ANALYSIS

E-commerce

Derogations from the principle of supervision in the home Member State in respect of information society services and control over content by means of an algorithm

(Judgment of the Court (Grand Chamber) of 16 June 2016 in Joined Cases C-188/24 and C-190/24)

The Judgment of the Court (Grand Chamber) of 16 June 2026 (Joined Cases C-188/24 and C-190/24) addresses two central issues of the legal regime governing information society services: the scope of derogations from the principle of supervision in the home Member State on grounds of public policy, security and safety, and the liability of digital platforms when exercising control over content by means of an algorithm.

ÁNGEL GARCÍA VIDAL
Professor of Corporate & Commercial Law,
University of Santiago de Compostela
Academic counsel, Gómez-Acebo & Pombo

July 2026

1. Principles of supervision in the home Member State and mutual recognition as regards information society services and public policy-based derogations

1.1. *The regulatory framework*

Directive 2000/31/EC is based on the principle of supervision in the home Member State as regards information society services. In accordance with this principle (set out in Art. 3 of the directive), the legality of these services must be supervised at source, in the Member State that is the country of origin of the activity, and the other Member States of the European Union must prevent the free provision within their territory of information society services from other Member States. However, these principles of supervision in the home Member State and mutual recognition operate within the so-called *"coordinated field*," that is, in relation to legislative provisions concerning the requirements that the provider must meet in respect of the taking up of the activity of an information society service — such as requirements concerning qualifications, authorisations or notifications — and in respect of the pursuit of that activity — such as requirements concerning the behaviour of the service provider, the quality or content of the service, or the liability of the service provider —.

However, as a derogation, these principles do not apply to certain fields listed in the annex to the directive: copyright, neighbouring rights, and industrial property rights; the emission of electronic money; undertakings for collective investment; insurance activities; the freedom of the parties to choose the law applicable to their contract; contractual obligations concerning consumer contracts; formal validity of contracts creating or transferring rights in real estate; and the permissibility of unsolicited commercial communications by electronic mail.

Similarly, Member States may adopt measures that constitute a derogation from these principles with respect to a specific information society service if the measures are necessary for reasons of public policy (in particular, the prevention, investigation, detection and prosecution of criminal offences, including the protection of minors and the fight against incitement to hatred on grounds of race, sex, religion, or nationality, as well as violations of the human dignity concerning individual persons), the protection of public health, the protection of consumers, or public security, including the safeguarding of national security and defence. Furthermore, such measures — which must be taken against a given information society service that prejudices or presents a serious and grave risk of prejudice to those objectives — must be proportionate to those objectives, and, before taking them, the Member State must have asked the State of origin to take measures, and the latter must either have failed to do so or the measures taken must have proved inadequate; it must also have notified the Commission and the State of origin of its intention to take such measures.

1.2. *The Court's judgment of 16 June 2026: the importance of distinguishing between general legislation and its specific application*

On this legislative basis, in the aforementioned judgment of 16 June 2026, the Court analysed whether two pieces of French legislation applicable to digital services providers established in other Member States comply with the Directive on electronic commerce and the aforementioned principles of supervision in the home Member State and mutual recognition. It concerned, firstly, the legislation establishing the obligation for pornographic websites to put in place effective age-verification systems to prevent access by minors, and, secondly, the legislation establishing for a given period of time a prohibition on the rebroadcasting of information concerning certain roadside checks through driver-assistance applications. Specifically, and for reasons of public policy, security and safety, provision is made for the implementation of a mechanism that enables the competent administrative authority to prohibit operators of services of the latter kind, for a limited period and within a limited geographical area, from rebroadcasting messages from their users likely to reveal the location of alcohol and drug testing, as well as certain police operations, for example against persons wanted for serious crimes or offences (including acts of terrorism) or because they have escaped from a psychiatric institution.

The Court first examines whether the aforementioned pieces of legislation fall within the aforementioned *coordinated scope* of the directive, which is where, as a general rule, the principles of supervision in the home Member State and mutual recognition apply. The Court concludes that criminal provisions intended to ensure the protection of minors and measures requiring the establishment of technical mechanisms for blocking access by minors to pornographic content fall within the 'coordinated field' and constitute a 'requirement' relating to the pursuit of the activity of an information society service, within the meaning of Directive 2000/31.

In this regard, the Court establishes several relevant guidelines, among which the following stand out:

1) the coordinated field is not limited to matters expressly regulated and harmonized in the Directive on electronic commerce;

2) the general and abstract nature of legislation cannot have the effect of excluding that legislation from the coordinated field;

3) national legislation (whether or not it forms part of criminal law) pursuing objectives of public policy, security and safety is not excluded, for that reason alone, from the scope of coordination. In fact, only legislation adopted in the fields of taxation, data protection, cartels, the notary profession, legal representation before the courts and gambling is specifically excluded from the scope of that directive by Article 1(5) thereof. Consequently, the

> Court concludes that, in so far as it does not relate to the fields excluded by that provision, legislation coming under criminal law or pursuing objectives of public policy, security and safety may fall within the scope of that directive and thus within the coordinated field.

However, even if such national legislation falls within the coordinated scope of the directive, it is possible, as has already been noted, for Member States to take measures in respect of a given information society service that derogate from the principles of supervision in the home Member State and mutual recognition when such measures are necessary in the interests of public policy, the protection of public health, public security or the protection of consumers; are adopted in respect of an information society service that actually undermines those objectives or poses a serious and grave risk of undermining them; and are proportionate to those objectives.

According to the Court of Justice, the objectives pursued by the first regulation at issue fall within the concept of *public policy*, since this concept covers, in particular, the protection of minors and the fight against violations of human dignity, as well as the prevention, investigation, detection and prosecution of criminal offenses. Similarly, reasons of public policy, security and safety are capable of justifying prohibitions on the rebroadcasting of information relating to roadside checks, such as those provided for in that legislation.

The nuance pointed out by the Court is highly relevant here, as it emphasises that these rules are not automatically excluded from the principle of supervision in the home Member State merely because they are criminal or public safety rules. According to the Court, the directive precludes a Member State from directly imposing on all service providers established in another Member State a general obligation to prevent minors from accessing pornographic content, as well as a general prohibition on rebroadcasting information relating to certain roadside checks. On the contrary, what is possible is for a Member State, in application of such general legislation, to adopt measures — individual and specific — against a service provider established in another Member State. On that basis, the Court notes that the aforementioned French pieces of legislation, in addition to the corresponding general prohibitions, provide that the administrative authority will issue an individualised order to each operator to comply with the legislation.

Therefore, although the general provisions do not, the formal individual notices to public communication service providers broadcasting pornographic content or decisions prohibiting the operators of a given service from rebroadcasting certain information, may constitute measures taken against a given information society service, within the meaning of Article 3(4)(a) of Directive 2000/31, thereby allowing the host country to derogate from the principle of supervision in the home Member State, provided that the requirements of proportionality and the procedural safeguards established by Union law are respected.

2. Control over information stored by means of an algorithm and loss of exemption from liability of hosting providers

Another issue analysed by the Court is whether the French legislation that prevents operators of electronic driving assistance or geolocation navigation services from rebroadcasting information relating to certain roadside checks effectively imposes on them a general obligation to monitor the information they transmit; such a general monitoring obligation is prohibited by Article 15 of the directive (an article now repealed by Regulation (EU) 2022/2065 on a Single Market for Digital Services, which establishes this prohibition in Article 8).

> *Individual measures may justify derogations from the principle of supervision in the home Member State*

First, the Court recalls its previous case law (Judgment of 3 October 2019, *Glawischnig-Piesczek*, C-18/18), according to which the prohibition imposed on Member States from imposing a general monitoring obligation on providers of intermediary services does not concern monitoring obligations "in a specific case" and, in particular, does not preclude decisions of national authorities taken in accordance with national law concerning such a case. Such an order does not require the hosting provider to carry out an independent assessment of the stored content, since it may confine itself to identifying the content covered by the order by means of automated search tools.

Under these circumstances, the prohibition on general monitoring applies to intermediary service providers, and a preliminary question would be whether the provider of the driver assistance service qualifies as such. The Court leaves the determination of this issue to the national court. However, in any case, it makes a very relevant observation regarding whether the exemption from liability of hosting intermediaries — originally set out in Article 14 of the directive (and currently in Article 6 of the Digital Services Regulation) — applies. Under this exemption, where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

According to the Court, those two conditions requiring knowledge and control should be understood as being alternative to and independent of each other. Therefore, the operator of an information society service which controls the stored information is excluded from the benefit of Article 14(1) of that directive, even if it does not become aware of that information due to the automation of the information processing.

In this regard, it is particularly significant that in the judgment under discussion, the Court states that control may be exercised by means of an algorithm, affirming that it is precisely by means of the algorithm used that such an operator exercises control over the information stored. Consequently, so long as it has predetermined, by means of that algorithm, the conditions under which such information may or may not be broadcast, it is irrelevant that that operator does not itself carry out additional interventions which have the effect of promoting, modifying or deleting information stored with a view to it being broadcast.

Therefore, if, beyond the mere categorisation and indexation of information for the purpose of improving its accessibility, the algorithm used determines, in the interest of the operator or its service, under what conditions, how and in which order of priority that information is or is not broadcast, that operator exercises control over that information, with the result that the service it offers cannot be classified as an 'information society service … that consists of the storage of information provided by a recipient of the service', and thus the exemption from liability would not apply to it.