LAO-VIET INTERNATIONAL TRANSLATION AND ADVERTISING SOLE CO.,LTD

LAO PEOPLE'S DEMOCRATIC REPUBLIC
PEACE INDEPENDENCE DEMOCRACY UNITY PROSPERITY

National Assembly **No. 61/NA**

Vientiane Capital, 15 July 2015

Law on Prevention and Combating Cyber Crime

Part I
General Provisions

Article 1. Purpose

This Law defines principles, regulations and measures on the managing, monitoring, inspecting the campaign of preventing and combating cyber crime to make it efficient aimed at preventing, combating, curbing and eliminating crime, protecting database system, server system, computer data and information in order to ensure the national security, create peace and order in society, integrate it regionally and internationally, and contributing to national socio-economic development with gradually and sustainably progress.

Article 2. Prevention and Combating Cyber Crime

Cyber Crime is a computer-related offence causing damages to state, person, legal entity, organization and society in accordance with the prescribed offences in the Article 8 of this law.

Prevention and Combating Cyber Crime is an act of curbing, eliminating and suppressing of persons, legal entities and organizations that are provided authorities and duties by state for directly finding cyber crime and implementing their tasks of prevention and combating cyber crime as prescribed in Article 19 and 24 of this law.

Article 3. Definitions

The terms used in this law have the following meaning:

1. **Crime** means any offence prescribed in the Penal Code and any other law prescribed criminal penalty;

2. **Computer System** means a piece of electronic equipment or sets of electronic equipment units is integrated together, for which contains an ordering, sets of ordering and other related process to enable the electronic equipments to perform the duty of processing data automatically in a computer or any interconnected computers through computer network or internet system;

3. **Server System** means a service system providing through the Computer System including Database Server, Web Server, Mail Server, File Server and other related components;

4. **Computer's data and information** means data, message, program or database system, personal data and information, computer traffic data in form of data processing and enabling computer to perform a function;

5. **Database System** means a storage data system in form of electronic mean that being able to manage, modify and use.

6. **Personal Data and Information** means any data and information directly or indirectly relating and identifying individual, action of person, legal entity and organization;

7. **Computer Traffic Data** means data related to communication through computer system-based developed by a computer system as a part of communication chain showing sender, source of origin, intermediary, route, destination, time, date as well as size and duration of communication, type of service and other service concerned relating to computer system communication;

8. **Service Provider** means a person providing of communication data and information through computer system and/or a person providing of computer data storage;

9. **Automatically Data Processing** means a process of calculating and developing data in any computer system by a computer program;

10. **Program** means an ordering system or sets of ordering for computer's operating and performing as manufactured design;

11. **Virus** means any specifically developed program for wide spreading virus, damaging and destroying computer system, computer network, computer's data and information;

12. **Malicious Code** means any developed set of ordering for destroying computer system or hacking computer's data and information;

13. **Fishing Website** means any new creating website containing the same characters and components similar to the original website in order to deceive for obtaining consumer information;

14. **Vulnerability** means a weakness of any software or program which is not be accomplished or updated allowing an attacker to use for destroying computer system, hacking or changing data, information and others in computer system;

15. **Consumer Information** means any information on consumer's address such as postal address, electronic address, geographical address, internet protocol, telephone number and other related code applying into any computer;

16. **Specific Access Prevention Measure** means an applying of any specific tool and/ or program into any computers for prevention and combating others from unauthorized computer access;

17. **Online Social Media** means an internet system disseminating and providing data and information to public by means of computer equipments and communication devices;

18. **Animation** means any created image moving as live action which can be visible through an electronic device such as cartoon movies.

Article 4. State Policy on Campaign of Prevention and Combating Cyber Crime

The state supports using of computer system with safe, convenient, fast and fairness usage, and protects the legitimate rights and benefits of service provider, consumer of computer system service, computer's data and information in according to laws and regulations.

The state develops conditions and provides facilities for the campaign of prevention and combating cyber crime by contribution of budget, developing and supplying of personnel, technical equipment and vehicle, researching and applying modern technology, developing of related infrastructure for the effective implementation of mentioned campaign.

The sate takes the campaign of prevention and combating cyber crime as the main task and regards the dealing with the cyber crime the important task.

The state supports and encourages person, legal entity and organization from both domestic and foreign country to invest in technical production and modern technology as well as participating in the campaign of prevention and combating cyber crime.

Article 5. Principles of Prevention and Combating Cyber Crime

The campaign of campaign of prevention and combating cyber crime shall ensure the following main principles:

1. Compliance with state's policy, laws, strategic plan and national socio-economic plan;
2. National security, peace and society order as well as national culture and fine tradition of the nation;
3. Protection of national and official secret confidence, secret of person, legal entity and organization;
4. Unity, safety, convenience, fast and fairness;
5. Protection of legitimate rights and benefits of service provider, consumer of computer system service, computer's data and information in according to laws and regulations;
6. Participation of society;
7. Implementation of the international agreements and treaties which the Lao PDR is party to.

Article 6. Scope of the law enforcement

This law applies to person, legal entity and organizations, both domestic and foreign country, living and researching and operating computer system and computer's data and information in the Lao PDR.

Article 7. International cooperation

The state opens and encourages the relations and cooperation with foreign countries, regional and international community in campaign of prevention and combating cyber crime through exchange of lessons, information, experiences, information, upgrade of technical knowledge and capacity building of technical staffs concerned as well as identifying and certifying data and information in accordance with international agreements and treaties, which the Lao PDR is party to.

Part II
Offences Regarding as Cyber Crime

Article 8. Offences regarding as cyber crime

The Offences regarding as cyber crime are following:

1. Disclosing of Specific Computer Access Prevention Measure;
2. Unauthorized Computer Access;
3. Unauthorized Editing Picture, Animation, Audio and Video;
4. Unauthorized Interception of Computer's Data and Information;
5. Causing Damages via Online Social Media;
6. Dissemination of Pornography;
7. Computer System Interference;
8. Computer's Data and Information Forgery;
9. Destroying Computer's Data and Information;
10. Operating Business of Tools and Equipments for Cyber Crime.

Article 9. Disclosing of Specific Computer Access Prevention Measure

Disclosing of specific computer access prevention measure is an offence taking specific computer access prevention measure to reveal without any authorization causing damage to state, person, legal entity, organization and society.

Article 10. Unauthorized Computer Access

Unauthorized computer access is an offence applying an electronic equipment or device to access any computer having specific computer access prevention measure or steal any commercial, financial data and information as well as secret confidence, other related information of person, legal entity and organization.

Article 11. Unauthorized Editing Picture, Animation, Audio and Video

Unauthorized Editing Picture, Animation, Audio and Video is an offence of editing picture or image, adding or modifying the original version by mean of electronic process or other means in order to disseminate the outcome through computer system causing damage to state, person, legal entity and organization concerned.

Article 12. Unauthorized Interception of Computer's Data and Information

Unauthorized Interception of Computer's Data and Information is an offence of interception of Computer's Data and Information by mean of applying any electronic equipment or device while the receiver is receiving, or the sender is sending, data and information via computer system.

Article 13. Causing Damages via Online Social Media

Causing Damages via Online Social Media are offences in the action of following:

1. Posting of computer's data and information containing of context on slandering, blaspheming, using impolite words through computer system;
2. Applying of violence, false, misleading and deception information into computer system;
3. Bringing the computer's data and information destroying national security, peace, order in society, national culture and fine tradition of the nation to apply into computer system;
4. Bringing the computer's data and information containing of aspects of convening, persuading and encouraging people to resist the government or separate the national solidarity;
5. Advertising of drug, weapon of war, chemical weapon selling as well as human, prostitute, prostitution trafficking and other illegal products concerned;
6. Disseminating and sending of computer's data and information prescribed in Article 11 and 14 of this law including the title number 1, 2, 3, 4 and 5 in this Article.

Article 14. Dissemination of Pornography

Pornography is data and information containing of context clearly appearing in physical aspects such as picture and image, animation, audio, video relating to sexual organs and sexual activities of human.

Dissemination of Pornography is an offence of selling, buying, distributing, transferring, introducing and disseminating of above prescribed in this Article.

Article 15. Computer System Interference

Computer System Interferences are offences in the actions of following:

1. Using of comport program, virus or other tools to interrupt or destroy the performance of computing;

2. Sending of computer system data and information or electronic mail or message with concealing of address, source of sender to disturb and/or destroy the performance of computing.

Article 16. Computer's Data and Information Forgery

Computer's Data and Information Forgery is an offence of using the computer, computer system and electronic equipment or device by means of action of following:

1. Intentionally inputting and changing data and information, forgery of electronic address or deleting of data and information in any computer consequently causing outcome of changing from the original data and information;
2. Inputting and changing data and information of financial and commercial transaction, secrete confidence as well as other data and information of person, legal entity, organization without any authorization;
3. Developing of fake website to mislead, deceive other persons using computer system or internet to input data and information of bank account, credit card codes, internet usage card codes as well as the other data and information concerned.

Article 17. Destroying Computer's Data and Information

Destroying Computer's Data and Information is an offence of deleting, editing and/or modifying of computer's data and information or data and information in computer system in order to cause data and information in computer system being damage and different from original aspects.

Article 18. Operating Business of Tools and Equipments for Cyber Crime

Operating Business of Tools and Equipments for Cyber Crime is an offence of developing of any new specific program, producing, importing, possessing, selling and buying, distributing, advertising, disseminating or distributing of the tools and equipment such as computer program or designing of computer's data and information for committing any cyber crime.

Part III
Campaign of Prevention and Combating Cyber Crime
Chapter I
Campaign of Prevention Cyber Crime

Article 19. Campaign of prevention cyber crime

The Campaign of prevention cyber crime are activities following:

1. Warning Notice;
2. Consultation Providing;
3. Emergency Notification;
4. Incident Response.

Article 20. Warning Notice

Ministry of Post and Telecommunications is an organization issuing the notice of risk and hazardous incident occurring in computer system and internet such as the warning notice of fake website, malicious software, notification of vulnerability, misleading and deceiving via electronic mail and message and other risks concerned.

Service provider of computer system must issues the warning notice and set conditions for computer access in order to limit or disallow some user categories to access.

Article 21. Consultations Providing

Sector of Post and Telecommunications is an organization providing of consultation and advice on methodology for protection and technical process dealing with risk and hazardous incident for person, legal entity and organization in order to reduce losing and interrupting of data and information, stop suspending of computer system operation, anti wide spreading of computer virus and accessing to destroy data and information in any computer system.

Article 22. Emergency Notification

Person, legal entity and organization, in both domestic and foreign, living, involving and using of computer system and/or computer's data and information in the Lao PDR must notify the existing of emergency incident relating to cyber crime occurring in their computer system to the Sector of Post and Telecommunications as prescribed in the Article 50 and 51 of this law.

The emergency notification for general incidents should be conducted by means of following:

1. Submission of specific provided Application Form;
2. Informing via telephone, fax or hotline;
3. Sending of electronic mail or message;
4. Notifying through other means.

Article 23. Incident Response

After receiving the warning notice on emergency incident relating to computer system, Ministry of Post and Telecommunication should bring it into consideration and reply with suggestion of dealing methodology to address the incident within five official working days.

In case of necessary and urgent incident, Ministry of Post and Telecommunication should immediately take action technical response and addressing in accordance with the incident notification concerned.

In case of receiving of incident notification relating to the acts prescribed in the Article 11 and 13 of this law affecting national security or dignity of any person, sectors

concerned of both central and local levels should bring it into consideration and respond basing on situations of case by case.

Chapter II
Campaign of Combating Cyber Crime

Article 24. Campaign of combating cyber crime

The Campaign of combating cyber crime are activities following:

1. Organizing Dissemination;
2. Training;
3. Providing Knowledge on Computer System Safety;
4. Developing of Activities for Data and Information Protection;
5. Surveillance of Emergency Incident;
6. Collection of Statistics.

Article 25. Organizing Dissemination

Ministry of Post and Telecommunications is an organization developing of handbook, sticker, poster, printing matter and video on surveillance, prevention of risk and hazard incident for computer system, also coordinating with other relating sectors and local administration authorities concerned for organizing dissemination throughout nationwide.

Article 26. Training

Sector of Post and Telecommunications should coordinate with other relating sectors and local administration authorities concerned to organize the training for officials and authorities concerned on prevention and combating cyber crime as well as process of investigating operation.

Article 27. Providing Knowledge on Computer System Safety

Ministry of Post and Telecommunications is the leading organization for coordination with sectors concerned to constitute the specific measures for maintaining computer system security and providing knowledge on the specific measures for society.

Ministry of Post and Telecommunication should take a leading role to coordinate with Ministry of Education and Sport for taking of study subject on computer system security to apply in the curriculums from the level of secondary school.

Article 28. Developing of Activities for Data and Information Protection

In order to secure the computer system security and protection of computer's data and information, the Sector of Post and Telecommunications and Sector of National Security, service providers as well as computer's data and information storage

persons should develop activities to provide knowledge and lessons on security, using of computer system for acknowledgement and awareness of techniques and methodologies to protect computer's data and information in the state organizations, private sectors and educational facilities.

Article 29. Surveillance of Emergency Incident

Sector of Post and Telecommunications is an organization taking responsibility of surveillance of emergency incident by means of tracking, monitoring, advising, preventing and responding the risk and hazard incidents occurring in computer system.

Article 30. Collection of Statistics

Sector of Post and Telecommunications and Sector of National Security should collect statistics and develop database system on cyber crime as well as take the responsibility of periodically searching and reviewing in order to find out the conditions and causes of cyber crime.

Chapter III
Lao Computer Emergency Response Center

Article 31. Lao Computer Emergency Response Center

In order to ensure the managing, monitoring, inspecting, preventing, combating, restricting and suppressing of crime, protection of database system, server system, computer's data and information, and the capacity of integration with regional and international community; state establish the Lao Computer Emergency Response Team which is written in the abbreviation form of "Lao CERT".

Lao Computer Emergency Response Team is an organization having role at the relevant level of a department of ministry including in the organization structure of Ministry of Post and Telecommunication, having responsibility roles of chief of operation for the above prescribed ministry in this Article in responsibilities of preventing and addressing of risk and hazard incidents for computer system.

Article 32. Rights and Duties of Lao Computer Emergency Response Team

The Lao Computer Emergency Response Team has the following rights and duties:

1. Study and elaborate strategic plan, policies into its work plans, programs and projects as well as take them into account of effective implementation;
2. Study and develop the regulations on management of campaign of prevention and combating cyber crime with submission to Ministry of Post and Telecommunications for consideration;
3. Disseminate laws and regulations regarding to campaign of prevention and combating cyber crime;

4. Develop, train and upgrade personnel working on security of computer system;

5. Oversee, track, monitor, inspect, advise, notify and respond risk and hazard incidents for computer system as assigning;

6. Receive the warning notification and reporting of cyber crime to the sectors concerned;

7. Coordinate and cooperate with sectors concerned in case procedure process of cyber crime;

8. Inform the service providers, data and information storage persons to provide facilities and information relating to cyber crime;

9. Carry out relations and coordination with foreign countries, regional and international community related to campaign of prevention and combating cyber crime as assigning;

10. Summarize and report on its activities regarding to campaign of prevention and combating cyber crime Ministry of Post and Telecommunication on a regular basis;

11. Perform rights and duties as prescribed in the laws and regulations concerned.

Part IV
International Cooperation in Campaign of Prevention and Combating Cyber Crime

Article 33. Principle of International Cooperation

International cooperation in Campaign of Prevention and Combating Cyber Crime between organizations having authorities concerned of the Lao PDR and foreign organizations should follow the principle of respecting of independence, sovereignty and territorial integrity, non-interference in each other's domestic affairs, mutual obtaining benefits and conformity with international agreements and treaties which the Lao PDR is party to.

Article 34. Technical Subjects Cooperation

Technical Subjects Cooperation in Campaign of Prevention and Combating Cyber Crime should be included the following:

1. Exchanging of technical information including studying measures on prevention and combating of computer system emergency incidents;

2. Suspension or notification to stop computer system destruction;

3. Coordinating with service providers in foreign countries on using of the online social media containing contents defined in the Article 13 of this law;

4. Providing mutual assistance on surveillance, combating and responding the computer system emergency incidents in any significant events such as meeting or

convention of national, regional and international levels as well as other fairs and festivals.

Article 35. Mutual Legal Assistance

Mutual Legal Assistances shall be aimed at the requests for conducting of investigation, applying of counting measures, issuing of ordinance for storage and protection of computer's data and information as well as computer traffic data, searching, diagnosing and identifying of offenders, seizing or confiscating equipments or tools used in and related to offences, request for additional information and evidence related to offences as well as request for extradition.

The mechanism and procedures of Mutual Legal Assistance shall follows the related laws and regulation of the Lao PDR, international agreements and treaties, which the Lao PDR is party to.

Article 36. Content of the request for Mutual Legal Assistance

Request for Mutual Legal Assistance shall include the following contents:

1. Purpose, necessity reasons and de facto condition of the request;
2. Any important information necessary for identifying and tracing and diagnosing of cyber crime offenders;
3. Brief Summarizing of computer system's data and information or computer traffic data wanting to protect and storage.
4. Legislative references and basis towards offences of the accused and the suspect;
5. Information of organizations or authorities concerned for the case of asking for any additional information from the requesting state.

Article 37. Requirement of Confidentiality

The Competent authority of the Lao PDR must ensure the confidentiality of requests from the related states.

Article 38. Requests Refusal

The competent authority of the Lao PDR may refuse the requests of Mutual Legal Assistance while the requests are not consistent with the basic Principle of International Cooperation defined in Article 33 of this law as well as the other related laws of the Lao P.D.R.

Part V
Prohibitions

Article 39. General prohibitions

Persons, legal entity and organizations are prohibited from the following behaviors:

1. Committing of offences defined in Article 8 of this law;

2. Propagating to destroy or against the political regime in order to causing turbulence in society;

3. Destroying or causing damages to any electronic equipment, computer and other relating facilities for exchanging and transmitting data and information through computer system;

4. Callusing with any person to disseminate pornography contents through online social media;

5. Asking, requesting, providing and receiving bribes;

6. Committing other activities contravening laws and regulations.

Article 40. Prohibitions for Service Providers

Service Providers are prohibited from the following behaviors:

1. Deleting computer traffic data before ninety days in case of having connection system and three hundred sixty five days of having no connection system;

2. Deleting data and information of any user causing damages before ninety days;

3. Supplying incorrect data and information to officials and authorities concerned;

4. Disclosing of data and information of service consumers without any authorizing;

5. Providing conditions or facilities for activities of cyber crime;

6. Committing other activities contravening laws and regulations.

Article 41. Prohibitions for Official and Competent Authorities

Official and competent authorities are prohibited from the following:

1. Disclosing of confidential data and information of state, official affairs, person, legal entity, organization through computer system;

2. Reveal computer system access code and specific access prevention measure of their working sector;

3. Sending or transferring computer traffic data or consumer's data and information except the sending or transferring for the purpose of cyber crime case procedure such as implementation of ordinance or in case of authorizing of the case procedure organization.

4. Postponing, holding and falsifying documents relating to cyber crime data and information;

5. Abusing duties, functions and positions for personal, family and group of friends benefits and interests;

6. Leaving off duties and responsibilities assigned by their working organizations;

7. Committing other activities contravening laws and regulations.

Part VI
Investigation of Cyber Crime Case

Article 42. Causes for Opening of Investigation

Causes for Opening of cyber crime case are as following:

1. Having a claim, reporting or complaint of person, legal entity or organization concerning of any offence regarding as cyber crime;
2. Capitulating of cyber crime perpetrators;
3. Discovering of cyber crime trace, evidence as well as data and information concerned for the offences prescribed in the Article 8 of this law.

Article 43. Process of Investigation of Cyber Crime Case

The investigation of cyber crime case shall be conducted as follows:

1. Claiming, reporting or complaining;
2. Opening of investigation;
3. Conducting of investigation;
4. Summarizing of investigation and preparation of case file.

Article 44. Claiming, reporting or complaining

The claiming, reporting or complaining an offence regarding as cyber crime shall be brought to notify or submit to the investigation organization of police or office of public prosecutor.

The organization of police or office of public prosecutor shall study and consider the claiming, reporting or complaining within five official working days from the day of receiving the claiming, reporting or complaining. In case of having any difficulty, the study and consideration period shall not be more than ten official working days.

Article 45. Opening of investigation

In case of having sufficient information and evidence of any offence regarding as a cyber crime, the head of investigation organization of police or public prosecutor shall issue the ordinance of opening of investigation basing on the scope of rights and duties of the issuing the ordinance in according to the Law on Criminal Procedure.

In case of emergency, necessity and having sufficient information and evidence proving that there is a preparation or committing of cyber crime, the head of investigation organization of police or public prosecutor shall issue an ordinance for protection and storage computer's date and information as well computer traffic data.

Service providers or sectors having duties of data and information management have obligations of protection and storage the prescribed data and information in good condition till the final process of cyber crime case procedure in order to ensure that they are not being lost or damaged.

Article 46. Conducting of investigation

The investigation organization of police or office of public prosecutor shall coordinate with sector of post and telecommunication and other sectors concerned in order to search and trace information and evidence as well as source of cyber crime for regarding as the basis of investigation conducting.

The conducting of cyber crime case investigation shall apply the investigation procedures and the prevention measures as prescribed under the Law on Criminal Procedures.

Article 47. Summarizing of investigation and preparation of case file

After completion of an investigation, in case of having sufficient information and evidence supporting that such violation is a cyber crime, the investigation organization shall conclude and summarize the investigation with preparation a cyber crime case file and then forward to the public prosecutor for consideration to submit the prosecution to the court.

In case of the competent office of public prosecutor conducts the investigation, the office of public prosecutor shall conclude and summarize the investigation with preparation a cyber crime case file and then submit the prosecution to the court.

Part VII
Management and Inspection
Chapter I
Management

Article 48. Management Organization

The government is taking official role as managing organization to centrally and uniformly manage the campaign of preventing and combating cyber crime by assigning Ministry of Post and Telecommunication to directly take responsibility and coordinate with the National Defence Ministry, Public Security Ministry, Information, Culture and Tourism, Science and Technology as well as other ministries and local administration authorities concerned.

The management organizations of the campaign of preventing and combating cyber crime are comprised of:

1. Ministry of Post and Telecommunication;
2. Provincial [and] the Capital Departments of Post and Telecommunication;
3. District [and] Municipal Offices of Post and Telecommunication.

Article 49. Rights and Duties of the Ministry of Post and Telecommunication

In the management of the campaign of preventing and combating cyber crime, the Ministry of Post and Telecommunication has the following rights and duties:

1. Study, develop the strategy, policies, law on campaign of preventing and combating cyber crime to propose to the government for consideration;

2. Disseminate, popularize and educate laws and regulations relating to preventing and combating cyber crime throughout nationwide.

3. Take supervising role of managing, developing, training, upgrading the knowledge, capacity and expertise to the personnel and staff working on computer system security;

4. Take leading role of surveillance, tracking, monitoring, advice, notification and responding computer system emergency incident;

5. Coordinate with other ministries, relevant organizations on campaign of preventing and combating cyber crime;

6. Collaborate and cooperate with other countries, regional and international on campaign of preventing and combating cyber crime;

7. Summarize, consolidate of its activities on campaign of preventing and combating cyber crime, then report to the government;

8. Perform other rights and duties as defined in the laws and regulations.

Article 50. Rights and Duties of the Provincial [and] the Capital Departments of Post and Telecommunication

In the management of the campaign of preventing and combating cyber crime, the Provincial [and] the Capital Departments of Post and Telecommunication have the following rights and duties:

1. Disseminate, popularize and educate laws and regulations relating to preventing and combating cyber crime and bring them to implement effectively;

2. Develop plan managing, developing, training, upgrading the knowledge