CYBER LAW CHALLENGES IN THE POST-PANDEMIC ERA: DATA PROTECTION AND PRIVACY

Lecture at the School of Strategic and Global Studies (SKSG), Universitas Indonesia, 22 October 2021

ASSOC. PROF. DR. SONNY ZULHUDA
International Islamic University Malaysia

sonny@iium.edu.my
sonnyzulhuda.com
twitter.com/zulhuda
Agenda

01 The Pandemic Check
02 New Cyberspace Intensity
03 The Global New Norms
04 Key Issues and Challenges
05 Lessons Learned
THE PANDEMIC
REALITY CHECK
Covid-19 Statistics as of 20 Oct 2021

- 241 million Confirmed cases
- 4.91 million Confirmed deaths
- 220 Countries, areas or territories with cases
POLICY MEASURES: Governments impose movement restriction, isolation, lockdown, surveillance, curfew, quarantine and border control.

HEALTH CONCERNS: intensified reporting, patients tagging, scheduled control, body temp scanning, contact tracing, high-risk people identification.


BRING ABOUT: Social, Psychological, Technical, Public Trusts, Business and Governance VULNERABILITIES.
Pandemic-created Vulnerabilities

People tend to rush collecting information about the Pandemic, click on links and web pages, spreading the information with poor exercise of fact-checking.

People work on official documents using home-based computers, with inadequate security protection and support as they have in office.

Reduced mobility, losing jobs, scarcity of earning opportunities, etc. creates financially challenged society, who would turn into shortcuts (crimes, etc).

Wide and fast adoption of mobile Apps for social networking, e-shopping, e-meeting, e-learning and cloud services, but with poor security and privacy measures or policies.
PANDEMIC
COVID-19

Pandemic-created Vulnerabilities

Tips to stay safe online

- Update all systems including Virtual Private Networks (VPN) and devices with the latest security patches
- Alert employees about phishing attempts
- Avoid logging in to your work environment using public Internet Wi-Fi
- Connect through your home or mobile network data
- Enable Multi-Factor Authentication

Tips to stay safe online

- Use legitimate, government websites for up-to-date, fact-based information
- Use the latest version of apps and security software
- Only download software from its official website or app store
- Never share confidential information during a meeting
- Enable non-recordable videos and audio, and limit file sharing
- If something is suspicious, log out
- If you lose your computer or mobile phone, log out from all clients immediately and change your login password
- Do not share or publish the confer
- Log out from the app after a meeting

Beware of cyberattacks!

Total number of incidents

- Cybersecurity cases increased by 82.5% during the MCO 2020 (March 18 to April 7) compared to the same period in 2019.

- 2018:
  - 417
- 2019:
  - 459
- 2020 (during the current MCO):
  - 838

Covid-19 scams

- Always verify information from emails, text messages and social media posts about Covid-19.
- Do not share personal or financial information in emails.
- Do not click on suspicious links provided to you on Covid-19.
- Verify with the sender or agencies that can help.

- 2018:
  - 417
- 2019:
  - 459
- 2020 (during the current MCO):
  - 838

sonnyzulhuda.com
Pandemic-created Vulnerabilities

1st

The United States declares its first case of COVID-19, cyber attacks go up 48%

Multiple states in the US declare a public emergency; cyber attacks go up 64%

The country of Italy goes into lockdown, attacks go up 28%

The World Health Organization declares COVID-19 a pandemic, cyber attacks go up 22%

30th January   29th February   8th March   11th March

Data source: Computer Weekly via Carbon Black
What had happened in the Cyberspace during Covid-19 Crisis?

- Intrusion to Critical Utilities
- Coronavirus research hack?
- Ransomware on public health system
- Ransomware on energy company
- Sabotage on Govt online meeting

Terrorists and cybercriminals are always interested to exploit cyberspace vulnerabilities. The activity of cyber terrorism does not relax during Covid-19. Several cyber attacks do target a critical information infrastructure (CII), a traditional target for cyber terrorism.
Investment due to COVID-19 crisis (Malaysia)

- Digital transformation: 4%, 35%, 54%
- Initiatives to realize cost efficiencies: 19%, 27%, 58%
- Cybersecurity and data privacy: 17%, 44%, 38%
- Leadership and talent development: 44%, 44%, 21%
- Organic growth programmes: 35%, 38%, 27%
- Sustainability and ESG initiatives: 4%, 33%, 29%
- R&D and new product innovation: 23%, 48%, 26%
- Capital investments: 39%, 50%, 19%
- Supply chain restructuring: 31%, 50%, 15%

Top potential threats to organizations in Malaysia

- Pandemics and other health crises: 85%
- Policy uncertainty: 75%
- Uncertain economic growth: 58%
- Cyber threats: 58%
- Social instability: 56%
- Over-regulation: 52%
- Misinformation: 52%
- Geopolitical uncertainty: 50%
- Changing consumer behaviour: 50%
- Availability of key skills: 48%
- Supply chain disruption: 46%
- Readiness to respond to a crisis: 44%
- Unemployment: 44%
- Declining health and well-being of your workforce: 44%
- Exchange rate volatility: 42%
- Trade conflicts: 40%
- Speed of technological change: 38%
- Increasing tax obligation: 35%
- Access to affordable capital: 35%
- Climate change and environmental damage: 35%
- Terrorism: 33%

Top threats considered in strategic risk management

- Pandemics and other health crises: 81%
- Uncertain economic growth: 67%
- Cyber threats: 65%
- Changing consumer behaviour: 65%
- Speed of technological change: 63%
- Availability of key skills: 63%
- Policy uncertainty: 60%
- Supply chain disruption: 50%
- Exchange rate volatility: 48%
- Geopolitical uncertainty: 44%

24th Annual Global CEO Survey 2021 – Malaysia (PWC)
How much specific issues raised companies’ long-term investment after Covid-19 crisis?
Emerging Privacy Risks post-Pandemic

Personal data exploitation through **illicit collections** via online services (eg P2P lending), Apps, etc;

**Scam via fake accounts** begging for donation, fake charity drives, fake emergencies etc.

**Misinformation**: citizen journalism with unaccountable stories – a test-bed for phishing attacks.

**Unsecured online platforms** prone to personal data breaches (online shopping, online meeting, social media, etc).

The rise of **surveillance** and Private data collection?
Data Breach Incidents – in the past two years*

PRIVACY RULES
THE GLOBAL NEW NORMS
Data Privacy as Epicenter of Global Disputes

- NSA SURVEILLANCE OVER THE US AND GLOBAL INTERNET USERS (SNOWDEN SAGA) - 2013
- FACEBOOK UNDER GLOBAL PRESSURE AFTER DATA MISUSE BY CAMBRIDGE ANALYTICA - 2017
- EU COURT ANNULLED EU-US AGREEMENT ON DATA TRANSFER - 2020
- PRES TRUMP BANNED CHINA-OWNED WECHAT AND TIKTOK IN THE US OVER PRIVACY CONCERNS - 2020
Who is interested to your Data?
1. BIG Brother
2. BIG Data Aggregator
3. BIG Fans!

sonnyzulhuda.com
The EU Court of Justice decided that the EU-USA Privacy Shield Agreement, which allows 3000 US companies to repatriate European personal data to US, is null and void, putting trans-Atlantic trade in a halt.
The US Government banned Chinese platforms TikTok and Wechat from operating in the US due to data security and data privacy concern.
APEC Privacy Framework (2015)

- Preventing Harm
- Notice
- Collection Limitations
- Uses of Personal Information
- Choice
- Integrity of Information
- Security Safeguards
- Access and Correction
- Accountability
European Union (EU) General Data Protection Regulation 2016

Fines of up to 4% of turnover
Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million.

Breach notification within 72 hrs
Breaches must be reported within 72 hours of first having become aware of the breach.

Increased territorial scope
Applies to any company processing personal data of EU citizens, regardless of location.

Privacy by design
Data protection from the onset of the designing of systems, rather than a retrospective addition.

Consent matters
Explicit consent must be provided in an intelligible and easily accessible form.

Right to be forgotten
Entitles the data subject to have the data controller erase his/her personal data (and potentially third parties, too).

Right to access and portability
Users can inquire whether and how their personal data is being processed.

Mandatory data protection officers
Appointed in certain cases, to facilitate the company’s need to demonstrate GDPR compliance.
G-20: Osaka Track on Data Free Flow with Trust (DFFT) - 2019
Privacy & Data Protection Rules on the Global and Regional Timeline

1948
- UN UDHR

1953
- ECHR

1976
- ICCPR

1980
- OECD Guidelines

1981
- CoE Conv. 108

1995
- EU Directive

2000
- CFREU

2007
- Lisbon Treaty

2007
- OECD Guidelines

2015
- APEC Privacy Framework

2016
- EU GDPR

2016
- ASEAN Framework on PDP

2020
- RCEP Agreement

sonnyzulhuda.com
A Quick Check on Other Jurisdictions

Most Recent Legislative Developments in key markets*

- **Canada** – Digital Privacy Act (November 2018), reforming the Personal Information and Protection and Electronic Documents Act (PIPEDA)
- **California** – Consumer Privacy Act (January 2020)
- **US** – Competing data privacy bills issued in Congress
- **Ecuador** – Data Protection Bill (still in drafting stage)
- **Chile** – Proposal Data Protection Law (still in drafting stage)
- **Brazil** – General Data Protection Law (LGPD - Law 13.709) (entering into force in August 2020)
- **Uruguay** – Law on the Protection of Personal Data and Habeas Data (Law 18.331/2008) amendments (January 2019) and Decree (No. 64/2020)
- **Argentina** – Proposal Data Protection Bill (MEH-2016-147-APN-PTE) (still in drafting stage)
- **South Africa** – Protection of Personal Information Act (POPIA) (entry into force to be determined)
- **Kenya** – Data Protection Act (November 2019)
- **Uganda** – Data Protection and Privacy Act (May 2019)
- **China** – Personal Information Security Specification (May 2018) and Amendments (entering into force in October 2020), Regulation on the Protection of Children’s Personal Information Online (October 2019), Draft Measures (proposed in May and June 2019) under discussion.
- **Thailand** – Personal Data Protection Act (entering into force in May 2020)
- **Singapore** – Personal Data Protection Act (PDPA) (2012)
- **New Zealand** – Privacy Bill 34-2 (still in drafting stage, entry into force planned for November 2020)
- **Australia** – Privacy Act 1988 and amendments (last amended in March 2014, including 13 Australian Privacy Principles)

https://medium.com/credify/data-regulations-for-business-743c69ee327b
sonnyzulhuda.com
PDP LAW

KEY ISSUES OF DATA PROTECTION
<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Collection</td>
<td>The collection of personal data shall be limited, specific, lawful, fair and</td>
</tr>
<tr>
<td></td>
<td>transparent.</td>
</tr>
<tr>
<td>b. Processing</td>
<td>Personal data shall be processed only for the purpose it is collected.</td>
</tr>
<tr>
<td>c. Processing Rights</td>
<td>Data is processed with ensuring rights of data subjects.</td>
</tr>
<tr>
<td>d. Accuracy</td>
<td>Personal data processed shall be accurate, complete, not misleading, update,</td>
</tr>
<tr>
<td></td>
<td>and accountable.</td>
</tr>
<tr>
<td>e. Protection</td>
<td>Personal data shall be protected from unlawful access, disclosure, and</td>
</tr>
<tr>
<td></td>
<td>modification; and shall be protected against misuse, damage, and loss.</td>
</tr>
<tr>
<td>f. Notification</td>
<td>Data subject must be informed of the processing purpose and activities, and</td>
</tr>
<tr>
<td></td>
<td>of any breach of data protection.</td>
</tr>
<tr>
<td>g. Disposal</td>
<td>Personal data shall be disposed of/deleted after the end of retention time</td>
</tr>
<tr>
<td></td>
<td>or as requested by the data subject.</td>
</tr>
<tr>
<td>h. Processing</td>
<td>Personal data processing shall be conducted responsibly in compliance of</td>
</tr>
<tr>
<td></td>
<td>the principles of data protection principles.</td>
</tr>
</tbody>
</table>

**Data Protection Principles in Indonesian Draft PDP Law – Article 17(2)**

- a. The collection of personal data shall be limited, specific, lawful, fair and transparent.
- b. Personal data shall be processed only for the purpose it is collected.
- c. Data is processed with ensuring rights of data subjects.
- d. Personal data processed shall be accurate, complete, not misleading, update, and accountable.
- e. Personal data shall be protected from unlawful access, disclosure, and modification; and shall be protected against misuse, damage, and loss.
- f. Data subject must be informed of the processing purpose and activities, and of any breach of data protection.
- g. Personal data shall be disposed of/deleted after the end of retention time or as requested by the data subject.
- h. Personal data processing shall be conducted responsibly in compliance of the principles of data protection principles.
## Data Protection Principles in the European General Data Protection Regulation (GDPR) – Article 5

<table>
<thead>
<tr>
<th>Principle</th>
<th>Article Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Lawfulness Principle – Art. 5(1)(a)</td>
<td></td>
</tr>
<tr>
<td>2. Fairness Principle – Art. 5(1)(a)</td>
<td></td>
</tr>
<tr>
<td>3. Transparency Principles – Art. 5(1)(a)</td>
<td></td>
</tr>
<tr>
<td>4. Purpose Limitation Principle – Art. 5(1)(b)</td>
<td></td>
</tr>
<tr>
<td>5. Data Minimisation – Art. 5(1)(c)</td>
<td></td>
</tr>
<tr>
<td>6. Accuracy Principle – Art. 5(1)(d)</td>
<td></td>
</tr>
<tr>
<td>7. Storage Limitation – Art. 5(1)(e)</td>
<td></td>
</tr>
<tr>
<td>8. Data Security (Integrity and Confidentiality) Principle – Art. 5(1)(f)</td>
<td></td>
</tr>
<tr>
<td>9. Accountability Principle – Art. 5(2)</td>
<td></td>
</tr>
</tbody>
</table>
Data Protection Principles in Indonesian Draft PDP Law – Article 17(2)

a. The collection of personal data shall be limited, specific, lawful, fair and transparent.
b. Personal data shall be processed only for the purpose it is collected.
c. Data is processed with ensuring rights of data subjects.
d. Personal data processed shall be accurate, complete, not misleading, update, and accountable.
e. Personal data shall be protected from unlawful access, disclosure, and modification; and shall be protected against misuse, damage, and loss.
f. Data subject must be informed of the processing purpose and activities, and of any breach of data protection.
g. Personal data shall be disposed of/deleted after the end of retention time or as requested by the data subject.
h. Personal data processing shall be conducted responsibly in compliance of the principles of data protection principles.

Data Protection Principles in the European General Data Protection Regulation (GDPR) – Article 5

1. Lawfulness Principle – Art. 5(1)(a)
2. Fairness Principle – Art. 5(1)(a)
3. Transparency Principles – Art. 5(1)(a)
4. Purpose Limitation Principle – Art. 5(1)(b)
5. Data Minimisation – Art. 5(1)(c)
6. Accuracy Principle – Art. 5(1)(d)
7. Storage Limitation – Art. 5(1)(e)
8. Data Security (Integrity and Confidentiality) Principle – Art. 5(1)(f)
9. Accountability Principle – Art. 5(2)
Fintech Lending Landscape in Indonesia

116 Registered Companies
77 Licensed Companies
193 P2PL comps
132M People without bank credit access
46.6M SMEs w/out credit access
667K Lenders using Fintech
64.8M Borrowers using Fintech

Rp 221,000,000,000,000
Successfully distributed loan (Jun 2021)
Source: OJK, AFPI
Fintech Lending Landscape in Indonesia

LINDUNGI DATA PRIBADI NASABAH PINJAMAN ONLINE

Catatan LBH Jakarta:

- 1,330 laporan korban pinjaman online (pinjol) dari 25 provinsi
- 89 fintech melanggar hukum dengan menyebar data pribadi nasabah
- 25 fintech yang melakukan penyebaran data pribadi terdaftar di OJK
- Akibat persebaran data, korban menerima ancaman, fitnah, hingga pelecehan seksual

3.193 PINJAMAN ONLINE ILEGAL DIBLOKIR

Satgas Waspada Investasi (SWI) Otoritas Jasa Keuangan (OJK) memblokir 3.193 pinjaman online atau pinjol ilegal.

Masyarakat terjebak pinjol ilegal karena rata-rata tidak meminta persyaratan yang ketat untuk menggaet nasabah.

Pembiayaan yang disediakan biasanya dengan bunga tinggi, mudah ditentukan, dan mudah disalahgunakan.

1. Satgas Waspada Investasi (SWI)
2. Otoritas Jasa Keuangan (OJK)
3. Pinjaman online ilegal
4. Masyarakat terjebak pinjol ilegal
5. Bunga bisa sampai 2-4% per hari
6. Pinjol ilegal yang diblokir 3.193 pinjol ilegal

Source: MNC Portal Indonesia | HSKB: Tim Okezone | INFRAKASI: Bayu Airlango

sonnyzulhuda.com
The collection of personal data shall be limited, specific, lawful, fair and transparent.

In May 2019, a German police officer was fined by the country’s Data Protection Authority EUR 1400 (Rp 23 million) for obtaining car license plate data via the official Central Traffic Information System of the Federal Motor Transport Authority and using it for private contact.

The police officer has processed personal data outside the scope of the law.

This infringement is attributable to him personally as he does not have sufficient legal basis for data processing contrary to Art. 6 GDPR.
In September 2021, a restaurant owner in Spain was fined EUR 3,000 (he Spanish DPA (AEPD) has fined a bar owner EUR 3,000 (Rp 49 million) for distributing a CCTV images through WhatsApp and online media which shows an accident that involved one customer of the restaurant.

The CCTV was meant for security purposes, therefore the images/videos shall not be distributed publicly as it is not in line with the security purpose.

As the publication of the images was not related to the purpose of the video surveillance, the restaurant owner as data controller violated the Purpose Limitation principle under the GDPR.
In April 2014, a Malaysian actress sued Malaysia Airlines over the publication of her flight details on a Facebook account. The posting of their boarding passes caused them to suffer emotional stress.

At the KL International Airport, the couple had given their boarding passes to the airliner staff at the departure gate. It appeared that the staff had subsequently taken the picture of the passes and uploaded them online.

In an out-of-court settlement, the couple received an undisclosed amount of compensation.

Legally, this would have potentially amounted to a violation of the purpose limitation principle of the PDP law.
A third party training vendor to Singapore Armed Forces was fined SGD 35,000 (Rp 367 million) in June 2021 for their failure to apply security measures to the data of more than 110,000 people in total.

- The database was affected by ransomware which locks up the data
- The vendor only applies a single, simple password, which was shared between few employees.
- Insufficient authentication method to protect the account from unauthorised log-ins.
In June 2021, the authority in Poland imposed a fine of EUR 3,000 (Rp 49 million) on a legal education foundation. The Foundation had earlier suffered from data breaches (i.e. data theft) and had failed to notify the authority about the breach. The failure to notify the authority amounts to a violation of a breach notification duty. The data file that was stolen included the names, addresses and telephone numbers, and also the national ID numbers of 96 individuals.

Data subject must be informed of the processing purpose and activities, and of any breach of data protection.
1. The use of **P2P Lending customers’** personal information irresponsibly to intimidate the customers upon repaying their loan.

2. The **disclosure of Covid-19 patients** information without consent or necessary procedure.

3. **Discreet collection of facial information** from surveillance camera for commercial purposes.

4. Failure to **notify the detailed purposes** and usage of personal information collected from the Covid-19 tracking apps.

Personal data processing shall be conducted responsibly in compliance of the principles of data protection principles.
LESSON LEARNED

KEY TAKEAWAYS
PDP deals with the full processing from collection to disposal. Confidentiality or security is only a component of it.

**Full Data Lifecycle**
PDP deals with the full processing from collection to disposal. Confidentiality or security is only a component of it.

**Data Stakeholders**
Data is not “owned” by the data user. Individuals’ rights are involved.

**Data Due Diligence**
Data is viewed as assets that have to be managed and protected within appropriate measurable steps.

**New Offences**
Restrictions are introduced to reshape the new expected behaviour on data.

**Data Accountability Over Sovereignty**
While it is important to preserve data sovereignty, data accountability is the priority.

**Resetting Data Culture**
Information society requires a resetting of ethical and cultural adjustment towards data.
Key debates on Indonesian Draft PDP Law

- Supervisory & Enforcement Authority?
- Legal and Institutional Harmonisation
- Ensuring efficient sanctions: Criminal, civil & administrative
- Data Sovereignty
Closing Remarks

01. PDP Law is about respect and dignity of every human being – fundamental rights to privacy

02. PDP Law seeks to strengthen national security and economic resilience

03. PDP Law sets a new norm in international trade

04. PDP Law governs data across sectors and industries

05. PDP Law evolves, changes and complicates alongside the technology
THANK YOU

DR SONNY ZULHUDA

Associate Professor at the International Islamic University Malaysia

sonny@iium.edu.my
sonnyzulhuda.com
twitter.com/zulhuda