The new Law Decree on National Cybersecurity

1. Introduction

On 21 September 2019, Law Decree No.105/2019, published in Official Journal No. 222 of 21.9.2019 (the "**Cybersecurity Law Decree**")[1], was adopted by the Government. The aim of the Cybersecurity Law Decree is to establish the national cybernetic security perimeter and to introduce suitable measures to guarantee safety standards for networks and information systems as well as IT services for public administrations, private and public national entities and operators, which perform essential functions of the State or provide essential services in the civil, social and economic fields and whose malfunction may cause a national security risk.

In order to adopt the appropriate measures to protect networks and information systems and broadband communication services based on 5G technology, as well as to coordinate the implementation of Regulation (EU) No. 2019/452, the Cybersecurity Law Decree also amends the regulatory framework for the exercise of the special powers by the Government referred to in Decree Law of 15 March 2012, n. 21 ("**Golden Power Decree**").

2. Main provisions of the Cybersecurity Law Decree

i. Scope of the national security perimeter

In order to identify the national security perimeter, Article 1 of the Cybersecurity Law Decree establishes that such provisions shall be implemented by means of (i) certain decrees of the Prime Minister ("DPCM") - to be updated every two years in relation to technological developments – which should be adopted on the basis of the proposal of the Interministerial Committee for the Security of the Republic (*Comitato interministeriale per la sicurezza della Repubblica*) ("CISR"), and (ii) a Presidential Decree. In particular, the implementation of the new rules is delegated to:

- a DPCM, to be adopted within four months from the date of entry into force of the law converting the Cybersecurity Law Decree, identifying (i) the public and private **entities** falling within the national security perimeter, and (ii) the **criteria** for the formation of the **lists of** the respective **networks, information systems and relevant services** to be updated annually. These criteria are elaborated by the CISR and the lists shall be sent by the public and private entities to the Presidency of the Council of Ministers and to the Ministry of Economic Development respectively (which perform verification activities), for onward transmission to the Department of Information for the security and to the Ministry of the Interior;
- a DPCM, to be adopted within ten months from the date of entry into force of the law converting the Cybersecurity Law Decree, defining the **procedures for the notification of incidents** having an impact on networks, information systems and IT services (which shall be sent to the Computer Security Response Team in case of incidents), and the relevant **measures** aimed at achieving a high level of cybersecurity, concerning *inter alia,* the prevention and mitigation of incidents, the operational management, etc.;

[1] The Cybersecurity Law Decree is already in full force and effect but it shall be converted into law by the Parliament within 60 days of its publication (otherwise the Decree will be retroactively ineffective).

- a Presidential Decree, to be adopted within ten months from the date of entry into force of the law converting the Cybersecurity Law Decree, determining a safer mechanism, to be followed by entities falling within the perimeter and concerning the **procurement for the supply of goods, ICT systems and services** to be used in networks, information systems and IT services. In particular, the National Evaluation and Certification Center (CVCN), on the basis of a specific risks assessment, can impose conditions and hardware/software tests which, by means of suspension or termination clauses, are integrated into the call for tenders or the related contract. Suppliers of goods, systems and IT services shall provide the necessary cooperation with the CVCN to carry out the required tests and shall support the costs incurred.

Article 1 also establishes a system of fines in the event of failure to comply with the obligations set out in the Cybersecurity Law Decree and it also introduces a criminal penalty, punished with imprisonment from one to five years, for anyone who provides (or fails to provide) information, data or facts which do not correspond to the true, and which are relevant, *inter alia*, for the preparation or the update of the abovementioned lists. At the same time, pursuant to the Legislative Decree n. 231/2001, a pecuniary sanction of up to four hundred shares, is applied to the related entity.

In addition, Article 1 defines the CVCN's specific tasks and responsibilities and Article 2 contains the discipline for the recruitment of professionally qualified personnel for the functioning of the CVCN, the Presidency of the Council of Ministers and the Ministry of Economic Development.

ii. Special powers concerning broadband communication with 5G technology and critical infrastructures and technologies (Golden Power rules and others special powers)

Article 3 of the Cybersecurity Decree provides that the **special powers** referred to in Article 1*bis* of the Golden Power Decree, in the sector of electronic broadband communication with 5G technology, **are exercised** after the **assessment**, by the aforementioned CVCN, in the presence of **risk factors**, capable of compromising the integrity and security of networks and data.

In addition, Article 4 of the Cybersecurity Decree integrates the discipline of special powers in critical infrastructures and technologies sectors, referred to in Article 2, paragraph 1*ter*, of the Golden Power Decree, specifying that the assessment of the existence of a threat to safety and public order also concerns the jeopardizing of the safety of networks and facilities and on the continuity of supplies and it also coordinates such provisions with the implementation of the Regulation (EU) No. 2019/452, establishing a framework for the screening of foreign direct investments, by extending its scope to **further critical infrastructures and technologies**, such as transport, water, health, media and communications.

In addition, Article 4, second paragraph, also specifies that, until the date of the entry into force of the regulation to be adopted pursuant to Article 2, paragraph 1*ter*, of the Golden Power Decree, the purchase for any reason from a foreign investor (i.e. non-European investor) of a controlling interest in Italian companies holding assets in critical infrastructure and technologies sectors as defined in Regulation (EU) No. 2019/452, which may determine lasting and permanent links between the foreign investor and the target company on the basis of the definition of control pursuant to article 2359 of the Italian Civil Code, is subject to the **obligation to notify to the special committee among the Presidency of the Council of Ministers** referred to in paragraph 5, of the Golden Power Decree.

Finally, the Cybersecurity Law Decree provides that the President of the Council of Ministers may require the disabling or the elimination, partially or totally, of one or more devices or products used in networks and informatics systems or for the performance of the relevant services, in the presence of a serious and imminent risk to national security linked to the vulnerability of networks, systems and services, and in case of cybernetic crises as defined by law (based on a resolution of the CISR), if not otherwise avoidable and for the time strictly necessary to eliminate or to mitigate the specific risk (according to a proportionality criteria).

Please note that the above is simply an overview of the subject matter and it is not, nor is it intended to be, a legal opinion or legal advice. Should you have any questions concerning the new law's requirements set out above or should you wish to receive information on our annual package, please do not hesitate to contact us.

Francesco Gianni
Founding Partner

Roma
+39 06 478751
fgianni@gop.it

Valentina Canalini
Counsel

Roma
+39 06 478751
vcanalini@gop.it

Sofia Gentiloni Silveri
Associate

Roma
+39 06 478751
sgentilonisilveri@gop.it