Cybersecurity Law
Important notices for business enterprises

Institute for Policy Studies and Media Development (IPS)
Hanoi, 16th August, 2018
Content

Part 1
Key features of Cybersecurity Law

Part 2
6 key issues and 6 groups of business enterprises

Part 3
Law drafting procedure: Guiding decree – What do business enterprises need to do?

Part 4
Implementing agency of Cybersecurity Law – trends and notices
Part 1: Key features of Cybersecurity Law
Transferring authority

Old issues
Vs
New administration
2 major areas

Cyber Attack

Content / Data
Hate speech, Fake news

Information security
Specialized agency for Cybersecurity
Instructing documents

• 2 Decrees
• 1 Resolution
Part 2:
6 major issues & 6 business groups under consideration
6 major issues

- National security information system
- Responsibilities towards users’ data
- Measures to protect Cyber security; report problems; and alert breakdowns
- Evaluating, investigating & inspecting cyber security
- Fake news & Hate speech – Prevent, Delete, Remove, & Cut-off Services
- Verifying users’ accounts
6 business groups

- Data exploiters (Google, Facebook, Zalo)
- E-Commerce
- Software applications/ Startup
- Data services (Cloud Computing)
- Finance & Banking
- Trading services & cybersecurity solutions
About users’ data

Article 26, Part 3:

Domestic and overseas providers of telecommunications services, internet services and value-added services in Vietnam’s cyberspace that collect, analyze or process private information or data about relationships of their service users or data created by their service users in Vietnam shall retain such data for a specific period of time defined by the Government.
Digital accounts - Part 2, Article 26

Article 26:
a) Verify users’ information when they open digital accounts; protect confidentiality of users’ information and accounts; provide users’ information for professional cybersecurity forces of the Ministry of Public Security upon request in writing to serve investigation into cybersecurity violations;
The definitions of : Fake news and Hate speech

1. A piece of information in cyberspace will be considered propaganda against the government of Socialist Republic of Vietnam if it:

   a) slanders or defames the people's government;
   
   b) is used for psychological warfare; provokes war of aggression; causes discrimination against or hostility towards a race, religion or country;
   
   c) offends the people or desecrate the national flag, national anthem, political leaders, honored people or national heroes.
The definitions of: Fake news and Hate speech

2. A piece of information in cyberspace will be considered provoking riots or disturbing the peace if it:

a) persuades, encourages, deceives, threatens people or causes discrimination for the purpose of armed activities or use of violent force to oppose the people's government.

b) encourages, deceives, threatens or persuades people to participate in public gathering intended to cause disruption or oppose law enforcers or obstructs operation of an organization, thus threatens public order and security
The definitions of: Fake news and Hate speech

3. A piece of information in cyberspace will be considered humiliating or slandering if it:

   a) seriously harms another person’s dignity or honor;

   b) is fabricated to harm another person’s dignity or honor or violate lawful rights and interests of another organization or individual.
The definitions of: Fake news and Hate speech

4. Information in cyberspace that is meant to commit violations against regulations of law on economic management includes:

a) Fabricated or false information about products, goods, money, bonds, treasury bills, checks and other financial instruments;

b) Fabricated or false information about finance, banking, e-commerce, electronic payment, foreign exchange, capital raising, multi-level marketing, securities.
The definitions of: Fake news and Hate speech

5. Other fabricated or false information in cyberspace that is meant to cause public confusion or economic loss, obstructing regulatory bodies or law enforcers, violate lawful rights and interests of other organizations and individuals.
Enterprises’ responsibilities towards Fake news & Hate speeches

Article 26

b) Block and delete information mentioned in Clause 1 through 5 Article 16 of this Law on their services or information systems within 24 hours after a request is given by the cybersecurity force of the Ministry of Public Security or a competent authority of the Ministry of Information and Communications; keep a log of such events to serve investigation into cybersecurity violations for a certain period of time specified by the Government;

c) Stop providing or refuse to provide the aforementioned services for the organizations or individuals that post the information mentioned in Clause 1 through 5 Article 16 of this Law upon request by the cybersecurity force of the Ministry of Public Security or a competent authority of the Ministry of Information and Communications.
Information system infrastructure

**Article 10: National security information systems**

1. A national security information system is an information system which will cause serious cybersecurity issues if it is broken down, infiltrated, overridden, interfered with, disrupted, paralyzed, attacked or sabotaged.

2. National security information systems include:
   a) Military, security, diplomacy and cryptography information systems;
   b) Systems for archiving and processing state-secret information;
   c) Information systems serving storage of particularly important items and documents;
   d) Information systems serving storage of materials or substances that are particularly harmful to humans or the environment;
   dd) Information systems serving storage, manufacturing and management of other facilities relevant to national security;
   e) Important information systems serving operation of central organizations;
   g) National information systems serving energy, finance, banking, telecommunications, transport, resources and environment, chemical, health, culture and press authorities;
   h) Automatic monitoring and control systems at important works relevant to national security or national security targets.
Authority of Cyber Security Law Force towards information infrastructure – National security information systems

a) Assess cybersecurity;
b) Evaluate cybersecurity conditions;
c) Inspect cybersecurity;
d) Monitor cybersecurity;
What are objects inspected?

<table>
<thead>
<tr>
<th>Part 3, Article 13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity inspection shall be carried out for:</td>
</tr>
<tr>
<td>a) Hardware systems, software systems, digital devices in information systems;</td>
</tr>
<tr>
<td>b) Cybersecurity regulations and measures;</td>
</tr>
<tr>
<td>c) Information stored, processed and transmitted within the information system;</td>
</tr>
<tr>
<td>d) Cybersecurity incident response and remediation plans of the information system admin;</td>
</tr>
<tr>
<td>dd) Measures for protection of state secrets; prevention of leak of state secrets through technical channels;</td>
</tr>
<tr>
<td>e) Cybersecurity protection.</td>
</tr>
</tbody>
</table>
What about those that are not listed as National security information systems?

**Article 24: Inspection of cybersecurity of information systems other than national security information systems**

1. An information system other than national security information systems shall undergo cybersecurity inspection in the following cases:
   a) There is a violation of regulations of law on cybersecurity that violates national security or seriously disrupts public order;
   b) The inspection is requested by the administrator of the information system.
Other vital issues

• Measures to protect cybersecurity (Article 41) – (Responsibilities of service providers in cyberspace)

• Alert users of cybersecurity threats and risks (Article 41)

• Protect children on cyberspace: Negative content towards children

• Representative office of foreign enterprises (Article 26)
Implementing Cybersecurity Law – whose authority?

• Merge Cybersecurity Department and the Police Department for High-Tech Crime Prevention;
• Cybersecurity specialized agency;
• Managing agency: ‘Administrators’ + Cybersecurity Force:
  + Ministry of Information and Communications;
  + In-charge Ministry
Part 3: Law drafting procedure: Guiding decree – What do business enterprises need to do?
Documents instructing implementation – What should business enterprises do?

• 2 decrees: Specification of content and procedures
• 1 Resolution: National security information systems
• Issues that need further instructions:
  + Which users’ data should be localized in Vietnam? – business costs and benefits
  + Which kinds of information belong to ”National security information systems”?
  + Verification of “Digital accounts” – what kinds of digital accounts?
  + Representative Office of foreign enterprises?
Drafting and recommending procedures for Draft Decree

• Editing agency: Ministry of Public Security (Cybersecurity Department)

• Draft to present to the government: October;

• Deadline to make recommendations to the Decree;

• Contributing channels;

• Updating information channels
Part 4: Cybersecurity implementing agency – trends and notices
Long-term cybersecurity trends – Protecting users’ data

• Enhance privacy rights and capacity to control users’ data;

• Tighten/ strengthen legal responsibilities to protect data and impose strict regulations on business enterprises;

• GDPR

• Enterprises’ responsibilities to actively protect users/ customers
### Popular regulations about data protection

<table>
<thead>
<tr>
<th></th>
<th>Brazil</th>
<th>China</th>
<th>The EU</th>
<th>India</th>
<th>Indonesia</th>
<th>South Korea</th>
<th>Viet Nam</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data localization</strong></td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Partial</td>
<td>Yes</td>
<td>Partial</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Consent to collect data</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Consent to transfer data to third parties</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Right to consider</strong></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Right to forget</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Alert misconduct</strong></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Evaluate impacts</strong></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Data security officials</strong></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Punish violations</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Request Government’s access</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Request to save data</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

(Source: European Center for International Political Economy, 2014)
Summary – Important articles:

• Article 5 – Cybersecurity protection measures, together with regulations on authority of cybersecurity specialized agency and enterprises’ additional responsibilities;

• Article 10 – About National security information system

• Article 16 – About misinformation, hate speech, fake news

• Article 26 – Direct responsibilities of enterprises;

• Article 41 – Other compliance responsibilities
THANK YOU!