blog/artificial-intelligence-in-india/

Kumar, S., Choudhury, S. (2022). *Gender and feminist considerations in artificial intelligence from a developing-world perspective, with India as a case study | Humanities and Social Sciences Communications*. Retrieved November 3, 2023, from https://www.nature.com/articles/s41599-022-01043-5

Nikore, M., Uppadhayay, I. (2021). *India's gendered digital divide: How the absence of digital access is leaving women behind*. ORF Observer Research Foundation. Retrieved November 3, 2023, from https://www.orfonline.org/expert-speak/indias-gendered-digital-divide/

Olmstead, K., & Smith, A. (2017). *Americans and Cybersecurity*. Pew Research Center, 1-43.

Rapid AI proliferation is a threat to democracy, experts say. (2023, November 9). The Business Standard. https://www.tbsnews.net/tech/rapid-ai-proliferation-threat-democracy-experts-say-736018

Safeguarding fundamental rights in the digital age. (2022, February 25). European Union Agency for Fundamental Rights. http://fra.europa.eu/en/speech/2022/safeguarding-fundamental-rights-digital-age

Segal, A. (2017). *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (2nd ed.). Perseus Books, 320.

The general data protection regulation. (2022, September 1). https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/

The Personal Data Protection Bill. (2019). PRS Legislative Research. Retrieved November 13, 2023, from https://prsindia.org/billtrack/the-personal-data-protection-bill-2019

https://www.unwomen.org/en/news/stories/2015/9/cyber-violence-report-press-release

Women—Cyber Laws in India. (2023). ISEA. Retrieved November 3, 2023, from https://www.infosecawareness.in/concept/cyber-laws-in-india/women

