EXTENDED SUMMARY

The right to the protection of personal data has evolved over time, gaining increased relevance in parallel with technological advancements. As data has become the central element of emerging technologies and newly designed services, this right has acquired a more critical function. Accordingly, developments that were previously unforeseen have now become necessary within the field of data protection, shaped by the rise of technology and data-driven services. The right to data portability constitutes one of these novel mechanisms.

Although the right to data portability was first codified in Article 20 of the GDPR, the number portability regulated under Article 30 of Directive 2002/22/EC can be regarded as the practical precursor of this right. Data portability refers to the transfer of data from one system to another without requiring the data subject to re-enter such data. Within this framework, the data subject is entitled to (i) receive their personal data in a structured, commonly used, and machine-readable format, (ii) transfer the personal data obtained from a controller to another controller, and (iii) request, where technically feasible, the direct transfer of personal data from one controller to another. However, the right to data portability is not an unlimited right, and the relevant provision also contains restrictive clauses.

The second part of this study addresses the ambiguities surrounding Article 20 of the GDPR on data portability. In this context, the concepts of 'data provided,' 'structured, commonly used and machine-readable format,' and 'technical feasibility' are characterized as unclear. It is argued that the notion of data provided should encompass not only the data actively submitted by the data subject to the controller (collected data), but also the data obtained through sensors (observed data). With regard to the concepts of structured, commonly used, and machine-readable formats, it is emphasized that, without delving into their technical dimension, such vague terminology may hinder the practical implementation of the right to data portability and its full realization. Accordingly, it is suggested that a standard should be established while maintaining technological neutrality. As for the concept of technical feasibility, the lack of clarity is highlighted as a potential source of abuse by data controllers to reject portability requests. Moreover, it is noted that technical feasibility may

vary depending on the specific case: while a data transfer request may be technically feasible for one controller, it may not be so for another.

In the third part of our study, an attempt is made to identify the value that the right to data portability, as regulated under Article 20 of the GDPR, seeks to protect. In this context, Article 21/1-c of the E-Commerce Regulation, which constitutes another data portability provision, is explained, and the potential legal issues that may arise from its application are discussed. Finally, Article 21/1-c of the E-Commerce Regulation is compared with GDPR Article 20, and the differences between these two provisions are set out. Within this framework, it is argued that Article 21/1-c of the E-Commerce Regulation is constructed from a competition law perspective, whereas the right to data portability under GDPR Article 20 aims to safeguard the protection of personal data.