BACKGROUND GUIDE

LPS G20 MODEL | ETHICS IN TECHNOLOGY

Agenda: Ethical use of technology in modern-day

Welcome Note from the Executive Board

Dear Delegates,
Welcome to the G20 Summit on Ethics in Technology! As representatives of your respective nations, you are tasked with navigating complex discussions on AI, digital privacy, misinformation, and cybersecurity. This study guide provides a foundation for understanding the ethical challenges and G20 perspectives on these critical topics.
We encourage you to explore the additional resources provided, engage in meaningful discussions, and collaborate to propose viable solutions. The future of technology governance lies in your hands, and we look forward to seeing the depth of insight you bring to the table.
Best regards,
The Executive Board

Introduction

The rapid advancement of technology in the 21st century has transformed industries and societies, bringing both opportunities and ethical challenges.

- AI-generated content has raised concerns about intellectual property, transparency, and the future of human creativity. The G20 supports responsible AI development while ensuring human-centered innovation.
- Digital privacy is another pressing issue, with tech giants like Meta and TikTok collecting vast amounts of user data, often without full transparency. The

challenge is balancing regulation with innovation, prompting the G20 to emphasize data protection and privacy rights.

- Misinformation spread through digital platforms influences public opinion and can pose national security risks. While combating fake news is essential, it must align with free speech protections. The G20 encourages platform transparency and responsible digital governance.
- Cybersecurity threats, from ransomware attacks to state-sponsored hacking, endanger critical infrastructure and economies. Strengthening global cooperation is essential to safeguarding digital spaces, making cybersecurity a priority for the G20.

Despite differences in national interests, the G20 fosters dialogue to develop ethical technology policies, ensuring a secure and inclusive digital future.

Key Discussion Areas

1. AI & Copyright: Ethics of AI-Generated Content

Introduction:

As artificial intelligence continues to reshape industries—ranging from media and entertainment to research and education—questions of copyright, authorship, and ethical responsibility have gained prominence. The G20, representing the world's largest economies, is crucial in shaping international frameworks to balance innovation with intellectual property rights. In today's world, where AI-generated art, music, and literature challenge traditional notions of creativity, policymakers must navigate the complexities of ownership, fair use, and accountability while ensuring that AI development remains ethical, transparent, and beneficial to all.

Key Questions:

1. Should AI-generated content be labeled?
2. How does AI-generated content impact creativity and intellectual property rights?
3. What legal frameworks should govern AI-created works?

G20 Perspective:

A key concern for the G20 is the question of authorship and accountability. Traditional copyright laws are designed to protect human creators, but AI challenges this notion. Some G20 nations propose a "hybrid model," where AI-generated works are co-attributed to both the AI system and the human who trained or guided it. Ethical considerations also extend to ensuring that AI does not infringe upon existing copyrighted works, raising concerns about plagiarism, unauthorized reproductions, and deepfakes.

Case Studies:

1. Meta's Use of Pirated Books for AI Training
   - In March 2025, it was revealed that Meta utilized a database containing pirated books, known as The Library Genesis, to train its AI models. This database hosts over 7.5 million books, including works by prominent authors such as Ta-Nehisi Coates and Sarah Silverman. The authors have filed a lawsuit against Meta, alleging copyright infringement. Meta contends that its use of these materials falls under the "fair use" doctrine, asserting that the data was transformed for purposes like personal tutoring and creative tasks without replicating the books themselves.
2. U.S. Appeals Court Denies Copyright for AI-Generated Art
   - In March 2025, the U.S. Court of Appeals for the District of Columbia Circuit upheld a decision by the U.S. Copyright Office, ruling that art created solely by AI without human input does not qualify for copyright protection.

---

2. Digital Privacy: Data Collection & Inclusion

Introduction:

G20 nations play a pivotal role in shaping policies that balance innovation, security, and individual rights. With increasing reliance on big data for decision-making, concerns over data ownership, surveillance, and algorithmic biases have intensified. The challenge for the G20 is to establish inclusive, transparent, and ethical frameworks that protect user privacy while ensuring equitable access to digital resources. In an era where data is often referred to as the "new oil," safeguarding digital privacy is not just a legal obligation but a fundamental aspect of maintaining trust in the digital age.

Key Questions:

1. How do tech companies collect and use data?
2. What policies ensure user privacy and digital inclusion?
3. How can nations balance privacy protection with technological innovation?

G20 Perspective:

G20 nations acknowledge the economic and societal benefits of data collection, particularly for AI, healthcare, smart cities, and digital finance. However, unregulated data collection poses risks such as identity theft, mass surveillance, and data monopolization by tech giants. Countries like the European Union, through the General Data Protection Regulation (GDPR), emphasize strict privacy laws, while others, like the U.S. and India, focus on sector-specific regulations. The G20 seeks to establish a middle ground where innovation thrives without compromising user rights.

Case Studies:

1. FTC Actions Against Data Brokers for Unlawful Tracking
    - In December 2024, the U.S. Federal Trade Commission (FTC) took action against data brokers Mobilewalla and Gravy Analytics for illegally collecting and selling sensitive location data. These companies tracked individuals around sensitive sites, including churches and military bases, and sold the data for purposes such as advertising and government use.
2. Australian Car Manufacturers' Data Collection Practices Under Scrutiny
    - An October 2024 investigation by Choice revealed that several top car manufacturers in Australia, including Kia, Hyundai, and Tesla, were collecting and sharing driver data with third parties. The data collected ranged from voice recognition inputs to video clips from in-car cameras. This raised concerns about consumer privacy and the adequacy of existing Australian privacy laws, prompting calls for stronger regulations to ensure data safety and transparency.

---

3. **Misinformation Control vs. Free Speech**

Introduction:

As misinformation proliferates across social media and online platforms, governments and tech companies face increasing pressure to regulate content while upholding free speech. The G20, as a global economic and political forum, plays a crucial role in shaping policies that balance misinformation control with the fundamental right to freedom of expression. While some nations advocate for stricter regulations to combat fake news, others warn against potential censorship and the suppression of diverse viewpoints. The challenge lies in developing transparent, accountable, and rights-based frameworks that prevent harm without stifling open discourse in the digital age.

Key Questions:

1. How can misinformation be tackled without infringing on free speech?
2. What role do social media platforms play in regulating misinformation?
3. What frameworks can ensure transparency in content moderation?

G20 Perspective:

While controlling misinformation is critical, G20 nations also recognize that excessive regulation can infringe on free speech and democratic debate. Countries with strict censorship laws often justify content restrictions as measures against misinformation, raising concerns about political repression. To prevent misuse, G20 discussions focus on transparent, accountable, and rights-based regulatory approaches that differentiate harmful misinformation from legitimate political discourse and diverse opinions.

Case Studies:

1. Arrests in India for Disseminating Deepfake Videos of Politicians
    - In November 2023, Indore police registered four First Information Reports (FIRs) against unidentified individuals for circulating deepfake videos of prominent politicians, including Prime Minister Narendra Modi. One such video depicted the Prime Minister laughing during a serious address, aiming to tarnish his image.
2. Europol's Warning on AI-Facilitated Criminal Activities
    - In March 2025, Europol raised alarms about the increasing use of artificial intelligence (AI) by criminal networks acting on behalf of hostile state actors like Russia and China. These AI-driven attacks enhance the speed, reach, and sophistication of criminal operations, including creating sophisticated malware, deceiving victims through synthetic media, and conducting targeted cyberattacks on governments and critical infrastructure.

4. Cybersecurity: Global Cooperation Against Threats

Introduction:

In today's interconnected digital world, cybersecurity threats pose significant risks to national security, economic stability, and public safety. Cyberattacks, ranging from ransomware attacks on critical infrastructure to state-sponsored espionage, have escalated in both scale and sophistication. As cyber threats transcend national borders, no single country can tackle them alone. However, challenges such as differing legal frameworks, geopolitical tensions, and evolving cyber risks make collaboration complex, necessitating a balanced approach to security, privacy, and technological innovation.

Key Questions:

1. How can nations collaborate to enhance cybersecurity?
2. What policies should regulate cyber defense strategies?
3. How can nations strengthen resilience against cyberattacks?

G20 Perspective:

Cybersecurity has become a key global priority, with threats ranging from ransomware attacks and financial fraud to state-sponsored cyber espionage and critical infrastructure sabotage. Given that cyber threats transcend national borders, the G20 plays a crucial role in fostering international cooperation to build a secure digital environment while maintaining economic growth and innovation. The G20's cybersecurity approach focuses on global collaboration, regulatory harmonization, intelligence sharing, and public-private partnerships to mitigate cyber risks effectively.

Case Studies:

1. Russian-Linked Sabotage and Cyberattacks Across Europe
    - Since the invasion of Ukraine, Western officials have attributed a series of sabotage incidents and cyberattacks across Europe to Russian operatives. The Associated Press documented 59 such events, encompassing cyberattacks, arson, and infrastructure sabotage. These actions are believed to be part of a coordinated effort to sow discord, undermine support for Ukraine, and destabilize European governments.

2. Surge in Digital Financial Scams Amid India’s Digital Payment Boom
    - India’s rapid adoption of digital payments has been accompanied by a rise in sophisticated financial scams. Scammers are employing advanced technologies, including artificial intelligence and deepfake techniques, to defraud individuals and businesses. The Indian finance ministry reported a significant increase in high-value cyber fraud cases, emphasizing the need for robust cybersecurity measures and public awareness.

Country-Specific Positions

1.Argentina:

- Supports AI development but prioritizes human labor.
- Advocates for digital inclusion and fair data policies.
- Strengthens cybersecurity cooperation within Latin America.
- Encourages social media regulation against misinformation.
- Invests in AI for economic growth.

2.Australia:

- Supports AI labeling and ethical frameworks.
- Enforces strict data privacy regulations.
- Advocates for platform responsibility in misinformation.
- Strengthens cybersecurity strategies with global partners.
- Invests in AI research and digital innovation.

3.Brazil:

- Calls for platform transparency and misinformation control.
- Prioritizes digital inclusion and fair internet governance.
- Strengthens data privacy through national regulations.
- Encourages AI for public welfare and economic growth.
- Invests in cybersecurity infrastructure.

4.Canada:

- Enforces ethical AI standards and policies.
- Strong advocate for digital privacy and user rights.
- Supports global cybersecurity cooperation.
- Regulates misinformation on social platforms.
- Promotes digital innovation with responsible governance.

5.China:

- Implements strict content monitoring policies.
- Expands state-controlled data collection frameworks.
- Regulates misinformation through government oversight.
- Leads in AI innovation under state supervision.
- Strengthens cybersecurity defenses against external threats.

6.France:

- Hosted the 2025 Paris AI Summit for ethical AI governance.
- Enforces strong digital privacy regulations (GDPR alignment).
- Invests in AI to boost the labor market.
- Regulates misinformation and deepfakes.
- Strengthens cybersecurity frameworks.

7.Germany:

- Supports AI-driven innovation with ethical oversight.
- Advocates for digital privacy under GDPR.
- Focuses on misinformation control while protecting free speech.
- Develops robust cybersecurity frameworks.
- Invests in responsible AI deployment.

8.India:

- Supports AI for social good and economic inclusion.
- Strengthens national data protection policies.
- Encourages responsible AI use in industries.
- Advocates for platform transparency in misinformation control.
- Invests in cybersecurity and digital safety.

9.Indonesia:

- Supports AI-driven economic transformation.
- Strengthens cybersecurity infrastructure for financial security.
- Advocates for inclusive digital policies.
- Works on misinformation control with regional partners.
- Invests in digital education and AI research.

10.Italy:

- Promotes responsible AI development in business sectors.
- Advocates for stringent data privacy laws.
- Supports EU-wide initiatives on misinformation regulation.
- Strengthens cybersecurity measures in public infrastructure.
- Encourages AI research and ethical frameworks.

11.Japan:

- Leads in AI safety research and development.
- Enforces strict data privacy laws and security protocols.
- Advocates for international cooperation against cyber threats.
- Supports platform transparency on misinformation control.
- Invests in ethical AI for social and economic benefits.

12.Mexico:

- Encourages AI growth while balancing labor rights.
- Strengthens data protection and digital privacy laws.
- Regulates misinformation through independent bodies.
- Invests in cybersecurity for national security.
- Supports AI-driven education and innovation programs.

13.Russia:

- Develops state-controlled AI technologies.
- Strengthens cybersecurity against global threats.
- Implements strict data monitoring policies.
- Regulates misinformation through controlled media.
- Invests in AI for national security and defense.

14.Saudi Arabia:

- Prioritizes AI for economic diversification.
- Invests in strong cybersecurity defense systems.
- Develops AI-powered misinformation control frameworks.
- Enforces strict digital content monitoring.
- Supports international cooperation on AI ethics.

15.South Africa:

- Promotes AI for social development and public welfare.
- Strengthens cybersecurity strategies for financial security.
- Advocates for responsible data usage in digital platforms.
- Works on misinformation control policies.
- Invests in AI research for innovation and job creation.

16.South Korea:

- Leads in AI and robotics innovation.
- Enforces strong digital privacy protections.
- Supports misinformation control policies without limiting speech.
- Strengthens cybersecurity cooperation with global allies.
- Encourages ethical AI development.

17.Turkey:

- Invests in AI for national security and defense.
- Develop strong cybersecurity frameworks.
- Advocates for misinformation control on digital platforms.
- Promotes ethical AI in government and business sectors.
- Strengthens international cooperation on technology ethics.

18.United Kingdom:

- Pushes for AI regulation for ethical use.
- Enforces strict digital privacy laws.
- Advocates for platform transparency in content moderation.
- Focuses on cybersecurity against cyber espionage.
- Encourages ethical AI safety development.

19.United States:

- Supports AI labeling and ethical guidelines.
- Advocates for strong digital privacy protections.
- Leads cybersecurity initiatives with allies.
- Promotes free speech while combating misinformation.
- Invests in AI safety research.

20.European Union (EU):

- Enforces GDPR as a global standard for privacy.
- Supports ethical AI development and sustainability.
- Regulates misinformation through legal policies.
- Promotes cybersecurity cooperation among member states.
- Invests in responsible AI governance frameworks.

21. African Union:

- Supports AI development with clear ethical guidelines to prevent digital colonization by major tech firms.
- Advocates for stringent data privacy laws to protect African users from exploitation by international corporations.
- Calls for balanced misinformation policies that do not restrict press freedom or political expression.
- Seeks international cooperation for cybersecurity infrastructure development in Africa.
- Encourages equitable access to emerging technologies to close the digital divide.

Valid Sources for Research

Artificial Intelligence & Copyright:

- World Intellectual Property Organization (WIPO): https://www.wipo.int
- MIT Technology Review: https://www.technologyreview.com
- The Verge: https://www.theverge.com

Digital Privacy & Inclusion:

- Electronic Frontier Foundation (EFF): https://www.eff.org
- Center for Democracy & Technology (CDT): https://cdt.org
- Data & Society Research Institute: https://datasociety.net

Misinformation Control:

- First Draft News: https://firstdraftnews.org
- FactCheck.org: https://www.factcheck.org
- Poynter Institute: https://www.poynter.org

Cybersecurity:

- Cybersecurity and Infrastructure Security Agency (CISA): https://www.cisa.gov
- European Union Agency for Cybersecurity (ENISA): https://www.enisa.europa.eu
- CyberPeace Institute: https://cyberpeaceinstitute.org

G20-Specific Research:

- G20 Official Website: https://www.g20.org
- OECD Digital Economy: https://www.oecd.org/digital/
- International Telecommunication Union (ITU): https://www.itu.int

---

Additional National Policies:

- U.S. National Institute of Standards and Technology (NIST): https://www.nist.gov
- UK AI Council: https://www.gov.uk/government/groups/ai-council
- China Cyberspace Administration: http://www.cac.gov.cn
- European Commission Digital Strategy: https://digital-strategy.ec.europa.eu
- French Ministry of Digital Affairs: https://www.numerique.gouv.fr
- India Ministry of Electronics and IT: https://www.meity.gov.in
- Brazil Internet Steering Committee: https://www.cgi.br
-

Expected Outcomes from the Delegates

- Agreement on AI labeling and intellectual property policies.
- Strengthened digital privacy regulations across G20 nations.
- Development of strategies to tackle misinformation while protecting free speech
- Collaborative initiatives for global cybersecurity cooperation.
- Consensus on ethical AI governance worldwide.

Conclusion

As technological advancements reshape societies, ethical considerations remain paramount. The G20's discussions on AI, digital privacy, misinformation, and cybersecurity reflect the need for balanced policies that encourage innovation while safeguarding rights and freedoms.

Understanding each country's stance and the broader international perspectives will help delegates contribute meaningfully to the debate. The thoughtful engagement will drive meaningful policy solutions for a more ethical digital future.
