

REGULATORY

The nexus: Disinformation, Misinformation, and Privacy in the Age of Gen AI

13 June 2024 4 min read

The risks associated with disinformation and misinformation have reached heights never seen before in the era of Generation AI (Gen AI), where artificial intelligence (AI) technologies filter into every facet of life. Amidst the conversation surrounding these threats, a crucial aspect often overlooked is the intersection with privacy concerns.

The prevalence of false information in the digital age has introduced numerous challenges that affect individuals, communities, and societies. False information undermines trust in traditional sources of news and information, such as media outlets and authoritative institutions. When individuals are exposed to misleading or fabricated content, they may become skeptical of all information sources, leading to a breakdown in trust within society. Disinformation campaigns often exploit existing social divisions and amplify ideological differences, leading to increased division within communities. By spreading divisive narratives and inciting conflict, false information can undermine social cohesion and hinder efforts to bridge divides. At the same time, misinformation about for instance health-related topics, such as vaccines, treatments, and pandemics, can have serious public health consequences. False information can lead to decreased vaccination rates, the spread of preventable diseases, and confusion about public health guidelines, putting individuals and communities at risk.

The rapid advancement of technology, including AI-generated content and deepfake technology, presents challenges for detecting and combating false information. It is therefore imperative to recognise the intricate relationship between disinformation, misinformation, privacy, and the broader implications for society.

Disinformation and misinformation exploit vulnerabilities in the digital ecosystem to spread false narratives, manipulate public opinion, and undermine trust. Whether it is through AI-generated fake news articles, manipulated images and videos, or orchestrated social media campaigns, the dissemination of false information poses a significant threat to democratic processes, social cohesion, and individual autonomy.

Simultaneously, the collection and analysis of personal data by AI systems raise intense privacy concerns. From targeted advertising, algorithmic discrimination to secret surveillance and data breaches, the potential erosion of privacy rights in the digital age has far-reaching implications for individuals. This relates to freedoms, autonomy, and dignity.

Disinformation and privacy concerns together, create a volatile mix. On one hand, the proliferation of false information can exploit personal data to craft more convincing and targeted disinformation campaigns. By leveraging insights gleaned from individuals' online behaviours, preferences, and vulnerabilities, malicious actors can tailor their messaging to maximize its impact and effectiveness.

Equally, the erosion of privacy rights can worsen the spread of misinformation by facilitating the unchecked collection and dissemination of personal information. When individuals' privacy is compromised, they become more susceptible to manipulation, exploitation, and coercion, making them prime targets for disinformation campaigns designed to exploit, amongst others, their biases, and fears.

Considering these intertwined challenges, safeguarding privacy rights is essential to mitigating the risks associated with disinformation and misinformation. This requires a multifaceted approach that addresses the underlying dynamics driving

both disinformation and misinformation, while upholding the principles of transparency, accountability, and individual autonomy.

First and foremost, this is informed by privacy laws and enforcement mechanisms that ensure that individuals have greater control over their personal information and how it is used. The Protection of Personal Information Act, 2013 (POPIA) empowers individuals to exercise their rights and hold organisations accountable for data misuse.

POPIA requires that technology companies and platform operators act in a responsible manner, taking into consideration to requirements of POPIA, when they design AI systems and algorithms. AI systems must prioritize privacy, transparency, and ethical considerations. This includes implementing privacy-enhancing technologies, such as differential privacy learning, to minimize the collection and storage of sensitive personal information/data, while enabling meaningful insights.

But most importantly, enhancing digital literacy and media literacy education is crucial to equipping individuals with the skills and knowledge to critically evaluate information, the sources of information, distinguish between misinformation and truth, and protect their privacy online.

As society confronts the challenges posed by disinformation and misinformation, it is imperative to recognise the underlying connection with privacy concerns. Only through concerted efforts to promote privacy rights, digital literacy, and ethical AI practices can the complex terrain of disinformation and misinformation be navigated, while safeguarding the fundamental rights and freedoms of all individuals.

Often the surest way to convey misinformation is to tell the strict truth.

~Mark Twain



Ahmore Burger-Smidt

Head of Regulatory

[View Profile](#)