Role of AI in Elections

Why in news?

The potential of AI in elections cannot be dismissed as the world is going to witness series of elections to be held across in 2024.

What is the significance of AI in elections?

- **Instant responses-** AI can enable political campaigns to respond instantly to developments, creating videos, speeches, or press releases in real-time which can influence voter perceptions and campaign dynamics.
- **Precise targeting**- AI can analyse vast amounts of microdata to target specific voter demographic with personalised messages which can be crucial in swaying undecided voters.
- **Campaign efficiency**- AI helps campaigns to micro-target potential voters, analyse data, and predict outcomes more efficiently, leading to more effective campaign strategies.
- **Efficiency-**AI can speed up and improve the cost-effectiveness of information operations, helping to analyse large amounts of data and predict outcomes.
- **Voter information**-AI can provide voters with targeted information about candidates and political parties, potentially increasing informed participation.
- **Election administration-** AI tools can assist in managing and securing the election process, making it more robust against fraud.

What are the challenges of AI in elections?

- **Deep fake elections**- There is a warning about the increased risk of AI-generated disinformation, which could *compromise the voters' capacity* to distinguish between what is true and what is false.

  World Economic Forum's Global Risks Perception Survey, ranks misinformation and disinformation among the top 10 risks

- **Misleading voters**- The use of AI in fake audio and video would create *misleading propaganda* and the inevitability of deep fakes in future elections.
- **Cheap production**- Generative AI have made deepfake production *cheaper and more sophisticated*, enabling the creation of hyper-realistic fake images, videos, and audio within seconds at minimal cost.
- **Cloned celebrity voices**- The combination of cloned celebrity voices with social media algorithms allows for targeted dissemination of *misinformation*, potentially distorting election outcomes.

- **Disinformation**- World Economic Forum has warned that disinformation in elections could destabilise societies by discrediting and questioning the legitimacy of governments
- **Impact of generative AI**- PNAS Nexus study predicts that disinformation campaigns will increasingly use generative AI to propagate election falsehoods.
- **Disrupt democracies-** AI technologies, particularly when used maliciously, can disrupt democratic processes through various means, such as the spread of misinformation, *manipulation of public opinion*, and *interference in electoral systems*.
- **Affect election integrity-** The AI generated disinformation has affected the past elections in Argentina and Slovakia.
- **Unreliability**- Despite advancements in AI may exhibit *biases, errors or unexpected behaviour* leading to inaccuracies and unintended consequences in their applications.
- **Data driven politics**- Pew survey cited that a majority of Indians support 'authoritarianism,' which could be exploited by those using AI to influence the electorate.
- **Mischief potential**-AI's capability to cause *unintended harm*, known as 'mischief potential,' is a significant concern, especially as reliance on AI solutions grows.
- **AI hallucinations**-Experts warn about AI's 'hallucinations,' where AI systems *fabricate solutions to new problems*, leading to probabilistic and often inaccurate results.
- **Dependability concern**- The current AI models can be unreliable, and overreliance on them may be problematic without suitable mitigation strategies.
- **Lack of regulation**- The Election Commission lacks specific guidelines for addressing deepfake threats, although the government is considering new policies for AI technologies.
- **Security risk**- The emergence of adversarial capabilities in AI such as ***poisoning*** (intentional corruption of training data), ***back dooring*** (insert malicious functionality in AI) and ***evasion*** (exploit weakness or blind spots in AI) poses significant security risk.

What are the steps taken to counter the challenges of AI in elections?

- **Advisory**- Recently Ministry of Electronics and Information Technology had issued an advisory that demands the social media intermediaries and platforms must ensure that their AI tools do not allow any bias or discrimination or threaten the integrity of electoral process.
- **Self-censorship**- AI platforms are implementing restrictions on the types of political queries they respond to, aiming to avoid generating responses that could provoke controversy or anger political leaders.
- **Code-level censorship-** The self-censorship is achieved through *algorithmic filters* that prevent AI platforms from generating responses to queries containing specific keywords.
- **Limited response-** Google's chatbot Gemini is limiting responses to election-related queries in India, providing *standard non-answers* to avoid controversy.

What lies ahead?

- The issues must be addressed holistically by involving multiple stakeholders who can help mitigate the negative impacts of AI while maximizing its potential benefits for the society.
- The Google's AI models Gemini has faced criticism for inaccuracies in historical image generation and varying responses to questions about world leaders highlight the importance of public awareness and the need for scepticism towards AI and AGI (Artificial General Intelligence).
- The regulators must strike a balance between countering AI-linked misinformation and fostering innovation in the AI industry.

References

1. The Hindu- AI's dark dimension in elections
2. Indian Express- Self censorship of political speech
3. Indian Express- AI on election disinformation

SHANKAR IAS PARLIAMENT
Information is Empowering