Legal Asia 2022: Re-Disrupting the New Norm

Kuala Lumpur, 21-23 June 2022

Cyber Law: The Pursuit of Digital Sovereignty and its Legal Implications

Anurag Bana
Senior Legal Advisor
Legal Policy & Research Unit
International Bar Association
(United Kingdom)

Table of Content

Concept of Digital Sovereignty

- Digital sovereignty refers to the right of a sovereign state to regulate the use of technology within its jurisdiction.
- It is essentially the idea that states across the world should take charge of their digital destiny by determining how data of users within their jurisdiction is used and regulated.
- States determine how personal and non-personal data of users is stored and used.
- It is the realisation of the economic & political benefits embedded in the exercise of sovereignty over data.
- Data localisation is widely used by states to assert data sovereignty.

EU's Approach to Digital Sovereignty

- EU proposed 'Data Act' to address the issue of digital sovereignty within the EU (published on 23 February 2022; yet to come into effect).
- Ensures fairness in how the value of data is allocated in data value chain.
- Requirements on design and use of IoT products & services.
- Applies extra-territorially to manufacturers, data holders, data processing services of EU data outside the EU.
- Grants EU public bodies the right to request data from data holders when urgent need.
- Grants users the power to require data holders to share their data with 3rd parties of 'their choice'.
- Limits the access of non-EU governments to EU non-personal data held by providers of cloud and edge services.

Challenges of Digital Sovereignty

- In some countries international data transfer is permissible where recipient countries ensure an adequate level of data protection.
- In EU, GDPR states that data transfer can take place with certain conditions:
    - Where the recipient is in a territory deemed by the EU Commission to offer an adequate level of protection for personal data;
    - Where safeguards are in place such as binding corporate rules approved by Data Protection Authorities;
    - Where a legal exemption applies (i.e., where data subjects provide explicit consent, where the data transfer is necessary to fulfil a contract or there is a public interest founded in EU or member state law).
- In India, the proposed Personal Data Protection Bill 2019 suggests that sensitive personal data must be stored in India. But a copy of the data may be internationally transferred:
    - Where the data principal provides explicit consent;
    - Where the Indian govt. deems the recipient country as capable of providing adequate protection;
    - Where the Data Protection Authority has specifically authorised the transfer.

Challenges of Digital Sovereignty

- Cross Border Data Transfers: E.g.
  - UK-India Cross Border Data Transfers for UK-India Free Trade Agreement;
  - UK-Australia Free Trade Agreement;
  - UK-Japan Comprehensive Economic Partnership Agreement;
  - Digital Economy Agreement with Singapore;
  - Comprehensive & Progressive Agreement for Trans-Pacific Partnership (CPTPP) access negotiations;
  - US-EU Trans-Atlantic Data Privacy Framework (proposed)
- In certain jurisdictions (including Africa) there is an absence of law on digital sovereignty.
- The African Union has now committed to cybersecurity as a priority for its 2063 Agenda.
- Data localisation measures impact:
  - Free flow of information that assist the global supply chain.
  - Email communications and social media services which global manufacturing and service industries depend on.
  - Compliance with cybersecurity obligations by BigTech gets challenging.

Challenges of Digital Sovereignty

- WannaCry 2017 Ransomware (due to EternalBlue exploit developed by NSA and leaked by Shadow Brokers) attack infected more than 200,000 computers in 150 different countries in 4 days - an important example to show that NOBUS ('nobody but us') cyberattack capabilities of governments can no longer be monopolised.
- NotPetya malware cyberattack interrupted global operations and resulted in huge worldwide financial losses for various companies like FedEx at US$400 million; AP Moller-Maersk at US$200-$300 million; Merck estimated impact of US$670 million because of direct costs & lost revenue.
- Other recent cyber incidents - Crypto.com (2 FA compromise $18 million BTC & $15 million ETH); Red Cross (malware attack - data of 515,000 individuals compromised).

Cyberspace Best Practice & Regulation

- National laws regulating the cyberspace are heterogenous and the heterogeneity do not make for certainty particularly for large tech companies that operate beyond national borders.
- Unwillingness of countries with control over vast data to relinquish position for a democratised data sharing arrangement.
- International legal industry stakeholders like the International Bar Association (IBA) are working towards the harmonisation on cybersecurity through their Cybersecurity Guidelines for the global legal profession.
- The IBA cybersecurity guidance provides advisory assistance for legal professionals in preparing and in keeping cross-border operations running if a breach does occur in order to protect the data of the clients. Link: https://www.ibanet.org/LPRU/Cybersecurity

Cyberspace Best Practice & Regulation

- The IBA Presidential Taskforce on Cybersecurity and the IBA Legal Policy & Research Unit are currently benchmarking global perspectives to develop guidance on best practices for protecting institutions and companies from cyber risks with a view to harmonising global efforts. (Global Best Practice Document in November 2022)
- The IBA Working Group on Digital Identity published Digital identity: principles on collection and use of information – a set of high-level principles around the collection, use and sharing of digital identity information that could serve as a basis for engaging in dialogue with stakeholders. Link: https://www.ibanet.org/LPD/Digital_Identity

  - *Rights over data*
  - *Protection of data*
  - *Enforcement mechanisms*
  - *Effective remedies*

Overarching Aim: - To provide for transparency, responsibility and security.
- Users should have control over their identifiable information.

Cyberspace Best Practice & Regulation

- United Nations Centre for Trade Facilitation and Electronic Business (UNCEFACT) develops technological standards and framework agreements for facilitation of international trade. E.g. Working on data standards for IoT based communications, link: https://unece.org/trade/uncefact
- United Nations Economic Commission for Europe (UNECE) Electronic Commerce Agreement, link: https://unece.org/fileadmin/DAM/cefact/recommendations/rec31/rec31_ecetrd257e.pdf
- United Nations Commission on International Trade Law (UNCITRAL) Working Group IV: Electronic Commerce – currently working on the Draft Model Law on the Use and Cross-Border Recognition of Identity Management and Trust Services, link: https://uncitral.un.org/en/working_groups/4/electronic_commerce

Data Strategies

- Emerging technologies are enabling next level of data management capabilities for businesses and In-house departments.
- Data strategies:
  - Defensive data - to minimise downside risk (compliance with regulations, data privacy, integrity of financial reports);
  - Offensive data - customer focused business functions (sales, marketing, real-time analytics), industry where strong competition for customers.
- Restructuring of technology + Inclusion of ML/AI.
- Developing business specific data architectures – SSOT, MVOT for information management.

Moving Forward

- Need for international cooperation (multilateral framework) on digital sovereignty, data protection, and cybersecurity.
- Addressing conflicting legislations will help minimise cybersecurity risks and encourage global collaboration in the cyberspace.
- Global cybersecurity outlook - need for a collective action for a more secure and resilient digital ecosystem (World Economic Forum Global Security Outlook 2022).
- Need to mobilise a global multistakeholder response to strengthen cyber resilience in systemically important critical infrastructure.
- An international guidance can be developed to help states enact laws that converge on vital areas of digital sovereignty, data protection, and cybersecurity.
- This approach gives states the freedom to enact their own legislations suited for their legal landscape and compatible with international requirements.

Moving Forward

- Strategic outlook on the digital economy – build socially inclusive and environmentally sustainable economic growth.
- Building responsible data ecosystems – businesses need to become more responsible about their data-sharing practices; CEOs incorporate public values into data-driven innovative decisions.
- Advancing digital cooperation – In 2023, the United Nations aims to agree a Global Digital Compact, which is a multistakeholder understanding between states, private sector and civil society on how to achieve the roadmap for global digital cooperation.

Thank You!

Contact:

Anurag Bana

anurag.bana@int-bar.org

anurag.bana@law-oxford.com

linkedin.com/in/anurag-bana-79780542

@AnuragBana

+44-(0)-757 527 0058

Anurag Bana

Senior Legal Advisor, International Bar Association