A Pan-India Workshop

on

India-Australia Partnership Framework on AI, Quantum and Critical Technologies enabling Digital Economy

(Workshop to examine digital developments in relation to cross border data flows, cyber security, artificial intelligence (AI), quantum & critical technologies between India and Australia)

14 December 2023

Venue: Gujarat National Law University

Mode: Hybrid

Organised by:

Gujarat National Law University, India & Victoria University, Australia

Sponsored by: Government of Australia

ABOUT THE WORKSHOP

Gujarat National Law University

VICTORIA UNIVERSITY
MELBOURNE AUSTRALIA

Victoria University, Melbourne, Australia, and Gujarat National Law University, Gandhinagar, India have been contracted by the Australian Government to examine digital developments in relation to cross border data flows, cyber security, artificial intelligence (AI) and quantum technologies between India and Australia and to propose framework of bilateral cooperation between India and Australia.

The aim of this project i.e. India-Australia Partnership Framework on AI, Quantum and Critical Technologies enabling Digital Economy is to bring together officials from Central Government, State Government, academicians, practitioners, industry experts, corporate managerial professionals, and Indian regulators to discuss and deliberate upon the law, policy and standards for data, cybersecurity, AI, quantum and critical technologies. This project is cutting edge and is for India and Australia to work together to develop mutually agreed Principles for the future management and governance of artificial intelligence and quantum technology that will be used in trade and investment between the two countries.

ABOUT THE WORKSHOP

It is noteworthy that the legal landscape surrounding data flows and cybersecurity is intricate and rapidly evolving. Moreover, in the realms of AI and quantum technologies, there exists a notable absence of specific laws or standards. By scrutinizing these pivotal facets of the emerging digital economy through the lens of a robust legal and regulatory framework, the recommendations through these workshops aim to position both India and Australia at the forefront, offering a trajectory for swiftly enhancing investment and trade across the entire digital spectrum incorporating ethical principles supporting Quantum and Critical technologies. The conclusion of this collaborative effort will result in a comprehensive report which will encapsulate key recommendations and will be submitted to the Australian Government., Indian Government and Universities. Furthermore, the successful completion of this project will open avenues for future collaborations, presenting opportunities to deepen the partnership with Australia and augment our respective trade and investment relations.

The proposed workshop format is centered around a question-answer structure (pls see Questionnaire section), with participants expected to articulate their thoughts in response to the queries provided in the questions.

AGENDA PLAN OF THE WORKSHOP

Workshop on India-Australia Partnership Framework on AI, Quantum and Critical Technologies enabling Digital Economy

Date: 14 December 2023; Time: 1000 hrs to 1630 hrs IST

Venue: Gujarat National Law University, Gandhinagar, Gujarat

Sessions Details	
Inaugural Session 1000 hrs to 1100 hrs IST	Welcome Address by Prof Dr S Shanthakumar, Director, GNLU Inaugural Address and Keynote Address
TEA BREAK and PHOTO SESSION (1100 hrs to 1130 hrs IST)	
Plenary Session on AI, Quantum and Critical Technologies 1130 hrs to 1300 hrs IST	Presentation on Ethical Principles within Regulation for the use of Technology in International Trade and Investment by Dr Robert Walters, Principal and Chief Investigator Presentations by Mr Bill Cole, Chair of Professionals in International Trade and Prof Bruno Zeller, University of Western Australia + Plenary Speakers
LUNCH BREAK (1300 hrs to 1400 hrs IST)	
Round Table Session 1400 hrs to 1515hrs IST	Round Tables Sessions (break out groups) will be constituted. During the Round Table Session – the facilitator will discuss the questionnaire with the participants
TEA BREAK (1515 hrs to 1545 hrs IST)	
Closing Session 1545 hrs to 1630 hrs IST	Presentation on Preliminary findings & Next Steps

QUESTIONNAIRE FOR ROUND TABLE SESSION

1. How do you define critical technologies? What do they mean to your organisation?

2. Does your organisation use artificial intelligence (AI) or critical technologies? Will your organisation be investing in either or both of these technologies to or from other countries?

3. Has your organisation thought about Quantum technology? Do you have an awareness of the implication of Quantum technology to trade and investment?

4. Have you considered the impacts of AI being amalgamated with Quantum technology – and what this might mean for your organisation?

5. What are the Opportunities to your organisation from international data, cybersecurity, AI, Quantum and critical technology transfers? (e.g., expansion of trade-investment, government-health, education, ITC, maritime, primary industries, legal and other services)?

6. What are the Risks to your organisation from not understanding the current day and future risks from this technology on trade and investment?

7. Critical-Quantum technologies and AI are not regulated – what are 3 to 6 ethical issues that need to be considered in the governance of this technology to strengthen trade and investment (provide a higher level of transparency, accountability and certainty)? Another way to think about this is how do we shape the ethical concepts and principles so as Australia - India trade and investment is not only protected but has a level of governance.

QUESTIONNAIRE FOR ROUND TABLE SESSION

8. Are the following considered a starting point for Ethical concepts and principles (similar to those in the OECD Guidelines for Data, embedded into national law)? Will these be suitable for trade to trade – investment to investment between organisation-countries:

Rules based system

Rule of Law

Accountability

Transparency

Privacy

Responsibility

Reporting

9. Should there be two layers of ethical concepts and principles? What might this look like? (government regulation versus industry self-regulation)

10. Is there a need for sector-by-sector level of ethical principles and concepts in the same way as risk management frameworks? That said, a general risk management assessment can be applied to every sector.

11. Should they be embedded as a minimum standard in government regulation? Or should they exist only in industry (sector) self-regulation?

12. Is there a place for ethics in technology and AI to be enforced by both government and/or private sector e.g. ISO Audits?

13. What are the main influences and drivers that make enforcement successful or otherwise?

QUESTIONNAIRE FOR ROUND TABLE SESSION

14. An enforcement mechanism could be mandatory reporting to the Regulator, similar to tax – is this a viable option, until the regulations and governance of critical technologies and AI is [relatively] settled?

15. In many countries the data laws require a point of contact within an organisation, such as, controller-processor. Should there be similar for cybersecurity-or the controller role expanded? Does this need to be in the law? (this is predicated on where there is a breach-incident from the use of AI-Quantum technology for example, commercial/personal data loss, economic loss-personal injury) certainty)? Another way to think about this is how do we shape the ethical concepts and principles so as Australia - India trade and investment is not only protected but has a level of governance.

16. Whether The Digital Personal Data Protection (DPDP) Act, 2023 of India addresses the challenges for the adoption of new technologies? If so, please explain.

17. Do you think any amendments would be required in the DPDP Act, 2023 for addressing such issues related to AI, quantum and critical technologies? If so, please suggest.

18. Do you think the DPDP Act, 2023 would be a supportive law for the Digital economy? If so, please explain.

BACKGROUND READING

VICTORIA UNIVERSITY
MELBOURNE AUSTRALIA

Gujarat National Law University

Background Reading - Ethics

The structure of an ethical theory is largely determined by how it is defined and connected to these two basic notions.[1] Ethics "is often formulated in formal codes or standards to which all members of a profession are held, such as those of medical or legal ethics. "[2] Simply put ethics assists everybody to choose the best decision within their work life in any situation including cooperation, productivity, and respect to others. Concepts and principles that have emerged include:

- AI for common and public good
- Placing humans first and well being
- Transparency
- Safety and Security
- Responsibility and Liability
- Accountability and Oversight
- Privacy
- Fairness, bias, and discrimination.[3]

On the other hand for an ethical hacker they will generally consider the implement the following practical steps:

- get *written permission* prior to stressing and assessing his or her client's IT-security.
- act *honestly* and stay within the scope of his or her *client's expectations*.
- *respect* his or her client's as well as its employees' *privacy*.
- use *scientific*, state-of-the-art and *documented processes*.
- *transparently communicate* to his or her client all the *findings* as well as a transcript of all his or her *actions*.
- remove his or her traces and will *not introduce* or keep any *backdoor* in the system.
- *inform* software and hardware vendors about *found vulnerabilities* in their products.[4]

The EU[5] proposes the following:

Autonomy Beneficence Dignity Equality Fairness Freedom Justice Privacy Responsibility	Human dignity Freedom Democracy Equality Non-discrimination The rule of law Respect for human rights Pluralism Tolerance Justice Solidarity Protection of EU citizens	Privacy Security Trust Suggested data protection goals: Availability Confidentiality Integrity Intervenability Transparency Unlinkability	Privacy Fairness Autonomy Practical goals of cyberse- curity technology: Availability Confidentiality Integrity

Cyberethics has also emerged to include:

- Philosophy;[6]

---

[1] John Rawls. A theory Of Justice, Harvard University, Press, 1999, 21. In Robert Walters Data, Cyber Laws of the Commonwealth, International Trade, Investment and Arbitration, forthcoming book.
[2] Shannon Vallor, An Introduction to Cybersecurity Ethics, 2. Santa Clara University. https://www.scu.edu/media/ethics-center/technology-ethics/IntroToCybersecurityEthics.pdf
[3] Elonnai Hickok, *Ethics and AI in India,* 2018, https://cis-india.org/internet-governance/files/ethics-and-ai
[4] Ibid, p 193.
[5] Markus Christen, Bert Gordijn, Nadine Kleine, Gwenyth Morgan, Karsten Weber, *Cybersecurity and Ethics*,White Paper 1, 2020, European Commission Erasmus Funding Grant.
[6] Ishaani Priyadarshini, Chase Cotton, *Cybersecurity Ethics, Legal, Risks, and Policies*, CRC Press Taylor Francis (2022), pp 14-15, It explores the philosophical aspect behind ethics that includes life between birth and death. Gaining unauthorized access to

BACKGROUND READING

- Societal Norms;[7]
- Environmental Ethics;[8]
- Political Ethics;[9]
- Economic Ethics;[10] and
- Religious Ethics.[11]

Further concepts that have also been developed and include:

- *Confidentiality:* It refers to protecting the information from disclosure to unauthorised parties. It is associated with the protection of details which should be visible or accessible to people who have appropriate privileges.
- *Integrity:* It is responsible for ensuring trustworthiness, accuracy, an completeness of the sensitive information. The main objective of integrity is to protect information from being altered by unauthorised or unintended parties and individuals.
- *Availability:* It is responsible for ensuring that only authorized parties can access the information when at the time of need.
- *Authentication:* It refers to the process of ensuring and confirming the identity of a user.
- *Non-Repudiation:* It can be used to ensure that a party involved in a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.[12]

These are being adopted on a sectorial approach. We are wanting to scale these up, to establish standardisation.

someone's account or compromising the privacy of an account are situations that are unethical and Ethics as Philosophy could avert such situations.

[7] Ibid, It deals with Community Ethics. These underpin questions of bad and good of social media, how it has an impact on the community life and chances of global communication. It also takes into account abuse in terms of cyber bullying, mobbing, etc. It manifests the core values and virtues that usually have their source in the family.

[8] Ibid, Itdeals with the impact of cyber technology on human-nature relations. It also highlights the environmental negative impact of energy use as well as the positive impact of environmental advantages of weather forecast, scientific research, etc. It deals with questions like whether it is ethical to jeopardize natural resources in order to carry out research.

[9] Ibid, It is concerned with changes in political systems. These may be in the form of elections, security, armies with autonomous weapons, need, and limits of regulation of cyberspace on international and national levels, etc. Elections have been known to get manipulated over cyberspace; Ethics from the political perspective may be one of the ways to avoid it.

[10] Ibid, It explores the positive and negative impacts of cyberspace. The factors taken into account are economic growth, job creation or job losses, financial investments in cybersecurity research, etc. The financial sector is frequently hit by data breaches and monetary losses. Economic Ethics could be followed while dealing with such situations.

[11] Ibid, It looks at the ethical and unethical impact of cyberspace on culture, music, art, dance, language diversity, cultural inclusion or discrimination, religious respect or hate messages through the internet, etc. Social media provides platforms for religious and cultural disputes. Keeping in mind Religious Ethics may be a way of avoiding it.

[12] Ishaani Priyadarshini, Chase Cotton, *Cybersecurity Ethics, Legal, Risks, and Policies*, CRC Press Taylor Francis (2022), p 5.

INFORMATION ON OTHER SERIES OF WORKSHOPS

Place	Date	Partner Law School	Mode
Workshop at New Delhi	22 November 2023	National Law University Delhi	Online
Workshop at Kolkata	28 November 2023	West Bengal National University of Juridical Sciences, Kolkata	Online
Workshop at Mumbai	2 December 2023	Maharashtra National Law University Mumbai	In-person
Workshop at Bengaluru	04 December 2023	RV University, Bangalore	Online
Workshop at Sonipat	09 December 2023	O. P. Jindal Global Law School, Sonipat, Haryana	Online

Our Institutional partners

ORGANISING TEAM AND CONTACT

Victoria University (VU):

Project Principal and Chief Investigator

Dr. Robert Walters,
Senior Lecturer and Head Digital Economy Research Group,
Arbitrator - Solicitor

Gujarat National Law University (GNLU)

Prof. Dr. S Shanthakumar, Director, Gujarat National Law University

Project Investigators: India Team

Prof. Dr. Mamata Biswal, Professor of Law, GNLU
Prof. Dr. Ranita Nagar, Professor of Economics, GNLU
Ms. Harsha Rajwanshi, Assistant Professor of Law, GNLU
Mr. Soaham Bajpai, Assistant Professor of Law, GNLU

Assistants:

Mr. Ayush Rastogi, Teaching and Research Associate (Law), Ms. Vinati Tahilianey, Teaching and Research Associate (Law), Ms. Sakshi Saini, Teaching and Research Associate (Economics), and Ms. Niharika Raizada, Ph.D. Scholar

For any query or information, pls contact us at indausproject@gnlu.ac.in or to Ms Harsha Rajwanshi, +91 9410422436 or Mr Soaham Bajpai, +91 8128650845