Legal Briefing

February 2021

LATEST DEVELOPMENTS IN THE AREA OF NETWORK AND INFORMATION SYSTEMS SECURITY

In this legal briefing, we provide analysis in respect of Royal Decree 43/2021 of 26 January, which implements Royal Decree-law 12/2018 of 7 September, concerning the security of networks and information systems ("**RD 43/2021**"), which regulates the security of networks and information systems used for the provision of essential services and digital services. RD 43/2021 was published in the Official State Bulletin on 28 January and came into effect on 29 January.

To date, this area had been regulated by (i) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (the "**NIS Directive**" as its acronym is known in English); and (ii) Royal Decree-law 12/2018, of 7 September, concerning the security of networks and information systems, which was responsible for the transposition into Spanish law of the aforementioned NIS Directive ("**RDL 12/2018**").

In addition, RD 43/2021 and RDL 12/2018 are implemented as supplements to Law 8/2011, of 28 April, which establishes measures for the protection of critical infrastructure ("**Law 8/2011**").

1. The objective of the regulatory implementation of RD43/2021

RDL 12/2018 established a general framework for the security of networks and information systems used by providers of essential services[1] and digital services such as online marketplaces[2], online search engines[3] and cloud computing services[4]. It created new tools

[1] According to Article 2 of Law 8/2011, essential services are those necessary for the maintenance of basic social functions, health, safety, social and economic welfare of citizens, or the effective functioning of State Institutions and Public Administrations, the operation of which rely on information networks and systems.
[2] An online marketplace according to Article 2 of Law 8/2011 is a digital service that allows consumers and sellers, as defined respectively in Articles 3 and 4 of the revised text of the General Law for the Protection of Consumers and Users and additional related laws, approved by Royal Legislative Decree 1/2007, of 16 November 2007, to enter into contracts of sale or provision of online services with sellers, either on a specific website of the online marketplace service or on a website of a seller using computer services provided for this purpose by the provider of the online marketplace service.
[3] An online search engine within the meaning of Article 2 of Law 8/2011 is a digital service that allows users to search for, in principle, all websites or websites in a particular language, by means of a query on a topic in the form of a keyword, phrase or other entry, and which, in response, displays links where information related to the requested content can be found.
[4] According to Article 2 of Law 8/2011, a cloud computing service is a digital service that enables access to a modular and flexible set of computing resources that can be shared.

aimed at increasing the protection against threats that may affect networks and information systems, creating a strategic and institutional framework for the security of networks and information systems, and enhancing cooperation between public authorities. It also established a series of security obligations for operators and regulated the reporting of incidents, placing special emphasis on those with a cross-border impact.

RD 43/2021 aims to build upon RDL 12/2018 in relation to:

(i) the strategic and institutional framework for the security of networks and information systems;

(ii) compliance with the security obligations of operators of essential services and digital service providers; and

(iii) the management of security incidents, expanding on the reporting obligations of operators of essential services in relation to (i) incidents that could have disruptive effects on such services; and (ii) incidents that could affect the networks and information systems that are used for the provision of essential services.

RD 43/2021 has the same scope of application as RDL 12/2018. Accordingly, said regulations apply to:

(i) the provision of essential services that rely on the networks and information systems of strategic sectors, and government departments and public bodies of the competent system[5]; and

(ii) digital services relating to online marketplaces, online search engines and cloud computing services.

From a geographic point of view, RDL 43/2021 applies to operators of essential services that are established in Spain, as well as to digital service providers that have their headquarters in Spain and have their main place of business in the European Union, and to those that, without being established in the European Union, have chosen Spain as their designated representative in the European Union for the purpose of compliance with the NIS Directive.

2. Key features of RD 43/2021

RD 43/2021 expands (to those already regulated by RDL 12/2018) the power of the competent authorities to supervise operators of essential services that are not considered critical

[5] The essential services that rely on the information networks and systems included in the strategic sectors are defined in the annexe to Law 8/2011.

operators, i.e. organisations that are not responsible for the investment in or daily operation of a facility, network, system, or hardware or IT asset designated as critical infrastructure[6].

By way of example, some of the competent authorities will be the following, depending on the sector to which they belong:

(i) Transport: the Ministry of Transport, Mobility and Urban Agenda, through the Secretary of State for Transport, Mobility and Urban Agenda.

(ii) Information and Telecommunications Technologies: the Ministry of Economic Affairs and Digital Transformation, through the Secretary of State for Digitalisation and Artificial Intelligence and the Secretariat of State for Telecommunications and Digital Infrastructure.

(iii) The chemical industry: the Ministry of the Interior, through the Secretary of State for Security.

(iv) Health: the Ministry of Health, through the Secretary of State for Health.

In addition, in Article 4, RD 43/2021 reaffirms the cooperation and coordination between the different computer security incident response teams ("**CSIRT**" *Computer Security Incident Response Team*), and structures the cooperation between the CSIRTs and the competent authorities, through the National Platform for Notification and Monitoring of Cyber Incidents.

Article 5 of RD43/2021 addresses the role of the single point of contact, which ensures cross-border cooperation by the competent authorities with (i) the competent authorities of other Member States of the European Union; (ii) the cooperation group formed by representatives of the Member States, the European Commission and the National Innovation Company; and (iii) the CSIRT network.

A. Security requirements

RD 43/2021 includes the obligation of operators of essential services and digital service providers to adopt the technical and organisational measures that are appropriate and proportionate for the management of risks affecting the security of the networks and information systems used to provide their services.

[6] According to the definitions in Article 2 of Law 8/2011, critical infrastructure is considered to be that which is of a strategic nature and whose operation is indispensable and does not allow alternative solutions, so that its destruction would have a serious impact on essential services.

The security policies for networks and information systems approved by operators of essential services must adhere to the principles of comprehensive security, risk management, prevention, response and recovery, lines of defence, periodic reassessment and segregation of duties. In addition, the measures adopted must be formally established in the Declaration of Applicability of security measures, which must be signed by the operator's information security officer. RD 43/2021 strengthens the role of the information security officer, which may be held by a person or a collective body, although in the latter case a personal representative must be appointed, whose appointment must be communicated to the competent authority within three months of his or her appointment.

Said security officer shall have direct contact with the operator's senior management, shall act as a point of contact and technical coordination with the competent authority and CSIRT (Article 7 of RD 43/2021) and shall have the following main functions:

(i) Prepare, propose for approval by the organisation and supervise the security policies, which shall include appropriate and proportionate technical and organisational measures to manage the risks posed to the security of the networks and information systems used, and to prevent and minimise the effects of cyber incidents affecting the organisation and services, in accordance with the provisions of Article 6.

(ii) Prepare the **Declaration of Applicability**, which contains the security measures provided in Article 6.3, paragraph 2 of RD 43/2021.

(iii) Receive, interpret and supervise the application of the instructions and guidelines issued by the competent authority, both for normal operations and for the correction of any deficiencies observed.

B. Management of security incidents

Article 8 of RD 43/2021 also provides that operators of essential services and digital service providers are responsible for managing and resolving security incidents affecting the networks and information systems used to provide the service.

In addition, Article 9 establishes the obligations regarding the reporting of incidents that (i) may have significant disruptive effects on essential services by operators of essential services; or that (ii) may affect the networks and information systems used for the provision of essential services. The operators of essential services must notify the competent authority, through CSIRT.

Accordingly, incidents will be associated with different levels of danger and impact, with the obligation to report all those categorised as critical, very high or high. The incident reporting procedure will be carried out through the National Platform for Notification and Monitoring of Cyber Incidents.

C. Supervision

In terms of supervision and control, the regulation establishes that the competent authorities will supervise compliance with the security and incident reporting obligations to which operators of essential services and digital service providers are subject, including the obligation of the latter to cooperate with the competent authority in such supervision. Furthermore, RD 43/2021 also establishes the scope for the competent authorities to carry out inspection tasks.

For more information,
please contact:

Andy Ramos Gil de la Haza
Intellectual Property and Technology Counsel
aramos@perezllorca.com
T: + 34 91 423 20 72