ROYAUME DU MAROC
ADMINISTRATION DE LA DEFENSE NATIONALE

المملكة المغربية
إدارة الدفاع الوطني

PRESENTATION NOTE OF LAW N ° 05-20 ON CYBERSECURITY

The rapid increase in the spectrum of cyberthreats in parallel with the evolution of uses, services and digital infrastructures has made necessary the reassessment of the legal bases so that they can be in line with the reality and adapted accordingly.
To this end, law 05.20 which objectives and main provisions are presented below, was adopted by the Council of Ministers on July 6th, 2020 and subsequently, unanimously, by the two Chambers of Parliament respectively on the 14th and 17th of July 2020.

1. AN INTERNATIONAL CONTEXT MARKED BY INTENSIFICATION OF CYBERSECURITY LEGISLATION

In recent years, cybersecurity legislation has intensified at the international level. Regulatory compliance is now emerging as a major issue for public and private entities. In this regard, it should be noted that the United Nations has recognized the principle of the applicability of international law to cyberspace.

In addition, several countries have had to take legislative and regulatory measures in the area of cybersecurity to secure their information systems, succeed in their digital transition and protect themselves in particular against the risks of cybercrime, sabotage, theft and misuse of personal and sensitive data.

In this context, the United States of America drew up a directive in 2015 which specifically creates a legal framework enacting rules for protection against cyberthreats.
In 2013, France required from critical infrastructure, through the law on military programming, to strengthen the security of their critical information systems. This law also requires telecom operators to actively participate in the detection of computer attacks targeting their subscribers and sanctions are planned against organizations that fail to meet their obligations.
Finally, the European Union recently implemented two directives governing information security and data protection, which have become enforceable for member states.

2. CYBERSECURITY IN MOROCCO: A PROGRESSIVELY COMMITTED PROCESS SINCE 2011

Under the Enlightened Guidance of His Majesty the King, may God assist him, Morocco has been involved since 2011 on the path of strengthening its national cyber capacities and the consolidation of digital trust.

In line with the actions that have been undertaken, in 2012 the Kingdom adopted a National Cybersecurity Strategy and a National Information Systems Security Directive applicable since 2014 to administrations and public entities.
To accelerate the ramp-up of this disposal, the National Defense Administration (NDA) also issued in 2016 a decree setting out the measures to protect the sensitive information systems (SIS) of critical infrastructure.

This text was completed by an order from the Head of Government in 2018 setting the criteria for the approval of SIS audit service providers for critical infrastructure and the procedures for carrying out the audit.

Given the challenges our country is facing in the field of cybersecurity, it is becoming more necessary than ever to have a complete legal framework that would build on the actions already launched. This framework would make it possible to strengthen the security of State and critical infrastructure information systems and would recommend awareness-raising actions for the benefit of private sector operators and individuals. By capitalizing on this international context of strengthening legislation on cybersecurity and on the national legal structure in the field, NDA, following the Royal High Assent, developed this law on cybersecurity.

3. A LAW TO REINFORCE DIGITAL CONFIDENCE AND SECURITY

- **A law to strengthen the protection and resilience of information systems**

The objective of this law is to establish the means of protection in order to develop digital confidence, to promote the digitization of the economy and more generally to ensure the continuity of economic and societal activities in our country.

For this purpose, the law aims to respond to one of the objectives of the National Cybersecurity Strategy which is to strengthen the protection and the resilience of the information systems of critical infrastructure (CI) and entities (Entity: state administrations, territorial communities, institutions, state-owned companies and any other state legal person governed by public law). Therefore, the law set out security measures intended to increase national capacities in the field of cybersecurity, to contribute to securing the digital transition of the Kingdom and to coordinate action to prevent and protect against attacks and cybersecurity incidents.

The cybersecurity law set up a legal framework recommending to entities a minimum set of rules and security measures in order to ensure the reliability and resilience of their networks and information systems. These rules would include, in particular, the implementation of technical and organizational measures to manage cyber risks and avoid incidents that could harm the information systems of the entities.

Furthermore, this law obliges entities to report, to the National Cybersecurity Authority, security incidents of which they are victims in order to help to prevent and resolve these vulnerabilities.

It recommends also that each entity designate a chief information security officer and prepare a continuity and recovery plans to neutralize business interruptions, to protect business processes from the effects caused by the main vulnerabilities of information systems and to ensure a rapid resumption of these processes.

Finally, in addition to the security measures to which the entities are subject, the law includes additional and specific provisions for CI who has sensitive information systems, for example the certification of their sensitive information systems, the submission of this systems to security audits by authorized agents of the National Authority or by audit service providers qualified by said Authority.

- **A law which widens the perimeter of protection by integrating other categories of actors**

The cybersecurity law recommends measures to protect networks and information systems for other categories of actors such as public telecommunications network operators, Internet service providers, cybersecurity service providers, digital service providers and internet platform editors.

These actors are strategic stakeholders for strengthening the security of the of entities and CI information systems. The law recommends, in fact, the conservation of technical data useful for the identification of cybersecurity incidents, the reporting of any incident likely to affect the security of their customers' information systems and the taking of protective measures. necessary to prevent and neutralize threats or attacks targeting them.

With regard to cyber risks, the law attaches a primordial importance to prevention and awareness of cybersecurity issues. Cybersecurity hygiene advice and recommendations will be regularly communicated by the National Authority for the benefit of entities, CI, private sector operators and individuals.

- **A law to better fight against cyber-malicious acts, to help strengthen digitization and the protection of personal and sensitive data**

The fight against cyber-malicious acts is based in part on the quality of the exchange of information and data between the competent services of the State. To this end, the law 05.20 sets a framework for collaboration and information exchange between the National Cyber Security Authority and the competent State services responsible for handling offenses against automated data processing systems.

The law also establishes the assistance that the National Authority must provide to the competent national authorities for the strengthening of digital trust, the development of the digitization of State services and the protection of personal data.

Taking into account the transnational dimension of computer attacks and cybersecurity risks, the law also grants a major interest in the development of cooperation with foreign organizations. This cooperation will promote the sharing of experience and expertise in this field and thus increase the capacity to respond to cyber attacks.

- **A law that endows the Strategic Committee and the National Authority with the powers and means to assume responsibility for the protection of information systems**

The law attaches capital importance to the governance of cybersecurity by setting out the missions assigned to the Cybersecurity Strategy Committee, the National Cybersecurity Authority and the management of major cybernetic crises and events Committee. In addition, the law stipulate that the audits can be carried out to ensure the implementation of security and protection rules for information systems.

- **A law that will promote the development of a national cybersecurity ecosystem**

Beyond the direct impact on the functioning of the economy and society, the law promotes the development of a national cybersecurity ecosystem. It gives impetus to the development of services in terms of consulting, auditing, detection and treatment of cybersecurity incidents and products for securing networks and information systems. Therefore, it is the entire cybersecurity sector that benefit from the implementation of this law.

Finally, penalties are established by the law in case of failure to comply with certain obligations. These offenses mainly concern the failure to report incidents affecting information systems, the hosting of sensitive data outside the national territory, the impediment of information systems security audit missions and the failure to apply security provisions and measures issued by the National Cyber Security Authority.