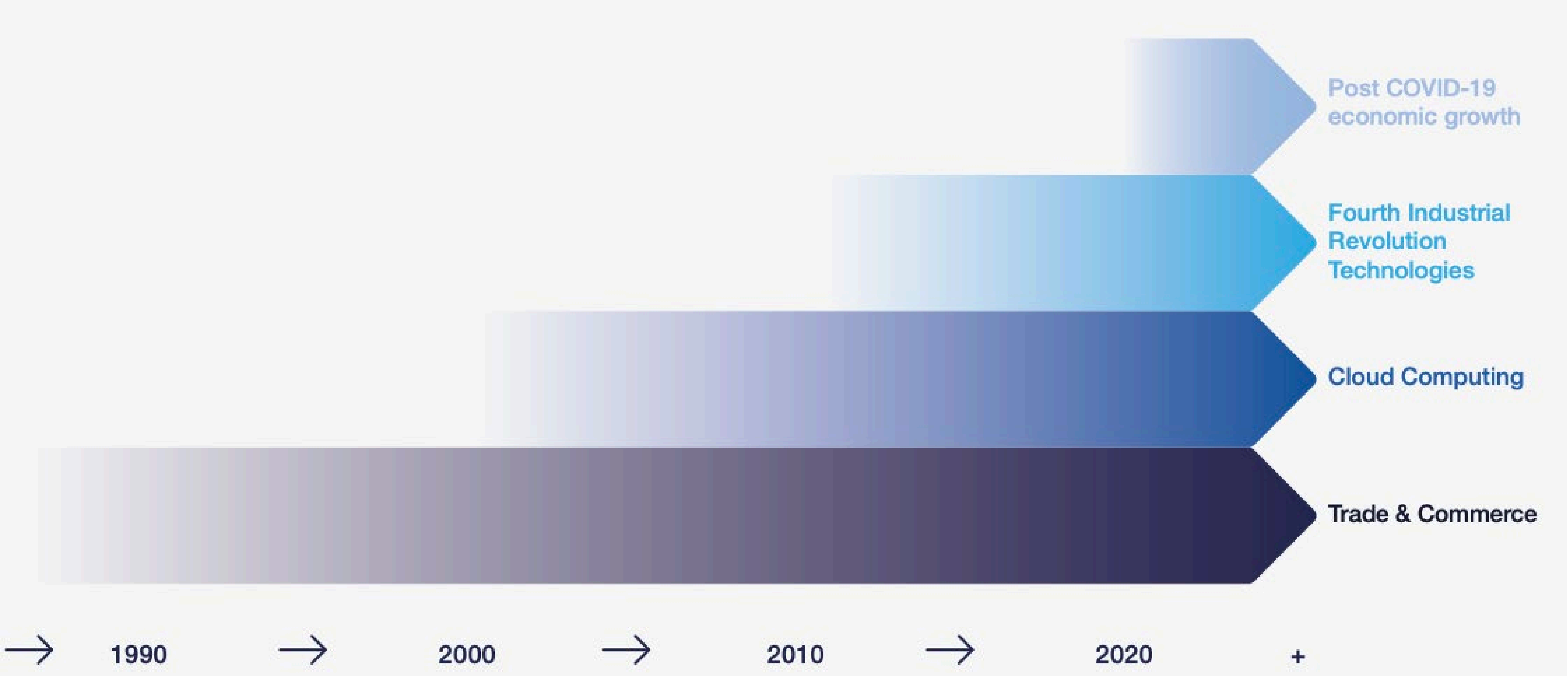
UNECE
Advancements in AI towards facilitating cross border paperless trade

AI Ethics in Cross Border Commerce

Sray Agarwal

UNECE
UN/CEFACT

Increasing Importance of International Trade



Post COVID-19 economic growth

Fourth Industrial Revolution Technologies

Cloud Computing

Trade & Commerce

Types of Data Breaches

- where a breach impacts the processing of establishments in several countries (for example, a ransomware attack on a pan-European group of companies)

- where a breach affects individuals in multiple countries (for example, an online payments company’s servers being hacked, leading to financial data of residents of several EU countries being affected)

It Happened All Across..

- Following an extensive investigation British Airways was fined with £183.39M for infringements of GDPR as user traffic was being diverted to a fraudulent site and personal data of approximately 500,000 customers were compromised

- Experian, a consumer credit reporting company, on 19 August experienced a breach of data which has exposed personal information for 24 million South Africans, and 793,749 business entities

- Data regulators in the UK and Australia have announced a joint investigation into the practices of controversial facial-recognition start-up Clearview AI

Policies For Data Privacy

- Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), formerly the **Trans-Pacific Partnership** (TPP)
    - Includes explicit and binding language to govern the cross border data flows that fuel AI
- Egypt **Personal Data Protection Law** (Oct’20)
    - Cross-border transfer or sharing of personal data is prohibited, unless the country guarantees a level of protection for personal data that does not fall below the requirements stipulated under this Law, and subject to obtaining a relevant licence from the Authority. Additional guidance on this front is expected in due course.
- China’s **Global Initiative on Data Security**
- **Asia-Pacific Economic Cooperation Cross-Border** Privacy Rules
    - Facilitates data flows while promoting privacy protection by requiring that countries who accede to the system comply with the APEC Privacy Framework
- **EU-US Privacy Shield**
    - Provides companies with low-cost means of moving data between the U.S. and the EU provided that companies who self-certify commit to complying with the Privacy Shield’s consumer notice, data protection, and data retention requirements
- **US Mexico Canada Agreement**
    - Contains a digital trade chapter that includes provisions banning data localization, encouraging the free flow of data, and promoting data privacy

How To Safeguard Your Cross-border Data Analytics

- **Data Sovereignty**
  - Future proof assumption: data should remain resident where it was created when establishing data pipelines and architecture
- **Cloud Migration and Multi-Cloud**
  - Future proof assumption: my cloud provider must have a local data center in my countries of operation, and a multi-cloud approach may be required
- **Privacy-by-design (PBD) and privacy-enhancing technologies (PETs)**
  - Future proof assumption: data ops and analytics should include best practices to mathematically limit privacy risk

Transboundary Effects of Artificial Intelligence

Developers, vendors, customers and users of an algorithmic system can be spread around the world. In addition, programming code, training datasets and predictive outcomes are increasingly held in geographically dispersed locations. The following patterns in transnational algorithmic flows have emerged:

1. Data or datasets are transferred to the machine learning system
2. A machine learning algorithm can also be transferred to where the data resides
3. The predictive outcomes of a machine learning system can be applied at a distance

Prelude to Federate Learning

- One method is *differential privacy*, where a randomized mechanism is considered differentially private if the change of one input element leads to only a small difference in the output distribution. This means that one is unable to draw any conclusions about whether or not a specific sample is used in the learning process

- Another method for securing the learning process is *homomorphic encryption* where computing is done on encrypted data

- *Secure multiparty computation* (SMC) that enables multiple parties to collaboratively compute an agreed-upon function without leaking input information from any party except for what can be inferred from the output

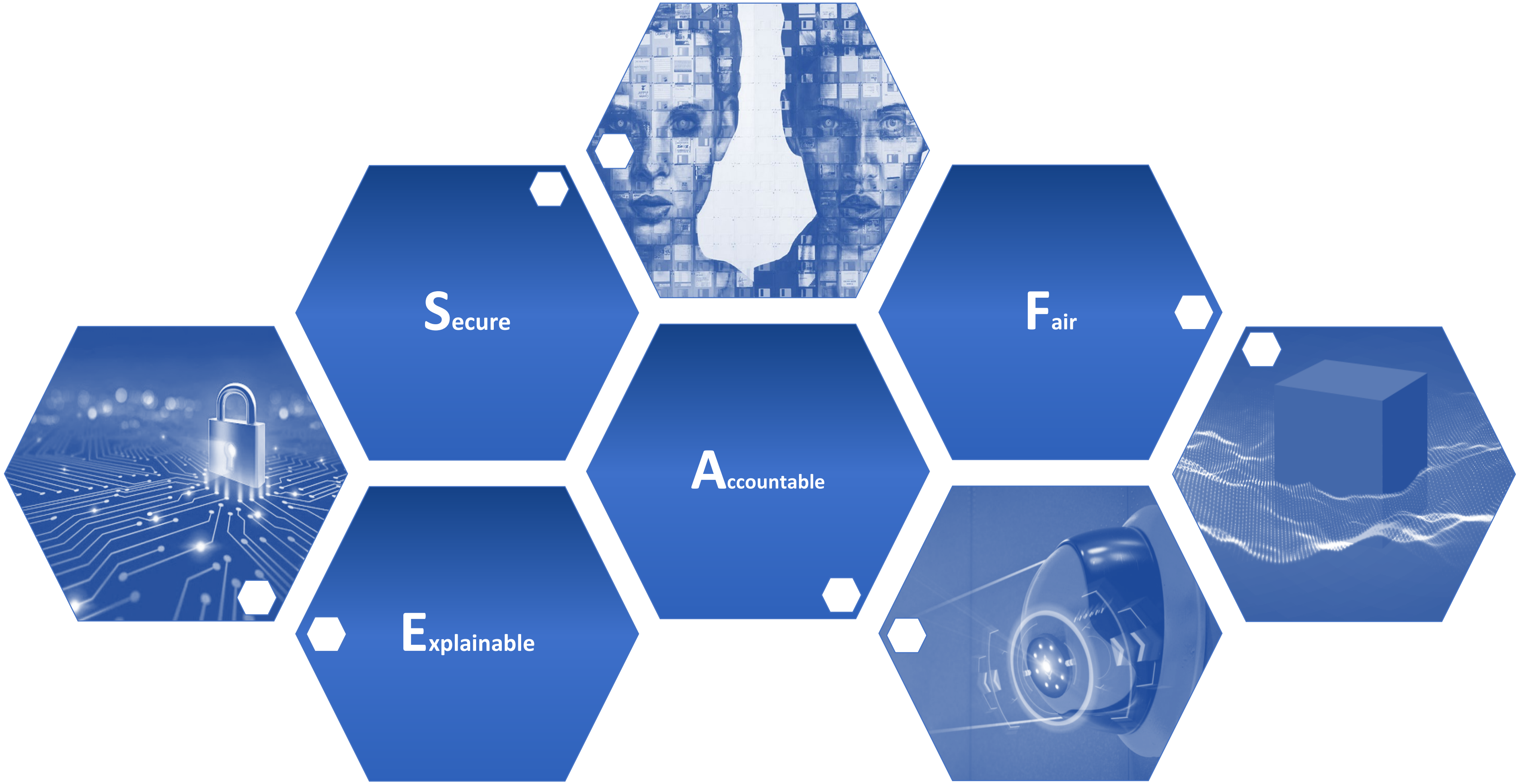
Federate Learning

Federated learning, originated by Google in 2017, makes it possible to build collaborative machine learning models without direct access to training data. This preserves privacy, and creates lighter workloads without requiring that the data be moved from its original location

The singular intent of FL is to cooperatively learn a global model without directly sacrificing data privacy. In particular, FL has distinct privacy advantages compared to data center training on a data set. Even holding an “anonymized” data set at a server can still put client privacy at risk via linkage to other data sets

With FL, privacy can be classified in two ways: *global privacy* and *local privacy*. Global privacy necessitates that the model updates generated at each round are private to all untrusted third parties other than the central server. At the same time local privacy further requires that the updates are also private to the server

SAFE AI : A Complete Solution



Secure

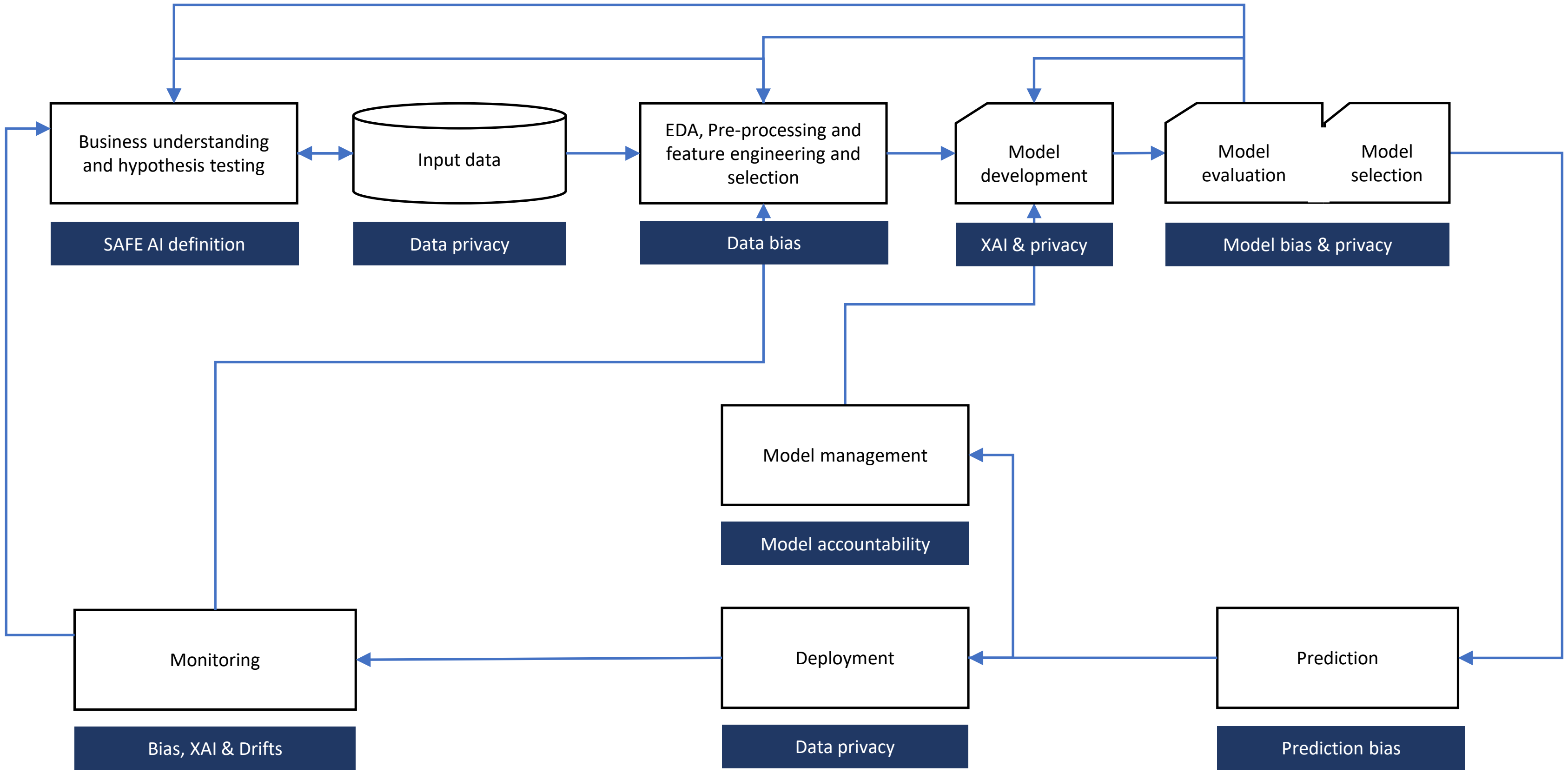
Fair

Accountable

Explainable

UNECE
UN/CEFACT

Data Science Lifecycle with SAFE AI



UNECE
UN/CEFACT

A Roadmap for Cross-Border Data Flows

① **Allow data to flow by default**

Prohibit data localization requirements except in very specific circumstances in order to create regulatory certainty for businesses.

② **Establish a level of data protection**

Establish national legal frameworks that protect the data of private individuals. Complement this with laws that protect proprietary rights.

③ **Prioritize cybersecurity**

Enact transparent cybersecurity legislation in line with international norms and maintain robust data security infrastructure.

④ **Hardwire accountability between nations**

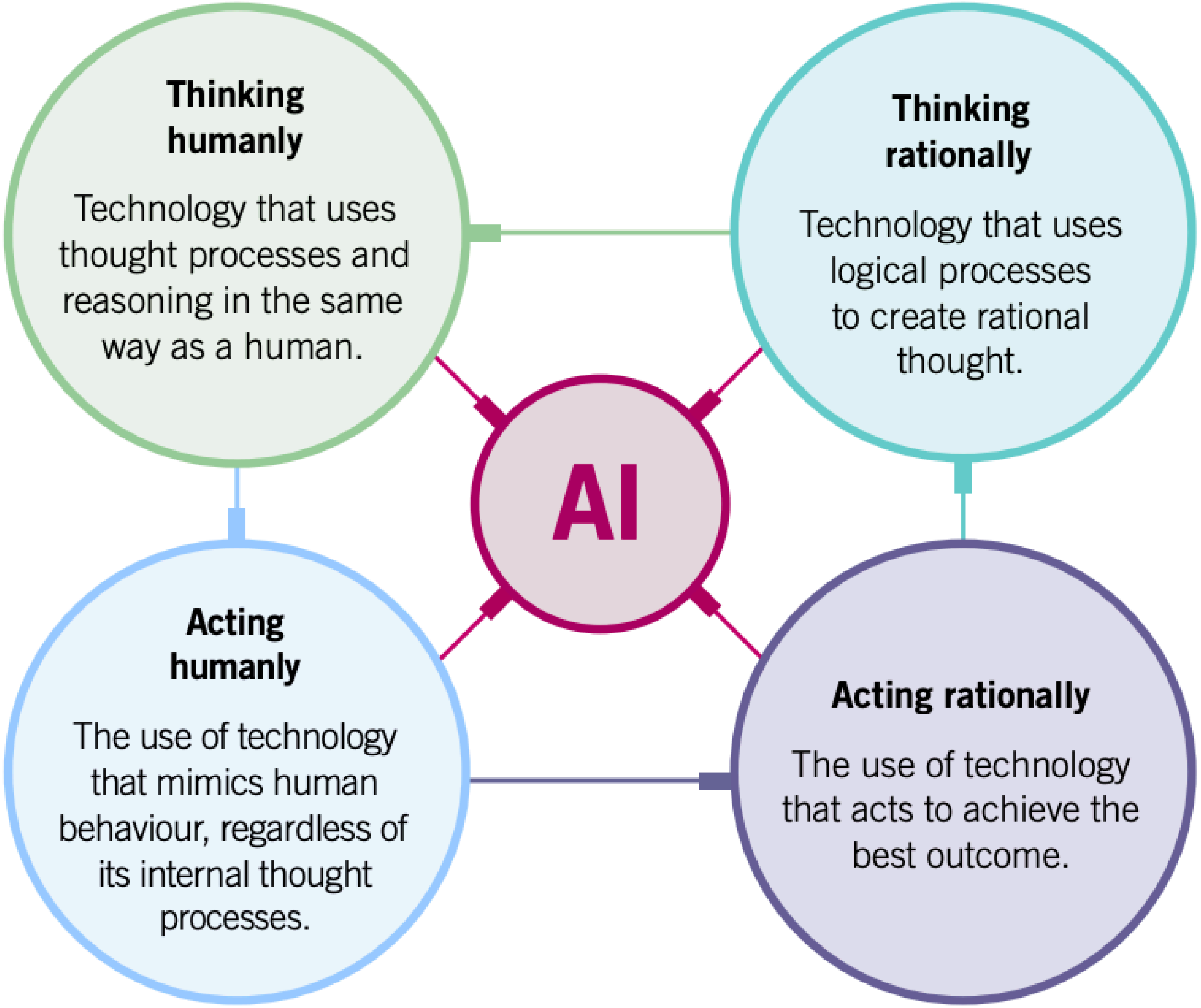
Establish cooperation mechanisms between national authorities to hold governments accountable for the security and confidentiality of the data they share, while making allowances for compliance.

⑤ **Prioritize connectivity, technical interoperability, data portability and data provenance**

Prioritize the development of connectivity infrastructure as a prerequisite to building a local data economy, encourage technical standards to increase interoperability, facilitate data portability at the B2B level to support SMEs, and encourage data publishers to ensure data integrity.

⑥ **Future-proof the policy environment**

Allow for the possibility of future alternative models (such as federated learning models and data trusts) that can also fulfil the spirit of cross-border data flows.



Thinking humanly

Technology that uses thought processes and reasoning in the same way as a human.

Thinking rationally

Technology that uses logical processes to create rational thought.

AI

Acting humanly

The use of technology that mimics human behaviour, regardless of its internal thought processes.

Acting rationally

The use of technology that acts to achieve the best outcome.

Conclusion

- No nation alone can regulate artificial intelligence (AI) because it is built on crossborder data flows.
- Countries are just beginning to figure out how best to use and to protect various types of data that are used in AI, whether proprietary, personal, public or metadata.
- Countries could alter comparative advantage in data through various approaches to regulating data — for example, requiring companies to pay for personal data.
- Countries should carefully monitor and integrate its domestic regulatory and trade strategies related to data utilized in AI.

https://www.linkedin.com/in/srayagarwal/

https://twitter.com/srayagarwal

Thank you,