

NEWSLETTER

Manuela António - 安文娜 大律師及公證員 | *Lawyers and Notaries*

3 JULY 2019

DATA PROTECTION

The Cybersecurity Law

Cybersecurity is a world-wide hot topic nowadays, and hence it is no surprise that progressively more and more countries are adopting relevant laws to regulate the matter.

As for the newly enacted Macau SAR's Cybersecurity Law, published in the Official Gazette this 24 June 2019, although not publicly assumed, it follows the trend imposed by its PRC's homonymous law, at least to a certain extent. The basic principles, duties and enforcement ideas are somewhat present. Nevertheless, the powers vested to the new regulatory supervising entities are still less comprehensive than those existing in PRC's.

As the Region's first comprehensive privacy and security body of rules over cyberspace, we are yet to fully discover the challenges that this new Law and its enforcement will pose, notably its articulation with the existing Personal Data Protection Law.

Nevertheless, despite being approved amidst some criticism and concerns regarding potential violations of basic freedoms, as it will only come into effect on 21 December 2019, there will hopefully be enough time to produce the set of regulations foreseen in the Cybersecurity Law and, most importantly, to quell the concerns with its implementation and enforcement.

At this stage it is however certain that, while bringing necessary regulation to prevent the failure of essential infrastructures for the security and the economy of the Macau SAR, the potential reach of the Cybersecurity Law and the duties imposed on operators of critical infrastructures mean that this new piece of legislation will present unprecedented challenges to local people as well as local and foreign businesses in Macau.

General Overview

The law is intended to determine and regulate the Macau SAR's cybersecurity system, aiming to protect the networks, systems and computer data of the operators of critical infrastructure.

It provides for three levels of supervision: the Commission for Cybersecurity (CPC) in a first level, the Cyber Security Incident Response and Response Center (CARIC) in an intermediate level, and the supervisory bodies, as the final level.

(...) it is however certain that, while bringing necessary regulation to prevent the failure of essential infrastructures for the security and the economy of the Macau SAR, the potential reach of the Cybersecurity Law and the duties imposed on operators of critical infrastructures mean that this new piece of legislation will present unprecedented challenges to local people as well as local and foreign businesses in Macau.

The CPC is the top political body, chaired by the Chief Executive of the Macau SAR, and will be responsible for defining the guidelines, objectives and strategies towards cybersecurity goals, as well as proposing and negotiating agreements and protocols that may be deemed necessary to guarantee the Region's cybersecurity, with both local or foreign public and private entities.

The CARIC, a specialized structure for the prevention and handling of any cybersecurity incidents, shall be coordinated by the Judiciary Police, and is responsible for monitoring the computer data transmitted between the operators of critical infrastructure networks and the internet, aiming to prevent, detect and fight cybersecurity incidents.

Finally, the supervisory bodies shall be responsible for overseeing private operators by areas of activity (v.g. the Monetary Authority will inspect banks, the Health Services will inspect private hospitals, etc.).

The composition, powers and mode of operation of all these entities will be defined by the Chief Executive in complementary regulation, thus meaning that the real range of this Law (and the competence of the new entities related thereto) shall only be fully comprehended when those regulatory pieces of legislation are enacted.

Critical Infrastructures operators

The Cybersecurity Law is applicable to both public and private operators of critical infrastructures using computer networks or systems. The former generally include the Chief Executive's Office and other holders of political and judicial offices, the Region's public services and agencies. In turn, the latter include all private entities, with or without registered address in Macau, that are allowed to conduct business in Macau in certain key areas which include, amongst others, banking, insurance and finance activity, healthcare services, gaming concessionaires, media (that are not exclusively aimed at broadcasting entertainment contents) and telecommunications.

Duties

Amongst the vast group of duties that the Cybersecurity Law imposes (organic duties, procedural, preventive and reactive duties, self-evaluation and report duties and collaboration duties), the most noteworthy are:

1. allowing the representatives of CARIC or of the supervisory bodies to access their networks (without any prior judicial decision approving the said access);
2. appoint a person in charge of cybersecurity, and its substitute, who shall be in constant contact with the regulatory supervising entities (being subject to a prior probity check);
3. approve an internal cybersecurity plan and procedural guide aimed at the prevention, monitoring, report and reply to cybersecurity incidents;
4. regularly check the security and the existing risks to its networks and systems;
5. submitting an yearly cybersecurity report listing, inter alia, the cybersecurity incidents and the measures adopted to prevent new incidents;
6. network operators must register the identification of the pre-paid SIM card users acquired before of the enactment of the law (or otherwise suspend service to such SIM cards);

The CPC (...) will be responsible for defining the guidelines, objectives and strategies towards cybersecurity goals, as well as proposing and negotiating agreements and protocols (...)

The CARIC (...) is responsible for monitoring the computer data transmitted between the operators of critical infrastructure networks and the internet (...)

The supervisory bodies shall be responsible for overseeing private operators by areas of activity (...)

7. network operations must verify and register the identity of the clients upon the execution of agreements, confirmation of provision of internet access services, registration of domain names or public services of land or mobile telecommunications;
8. the internet services providers must keep, for a year, the network address translation records from private networks addresses into public network addresses.

Needless to say that the aforementioned duties will definitively bring implementation and maintenance costs to each of the entities covered by this new Law although, again, the full extent of such costs is still to be assessed, pending further regulation of the Cybersecurity Law.

Penalties for infractions

As for penalties, those in breach of the Cybersecurity Law may be fined up to **MOP5 Million**.

Other ancillary penalties may also be imposed on those in breach such as the loss of the right to supply products to the Government or to receive Government subsidies for a period of up to 2 years.

In addition, individuals in breach of preventive, reactive or procedural duties may see their employment suspended or terminated or sent to compulsory retirement.

Concerns raised with the implementation of the Cybersecurity Law

The major concern lies on the authority granted to CARIC, which is coordinated by the Judiciary Police, to conduct real-time monitoring of the computer data transmitted between the operators of critical infrastructure networks and the internet.

Considering that the operators of telecommunications infrastructures are subject to the Cybersecurity Law, this provision has raised fears of opening the door to real time monitoring of virtually every person and entity in the Macau SAR.

In addition, the Cybersecurity Law does not seem to implement any mechanism of oversight of CARIC's actions, e.g. when monitoring data and accessing critical infrastructure operators' premises and networks, which again poses the concern of unsupervised police action in extremely sensitive areas of the Macau SAR's economy as well as unwarranted interference in the citizens' privacy and personal data.

Without a streamlined oversight mechanism, citizens and companies will have to rely on existing channels (e.g. the Data Protection Office, the Commission Against Corruption, the Public Prosecutors Office and the Courts), which also entails an additional level of uncertainty and, eventually, a long period of time before a final decision over a claim is obtained.

Finally, the requirement that the identification of all SIM card owners is registered, has also attracted criticism towards the abuses that such provision may lead to.

Considering that the operators of telecommunications infrastructures are subject to the Cybersecurity Law, this provision has raised fears of opening the door to real time monitoring of virtually every person and entity in the Macau SAR.

In any case, the Government has continuously maintained that it will only analyze the flow of computer data, meaning that, according to the Government, data will not be decoded nor freedom of expression and/or economic freedom and/or intellectual property rights will be affected.

In summary, in a world where cyber risks are a constant threat, there is definitively the need to implement a cybersecurity legal framework and to impose special duties of care to certain industries. However, only time will tell whether the Cybersecurity Law will serve its legitimate purposes or whether it will lead to abuse.

(...) only time will tell whether the Cybersecurity Law will serve its legitimate purposes or whether it will lead to abuse.

NEWSLETTER

Manuela António - 安文娜 大律師及公證員 | *Lawyers and Notaries*

The distribution of this communication is limited and the information herein expressed is for general purposes only, not substituting legal advice on specific issues.

Contacts

Dr. Carlos D'Assumpção, n.ºs 411-417, Edifício Dynasty Plaza, 15.º andar D-H, Macau, China

T.: +853 28 591 592 / 128
F.: +853 28 345 678
info@mantonio.net
www.mantonio.net