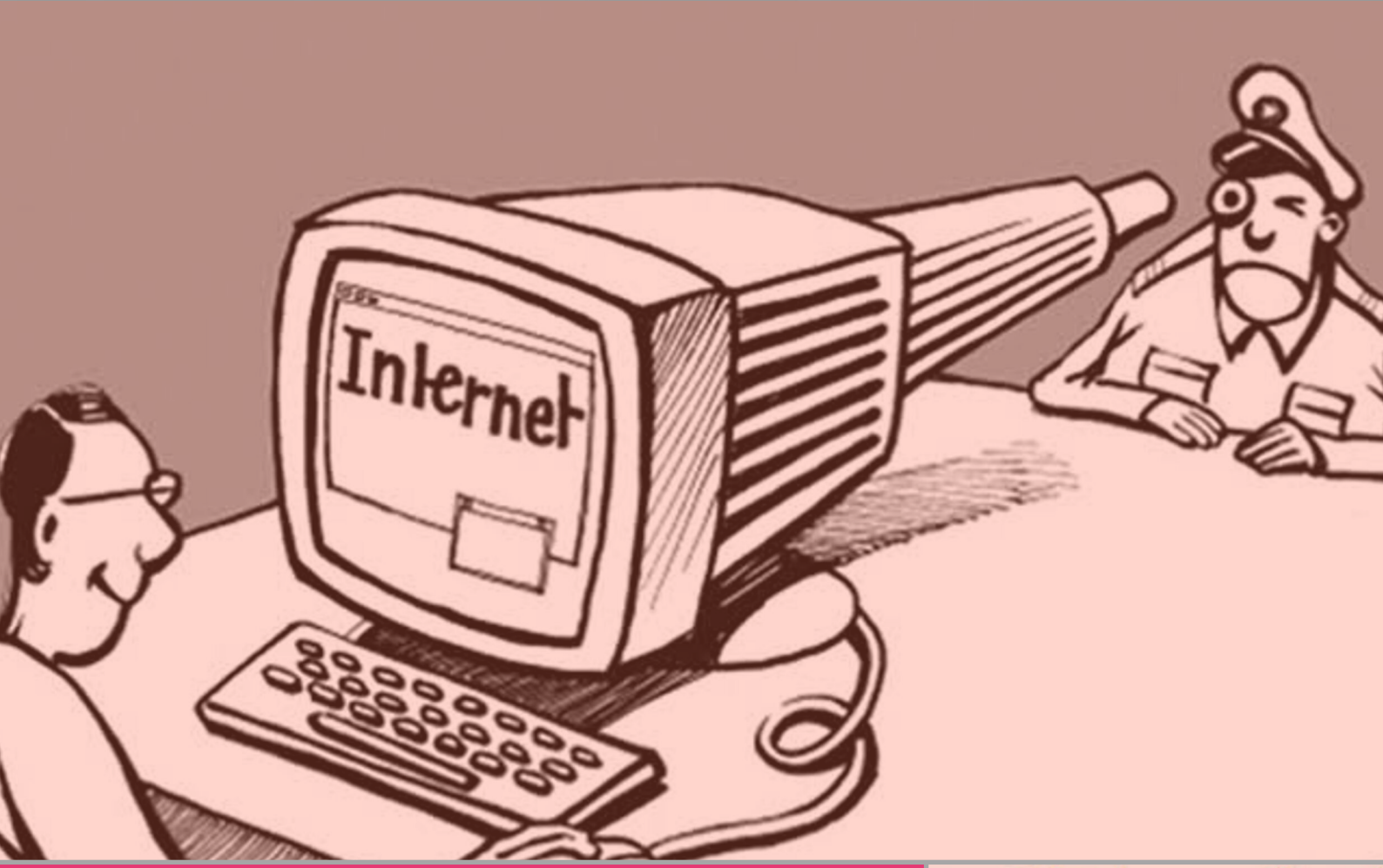


THAILAND'S CYBERSECURITY ACT: DOs & DON'Ts

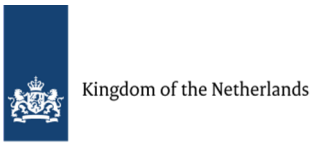
Towards a Human-centred Act protecting online freedom and privacy, while tackling cyber threats

September 2019

MANUSHYA
Empowering Communities | Advancing Social Justice

Acknowledgements:

Manushya Foundation would like to sincerely thank the **Netherlands Embassy in Thailand**, **Access Now**, **Thai Netizen Network** and **FIDH** for their kind support and partnership on its *'Thailand's Cybersecurity Act'* project.



Authors:

Emilie Palamy Pradichit,
Founder & Director
and
Ananya Ramani,
Human Rights Research & Advocacy Officer,
Manushya Foundation

Publication design:

Laurene Cailloce,
Communications & Advocacy Volunteer,
Manushya Foundation

Photos credit:

Cover page: Cartoon by Patrick Chappatte for the International Herald Tribune (known now as The International New York Times); and Digital communications image via shutterstock.com
Page 4: Photo by Reuters, from Daily Mail Online; and Cybersecurity picture from pexels.com
Page 5: Picture from Mailfence

For more information about Manushya Foundation's Digital Rights project, please contact:

Emilie Palamy Pradichit, Founder & Director
emilie@manushyafoundation.org

Ananya Ramani, Human Rights Research & Advocacy Officer
ananya@manushyafoundation.org

CHALLENGE 1: Broad scope and definition *using National security, economic security, martial security and public order in the implementation and monitoring of the Act*

DOs

1. **DO** ensure the scope and definition of cybersecurity threats and other aspects adequately takes into consideration democratic aspirations and human rights.
2. **DO** ensure all limitations to rights are clearly explained, compliant with the rule of law and necessary in accordance with the law, in line with Thailand's international human rights obligations under ICCPR.
3. **DO** consider the impact of a cyber threat on the availability, confidentiality and integrity of information and its related infrastructure; as well as on the security of individuals.
4. **DO** guarantee data privacy and data protection throughout the Act, with an authority specifically responsible for protection of collected data and information.

DON'Ts

1. **DON'T** focus the scope of the Act on security and other particular versions of security such as national security, economic security, martial security and public order, without clarification as to what those security configurations are.
2. **DON'T** broadly limit rights and freedoms guaranteed in the Constitution, using the explanation of national security and public order both of which are not properly defined.
3. **DON'T** require a response against everything that is believed to threaten national security, economic security, martial security and public order which is seen as affecting State power and stability.
4. **DON'T** permit authorities under the Act to compel the violation of rights while implementing it, instead actions must follow procedural fairness, due process and due care in a timely manner.

CHALLENGE 2: Problematic substantive provisions and failure to define them *in relation to Three Level of Cyber Threats (non-critical, critical and crisis threats)*

DOs

1. **DO** define limits and conditions to prove that a cybersecurity threat exists, to assess damage caused and to determine a response in preventing, addressing and mitigating threats; and protect human rights as enshrined in the Constitution, in domestic legislation and international human rights law in this process.
2. **DO** provide clear criteria to identify a cyber threat, make it publicly available, and ensure it is supported by evidence.
3. **DO** apply a higher standard of proof to identify evidence that a cyber threat exists through effective investigation or evidence that establishes the belief that there may be a risk of serious harm.
4. **DO** protect human rights as enshrined in the Constitution, in domestic legislation and international human rights law in this process, while identifying and responding to threats and damage caused.
5. **DO** limit damage to the extent possible and provide compensation for damages incurred when unavoidable.
6. **DO** give individuals a choice on how to respond with respect to actions taken by the authorities under the Act.

DON'Ts

1. **DON'T** make a cybersecurity threat where one does not exist, by relying on fictitious criteria.
2. **DON'T** act without clear evaluation on the existence of a cybersecurity threat.
3. **DON'T** identify and act upon a threat based on suspicion or that a threat may exist, without investigation as this assumes guilt and does not rely on proof.
4. **DON'T** allow for conflict between rights and action taken to deal with cybersecurity threats, such as violation of the right to privacy as well as accessing computer systems and extracting information only 'as necessary'.
5. **DON'T** compel any individuals to give permission unless voluntary to enter, access and search premises under the Act
6. **DON'T** allow for any action to be taken in the case of crisis-level threats, without any explanation of what action will be taken.

CHALLENGE 3: Controversial control mechanisms (government bodies and agencies) under the Act: *Top-down structure, broad powers given to authorities putting netizens under surveillance, lack of transparency and standards*

DOs

1. **DO** ensure the act is only applied to what is necessary to achieve a legitimate goal, proportionate to the goal to be achieved, and addressed through appropriate action. To do so, ensure capacity building education beforehand, including having outreach to law enforcement officials and provide them with training on human rights and privacy, as well as with cyberliteracy so as to not abuse their power.
2. **DO** ensure bodies and agencies under the Act include independent experts representing all stakeholder groups, selected in a transparent manner and subject to review, to guarantee power is vested in an independent agency and not with the executive branch or a body which is vested with the security of the people.
3. **DO** ensure that all bodies and agencies under the Act abide by laws on labour protection, labour relations, social security, and compensation.
4. **DO** ensure all policy and action under the Act is evidence based, with clear reasons, precise, comprehensive, publicly available and accessible.
5. **DO** provide appropriate and effective safeguards for handling personal information retained by authorities to investigate cyber threats, while utilizing innovation and collaboration. To do so, provide guidelines or standard operational procedures in terms of power and how authorities are supposed to act. These should align with international good practices adopted by other countries.

DON'Ts

1. **DON'T** allow powers of government agencies and bodies to be applied broadly, without explaining how they will be applied or without checks and balances to their power.
2. **DON'T** allow bodies and agencies established under this Act to retain power to implement the Act, with a few powerful government officials who already misinterpret and misuse other related laws, such as the Computer Crime Act and that are tasked with monitoring fake news.
3. **DON'T** allow for exemptions to authorities to exercise broad powers, such as the Office of the National Cybersecurity Agency that is recognized as a juristic person instead of a public office thus exempting it from the application of administrative law.
4. **DON'T** act without following guarantees of procedural fairness and due process, including consulting with all stakeholders, such as authorities under the Act, private sector, civil society and technical experts.
5. **DON'T** demand information, documents, copies of documents deemed necessary to assess a cyber threat; don't search premises, computers and/or computer systems and confiscate documents and/or computers for the same purposes, without notifying users that such information is being accessed and retained in the first place.

CHALLENGE 4: Powerplay in the application of the Act: *Control over Critical Information Infrastructures (CII) and reporting obligations placed on them*

DOs

1. **DO** provide clear criteria for identification of critical information infrastructure (CII), receive input of all stakeholders, give specific examples, limit control to situations considered legitimate in a democracy, and allow for review by an independent, multi-stakeholder body.
2. **DO** draw a connection between the damage caused to the critical information infrastructure (CII) and the destructive impact on an important aspect to be protected.
3. **DO** apply the same standards to government agencies and private entities recognized as CII.
4. **DO** allow individuals and CIIs sufficient time and opportunity, to provide information to establish why they are unable to carry out an action including legal and technical limitations.

DON'Ts

1. **DON'T** give broad powers to any government body that is not independent and impartial for designating any organization as a CII.
2. **DON'T** identify critical information infrastructure (CII) as just anything related to national security, economic security, martial security and public order.
3. **DON'T** require over-reporting cyber threats where 'a real risk of harm' does not exist.
4. **DON'T** place strict obligations on individuals and CIIs to report cyber threats or to follow orders for tackling them, that they cannot comply with or place heavy fines and penalties for this.

NATIONAL SECURITY ?

CHALLENGE 5: Absence of checks and balances: *Cybersecurity Threats, lack of accountability and the use of the Court system*

DOs

1. **DO** guarantee bodies and agencies under the Act are transparent and accountable, and report on their actions on a yearly basis; and establish an independent monitoring mechanism, comprising relevant stakeholders (government, private sector, national human rights commission, civil society and experts) to monitor and assess the work and actions of bodies and agencies under the Act.
2. **DO** establish a special court comprising specialized judges with necessary legal and technical expertise, and knowledge on the content and process of the Act to consider cases and provide remedy, including through temporary orders or injunctions against unlawful actions.
3. **DO** allow for investigation of complaints, review & monitoring of action by an independent, multi-stakeholder agency that carries out this duty with equal representation of government representatives, the private sector, and civil society.
4. **DO** guarantee protection to individuals by limiting the damaging impact that can be caused from the misuse of information, that is retained under this Act.
5. **DO** guarantee identification of an action taken against crisis cybersecurity threats is done after seeking court permission & that these steps can be reviewed by an independent multi-stakeholder body of experts.

DON'Ts

1. **DON'T** give broad powers to government bodies and agencies under the Act allowing for a lack of check and balance of their decision-making and actions.
2. **DON'T** prevent action taken against authorities for misuse, wrongful application or excessive action under the Act, including access to courts to appeal specifically in the case of action taken with respect to critical and crisis level threats.
3. **DON'T** reach decisions on determination of threat level, damage, and compensation only with review by Cabinet and without input of an authority that is independent, impartial or competent, or without the support of an ombudsperson.
4. **DON'T** allow the information collected under the Act to be used in lawsuits under other laws, especially in cases claiming defamation, libel, slander against the government, and committing a crime under the Computer Crime Act.
5. **DON'T** access real-time computer information or analyze the content of information, when having to deal with crisis cybersecurity threats and don't take action without seeking court permission.

CHALLENGE 6: Failure to ensure remedies: *Grievance redressal, imprisonment, fine and compensation*

DOs

1. **DO** provide effective remedy and compensation to any victim of bad evaluation of cyber-threat and wrongful application of the Act, whose information has been seized unfairly and inappropriately.
2. **DO** permit the challenging of the criminal penalty and fine set under the Act, by those whose information has been collected and revealed so they get fair treatment, compensation based on damage and to prevent repetition of this situation.
3. **DO** give an opportunity to provide a reasonable explanation or to remedy any situation, where an individual is held responsible for acts committed to the private sector entity he belongs to or makes decisions for.

DON'Ts

1. **DON'T** allow persons or officers to access information under this Act while there was no existence of a real cyber-threat
   &
   DON'T prevent remedy against authorities for misuse, wrongful application or excessive action under the Act, specifically by appealing these actions in court when critical and crisis level threats occur.
2. **DON'T** allow persons or officers who get access to information under this Act to misuse it or reveal it by negligence, without providing a grievance redressal mechanism that is effective and can be accessed.
3. **DON'T** hold an individual liable for an offense by a juristic person, resulting from an act or omissions following an order made by them.


HANDS OFF
MY INTERNET!
THE INTERNET
TOOL OF THE PEOPLE
DO YOU REALLY WANT
YOUR GOVERNMENT
TO CONTROL IT?
© Reuters


Security


©Mailfence

MANUSHYA

Empowering Communities | Advancing Social Justice

About Manushya Foundation

Founded in 2017, Manushya Foundation serves as a bridge to engage, mobilise, and empower agents of change by: connecting humans through inclusive coalition building and; by developing strategies focused at placing local communities' voices in the centre of human rights advocacy and domestic implementation of international human rights obligations and standards.

Manushya Foundation strengthens the solidarity and capacity of communities and grassroots to ensure they can constructively raise their own concerns and provide solutions in order to improve their livelihoods and the human rights situation on the ground.

CONTACT US:

5/4 Thanon Sutthisan Winitchai 1, Samsen Nai, Phayathai, Bangkok 10400, Thailand

contact@manushyafoundation.org

+66 (0) 945-811-827

www.manushyafoundation.org

facebook.com/ManushyaFdn

twitter.com/ManushyaFdn