COURT OF JUSTICE
OF THE EUROPEAN UNION

EN

Fact sheet

Electronic commerce and contractual obligations

Research and Documentation Directorate

curia.europa.eu

Foreword

The rules on electronic commerce lie at the heart of Directive 2000/31/EC [1] on certain legal aspects of information society services, in particular electronic commerce, in the internal market, which lays down provisions on the establishment and information requirements applicable to information society service providers and on the liability of intermediary service providers.

However, electronic commerce affects a variety of areas of economic life falling outside the ambit of that directive, such as games of chance, questions relating to agreements or practices governed by cartel law and taxation (see Article 1(5) of the Directive on electronic commerce concerning the directive's objective and scope). Similarly, copyright and related rights, trade mark rights, consumer protection and the protection of personal data fall within the realm of electronic commerce but are governed by a set of specific directives and regulations.

This fact sheet provides an overview of the relevant case-law delivered until 30 April 2024. To that end, it divides the main judgments covering this range of areas into two parts, one relating to aspects of contractual obligations between parties and the other the legal framework governing electronic commerce.

For the purposes of this fact sheet, the judgments selected are those of the Court, deemed to be the most relevant in the field, most of them having been delivered by the Grand Chamber.

[1] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ 2000 L 178, p. 1).

List of acts referred to

REGULATIONS

Council Regulation (EC) No 40/94 of 20 December 1993 on the Community trade mark (OJ 1994 L 11, p. 1).

Commission Regulation (EC) No 2790/1999 of 22 December 1999 on the application of Article 81(3) of the Treaty to categories of vertical agreements and concerted practices (OJ 1999 L 336, p. 21).

Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ 2001 L 12, p. 1).

Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) (OJ 2007 L 199, p. 40).

Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) (OJ 2008 L 177, p. 6).

Commission Regulation (EU) No 330/2010 of 20 April 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices (OJ 2010 L 102, p. 1).

Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (OJ 2015 L 310, p. 1).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1).

Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark (OJ 2017 L 154, p. 1).

IMPLEMENTING REGULATION

Council Implementing Regulation (EU) No 282/2011 of 15 March 2011 laying down implementing measures for Directive 2006/112/EC on the common system of value added tax (OJ 2011 L 77, p. 1).

DIRECTIVES

Council Directive 84/450/EEC of 10 September 1984 relating to the approximation of the laws, regulations and administrative provisions of the Member States concerning misleading advertising, as amended by Directive 2005/29/EC (OJ 1984 L 250, p. 17).

Council Directive 89/104/EEC of 21 December 1988 to approximate the laws of the Member States relating to trade marks (OJ 1989 L 40, p. 1).

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ 1993 L 95, p. 29).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).

Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts (OJ 1997 L 144, p. 19).

Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services (OJ 1998 L 204, p. 37), as amended by Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 (OJ 1998 L 217, p. 18) ('Directive 98/34').

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ 2000 L 178, p. 1).

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ 2001 L 167, p. 10).

Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (OJ 2001 L 311, p. 67), as amended by Directive 2011/62/EU of the European Parliament and of the Council of 8 June 2011 (OJ 2011 L 174, p. 74).

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

(OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11).

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ 2004 L 157, p. 45, and corrigendum OJ 2004 L 195, p. 16).

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (OJ 2005 L 149, p. 22).

Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax (OJ 2006 L 347, p. 1).

Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising (OJ 2006 L 376, p. 21).

Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (OJ 2006 L 376, p. 28).

Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market (OJ 2006 L 376, p. 36).

Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (OJ 2007 L 319, p. 1).

Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests (OJ 2009 L 110, p. 30).

Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (OJ 2009 L 111, p. 16).

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ 2015 L 241, p. 1).

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (OJ 2019 L 130, p. 92).

DECISIONS

Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p. 7).

Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ 2010 L 39, p. 5), as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344, p. 100).

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (OJ 2016 L 207, p. 1).

Contents

I. Contractual relations between parties

1. Conclusion of the contract

Judgment of 5 July 2012,* Content Services *(C-49/11, EU:C:2012:419)

The company Content Services operated a subsidiary in Mannheim (Germany) and offered various services online on its website, configured in German and also accessible in Austria. On that site, it was possible inter alia to download free software or trial versions of software which incur a charge. Before placing an order, internet users had to fill in a registration form and tick a specific box on the form declaring that they accepted the general terms and conditions of sale and waived their right of withdrawal.

That information was not shown directly to internet users, but they could nonetheless view it by clicking on a link on the contract sign-up page. The conclusion of a contract was impossible if the box had not been ticked. Next, the internet user concerned would receive an email from Content Services which did not contain any information on the right of withdrawal but, as before, contained a link in order to view the information. The Oberlandesgericht Wien (Higher Regional Court, Vienna, Austria) referred a question to the Court of Justice for a preliminary ruling on the interpretation of Article 5(1) of Directive 97/7/EC. [2] It asked whether a business practice consisting of making the information referred to in that provision accessible to the consumer only via a hyperlink on a website of the undertaking concerned meets the requirements of that provision.

According to the Court, Article 5(1) of Directive 97/7/EC must be interpreted as meaning that that business practice does not meet the requirements of that provision, since the information is neither 'given' by that undertaking nor 'received' by the consumer and a website cannot be regarded as a 'durable medium'.

The consumer must receive confirmation of that information without there being any requirement for active conduct on his part. Furthermore, if a website is to be regarded as a durable medium, it must ensure that the consumer, in a similar way to paper form, is in possession of the information referred to in that provision to enable him to exercise his rights where necessary. It must allow the consumer to store the information which has been addressed to him personally, ensure that its content is not altered and that the information is accessible for an adequate period, and give consumers the possibility to reproduce it unchanged.

[2] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts (OJ 1997 L 144, p. 19).

Judgment of 25 January 2017, **BAWAG** *(C-375/15, EU:C:2017:38)*

The bank BAWAG, which operated in Austria, used a standard contractual term to have consumers sign up to online banking services ('e-banking').

Under that term, 'notices and statements which the bank has to provide to the customer or make available to him shall be sent by post or electronically by means of e-banking'. The information could be sent using an online account messaging system. Consumers were able to view, reproduce and download the messages. The messages in the e-banking online accounts remained there without change and were not deleted during a period of time adequate for the purposes of informing those consumers, so that they could be viewed and reproduced unchanged by electronic or printed means. However, consumers were not informed of the receipt of a new message by any other means.

The Oberster Gerichtshof (Supreme Court, Austria) referred a question to the Court of Justice for a preliminary ruling in order to ascertain whether Article 41(1) of Directive 2007/64/EC, [3] read in conjunction with Article 36(1) thereof, must be interpreted as meaning that information sent by means of the electronic mailbox of an online banking platform is 'provided on a durable medium'.

The Court held that certain websites have to be classified as 'durable mediums' within the meaning of Article 4(25) of that directive.

However, changes to the framework contract, which are sent by the payment service provider to the user of those services by means of an electronic mailbox, may not be considered to have been provided on a durable medium unless the following two conditions are met:

- the website must allow only that user to store and reproduce information in such a way that he may access it for an adequate period;
- the transmission of that information must be accompanied by active behaviour on the part of the payment service provider aimed at drawing the user's attention to the availability of that information.

The sending of an email to the address regularly used by the user of those services to communicate with other persons and which the parties agreed to use in the framework contract entered into between the payment service provider and that user could also constitute such behaviour. The address thus chosen may not, however, be the address assigned to that user on the online banking website managed by the payment service provider.

[3] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market, amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (OJ 2007 L 319, p. 1).

Judgment of 15 September 2020 (Grand Chamber),* Telenor Magyarország *(C-807/18 and C-39/19, EU:C:2020:708)

Telenor, a company established in Hungary, provides internet-access services in particular. The services offered to its customers include two packages with preferential access (known as 'zero tariff'), and the specific feature of those packages is that the data traffic generated by certain specific applications and services does not count towards the consumption of the data volume purchased by customers. In addition, once that volume of data has been used up, those customers may continue to use those specific applications and services without restriction, while measures blocking or slowing down data traffic are applied to the other available applications and services.

After initiating two procedures to verify whether those two packages complied with Regulation 2015/2120 laying down measures concerning open internet access, [4] the Hungarian National Media and Communications Office adopted two decisions by which it found that those packages did not comply with the general obligation of equal and non-discriminatory treatment of traffic laid down in Article 3(3) of that regulation and that Telenor had to put an end to those measures.

The Fővárosi Törvényszék (Budapest High Court, Hungary), hearing two actions brought by Telenor, decided to refer the matter to the Court of Justice for a preliminary ruling, in order to ascertain how to interpret and apply Article 3(1) and (2) of Regulation 2015/2120, which safeguards a number of rights [5] for end users of internet access services and prohibits providers of such services from putting in place agreements or commercial practices limiting the exercise of those rights, and Article 3(3), which lays down a general obligation of equal and non-discriminatory treatment of traffic.

In its judgment of 15 September 2020, the Court, sitting as the Grand Chamber, interpreted for the first time Regulation 2015/2120, which enshrines the fundamental principle of an open internet (more colloquially known as 'net neutrality').

As regards, in the first place, the interpretation of Article 3(2) of Regulation 2015/2120, read in conjunction with Article 3(1) of that regulation, the Court observed that Article 3(1) provides that the rights which it safeguards for end users of internet access services are intended to be exercised 'via their internet access service', and that Article 3(2) requires that such a service does not entail any limitation of the exercise of those rights. In addition, it follows from Article 3(2) of Regulation 2015/2120 that the services of a given provider of internet access services must be assessed in the light of that requirement by the national regulatory authorities, [6] subject to review by the

---

4 Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (OJ 2015 L 310, p. 1).

5 Right for end users to access and use applications, content and services, but also the right to provide applications, content and services and to use terminals of their choice.

6 On the basis of Article 5 of Regulation 2015/2120.

competent national courts, and taking into consideration both the agreements concluded by that provider with end users and the commercial practices in which it engages.

In that context, after providing a series of general clarifications of the meaning of the concepts of 'agreements', 'commercial practices' and 'end users' [7] contained in Regulation 2015/2120, the Court found that the conclusion of agreements, by which given customers subscribe to a package combining a 'zero tariff' and measures blocking or slowing down the traffic linked to the use of 'non-zero tariff' services and applications, is liable to limit the exercise of end users' rights, within the meaning of Article 3(2) of Regulation 2015/2120, on a significant part of the market. Such packages are liable to increase the use of the favoured applications and services and, accordingly, to reduce the use of the other applications and services available, having regard to the measures by which the provider of the internet access services makes that use technically more difficult, if not impossible. Furthermore, the greater the number of customers concluding such agreements, the more likely it is that, given its scale, the cumulative effect of those agreements will result in a significant limitation of the exercise of end users' rights, or even undermine the very essence of those rights.

In the second place, as regards the interpretation of Article 3(3) of Regulation 2015/2120, the Court found that, in order to make a finding of incompatibility with that provision, no assessment of the effect of measures blocking or slowing down traffic on the exercise of end users' rights is required. Article 3(3) does not lay down such a requirement in order to assess whether the general obligation of equal and non-discriminatory treatment of traffic in that provision has been complied with. In addition, the Court held that, where measures blocking or slowing down traffic are based not on objectively different technical quality of service requirements for specific categories of traffic, but on commercial considerations, those measures must in themselves be regarded as incompatible with Article 3(3).

Consequently, packages such as those under review by the referring court are, generally, liable to infringe both paragraphs 2 and 3 of Article 3 of Regulation 2015/2120, it being specified that the competent national authorities and courts may examine those packages at the outset in the light of Article 3(3).

[7] The concept of 'end user' encompasses all legal entities or natural persons using or requesting a publicly available electronic communications service. It also includes both natural or legal persons who use or request internet access services in order to access content, applications and services, as well as those who rely on internet access to provide content, applications and services.

2. Applicable law/jurisdiction

Judgment of 28 July 2016,* Verein für Konsumenteninformation *(C-191/15, EU:C:2016:612)

The undertaking Amazon EU Sàrl, established in Luxembourg, sold goods online to consumers established in various Member States. In the main proceedings, the Austrian consumer protection association (Verein für Konsumenteninformation) had brought an action for an injunction, based on Directive 2009/22/EC, [8] claiming that the contractual terms used by Amazon were contrary to legal prohibitions or accepted principles of morality.

Proceedings having been brought before it by the Austrian association, the Oberster Gerichtshof (Supreme Court, Austria) enquired whether a term in the general terms and conditions of sale of a contract concluded in the course of electronic commerce between a seller or supplier and a consumer, under which the contract is to be governed by the law of the Member State in which the seller or supplier is established, is unfair within the meaning of Article 3(1) of Directive 93/13/EEC. [9] The Oberster Gerichtshof also asked whether the processing of personal data by an undertaking is subject, in accordance with Article 4(1)(a) of Directive 95/46/EC [10], to the law of the Member State towards which that undertaking directs its activities.

According to the Court, the Rome I [11] and Rome II [12] Regulations must be interpreted as meaning that the law applicable to an action for an injunction is to be determined in accordance with Article 6(1) of the Rome II Regulation, since the undermining of legal stability results from the use of unfair terms. On the other hand, the law applicable to the assessment of the contractual term in question must be determined pursuant to the Rome I Regulation, whether that assessment is made in an individual action or in a collective action.

However, it is apparent from Article 6(2) of the Rome I Regulation that the choice of the applicable law is without prejudice to the application of the mandatory provisions laid down by the law of the country of residence of the consumers whose interests are being defended by means of that action for an injunction. Those provisions may include the provisions transposing Directive 93/13/EEC, provided that they ensure a higher level of protection for the consumer.

---

8 Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests (OJ 2009 L 110, p. 30).

9 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ 1993 L 95, p. 29).

10 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).

11 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) (OJ 2008 L 177, p. 6).

12 Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) (OJ 2007 L 199, p. 40).

Thus, a term which has not been individually negotiated, under which the contract concluded with a consumer in the course of electronic commerce is to be governed by the law of the Member State in which the seller or supplier is established, is unfair within the meaning of Article 3(1) of Directive 93/13/EEC, in so far as it leads the consumer into error by giving him the impression that only the law of that Member State applies to the contract, without informing him that he also enjoys the protection of the mandatory provisions of the law that would be applicable in the absence of that term.

Moreover, Article 4(1)(a) of Directive 95/46/EC must be interpreted as meaning that the processing of personal data carried out by an undertaking engaged in electronic commerce is governed by the law of the Member State to which that undertaking directs its activities, if it is shown that the undertaking carries out the data processing at issue in the context of the activities of an establishment situated in that Member State. Both the degree of stability of the arrangements and the effective exercise of activities in the Member State in question must be assessed.

Judgment of 7 December 2010 (Grand Chamber),* Pammer and Alpenhof *(C-585/08 and C-144/09, EU:C:2010:740)

The joined cases *Pammer* and *Alpenhof* concern two sets of main proceedings dealing with similar issues. In *Pammer*, a consumer domiciled in Austria brought proceedings against a cargo shipper, established in Germany, concerning the reimbursement of the voyage cost. He argued that the vessel and the voyage did not correspond to the description provided on the website of the agency that acted as intermediary, also established in Germany, advertising such voyages.

The Austrian first-instance court found that it had jurisdiction to hear the case. By contrast, the appellate court held that the Austrian courts did not have jurisdiction. The question referred for a preliminary ruling by the Oberster Gerichtshof (Supreme Court, Austria) asked the Court of Justice to interpret the concept of contract combining travel and accommodation for an inclusive price, as referred to in Article 15(3) of Regulation (EC) No 44/2001, [13] to which the provisions of Section 4 of Chapter II thereof apply. The national court also wondered whether the fact that the Austrian consumer's attention had been drawn to the voyage by consulting the website of the intermediary agency, without the voyage having been reserved by internet, was sufficient to find that the Austrian courts had jurisdiction.

The second case, *Alpenhof*, involved proceedings brought by an Austrian company, which operated a hotel and had its seat in Austria, against a consumer, domiciled in Germany, concerning the payment of a bill for hotel services agreed upon by an exchange of

[13] Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ 2001 L 12, p. 1).

emails based on information provided on the applicant company's website. The Austrian courts dismissed the action on the ground that they lacked jurisdiction.

According to the Court, a contract concerning a voyage by freighter may constitute a contract of transport which, for an inclusive price, provides for a combination of travel and accommodation if that voyage by freighter involves, for an inclusive price, accommodation too and is for a period of more than 24 hours.

In order to determine whether a trader whose activity is presented on its website or on that of an intermediary can be considered to be 'directing' its activity to the Member State of the consumer's domicile, it should be ascertained whether that trader was envisaging doing business with consumers domiciled in one or more Member States.

The following matters, the list of which is not exhaustive, are capable of constituting evidence from which it may be concluded that the trader's activity is directed to the Member State of the consumer's domicile, namely the international nature of the activity, mention of itineraries from other Member States for going to the place where the trader is established, use of a language or a currency other than the language or currency generally used in the Member State in which the trader is established, and the possibility of making and confirming the reservation in that other language. On the other hand, the mere accessibility of the trader's or the intermediary's website in the Member State in which the consumer is domiciled is insufficient. The same is true of mention of an email address and of other contact details, or of use of a language or a currency which are the language and/or currency generally used in the Member State in which the trader is established.

Judgment of 6 September 2012,* Mühlleitner *(C-190/11, EU:C:2012:542)

The main proceedings involved a dispute between a consumer, Ms Daniela Mühlleitner, domiciled in Austria, and car sellers domiciled in Hamburg, Germany, concerning the purchase of a car. After locating their contact details on their website, Ms Mühlleitner telephoned the sellers from Austria, where she later received an offer by email. The contract was nonetheless concluded at the sellers' premises in Germany.

Subsequently, the first-instance court, the Landesgericht Wels (Regional Court, Wels, Austria), rejected the action on the ground that it lacked jurisdiction. The Oberlandesgericht Linz (Higher Regional Court, Linz, Austria) confirmed the decision, recalling that a purely 'passive' website was not sufficient for it to be considered that an activity is directed to the consumer's State. Ms Mühlleitner brought an appeal on a point of law against the judgment before the Oberster Gerichtshof (Supreme Court, Austria). That court asked the Court of Justice whether the application of Article 15(1)(c) of the

Brussels I Regulation [14] presupposes that the contract between the consumer and the trader has been concluded at a distance.

The Court ruled that Article 15(1)(c) of Regulation (EC) No 44/2001 must be interpreted as not requiring the contract between the consumer and the trader to be concluded at a distance.

In the first place, that provision does not expressly make its application conditional on the fact that the contracts falling within its scope have been concluded at a distance. In the second place, as regards a teleological interpretation of that provision, the addition of a condition concerning the conclusion of consumer contracts at a distance would run counter to the objective of that provision, in particular the objective of protecting consumers as the weaker parties to the contract. In the third place, the essential condition to which the application of Article 15(1)(c) of that regulation is subject is that relating to a commercial or professional activity directed to the State of the consumer's domicile. In that respect, both the establishment of contact at a distance and the reservation of goods or services at a distance or, *a fortiori*, the conclusion of a consumer contract at a distance are indications that the contract is connected with such an activity.

Judgment of 17 October 2013,* Emrek *(C-218/12, EU:C:2013:666)

Mr Emrek, domiciled in Saarbrücken (Germany), was looking for a car and had learned from acquaintances of Mr Sabranovic's business. Mr Sabranovic operated a business selling second-hand motor vehicles in Spicheren (France). He also had a website which contained the contact details for his business, including French telephone numbers and a German mobile telephone number, together with the respective international codes. However, Mr Emrek did not learn of the business from the website. Thus, Mr Emrek, as a consumer, concluded a written contract for the sale of a second-hand motor vehicle with Mr Sabranovic at his premises.

Mr Emrek subsequently brought an action against Mr Sabranovic under the warranty before the Amtsgericht Saarbrücken (Local Court, Saarbrücken, Germany). The court held that it lacked jurisdiction. Mr Emrek appealed against that decision before the referring court, the Landgericht Saarbrücken (Regional Court, Saarbrücken, Germany). The referring court sought to ascertain whether the application of Article 15(1)(c) of Regulation (EC) No 44/2001 required the existence of a causal link between the trader's activities directed to the Member State in which the consumer is domiciled over the internet and the conclusion of contracts.

The Court pointed out that in its judgment in *Pammer and Alpenhof* (C-585/08 and C-144/09), it had identified a non-exhaustive list of factors capable of constituting

[14] Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ 2001 L 12, p. 1).

evidence which national courts may use to determine whether the essential condition of commercial activity directed to the Member State of the consumer's domicile is fulfilled.

It found that Article 15(1)(c) of Regulation (EC) No 44/2001 must be interpreted as meaning that it does not require the existence of a causal link between the means employed to direct the commercial or professional activity to the Member State of the consumer's domicile, namely a website, and the conclusion of the contract with that consumer. However, the existence of such a causal link constitutes evidence of the connection between the contract and such activity.

Judgment of 21 May 2015, El Majdoub (C-322/14, EU:C:2015:334)

The dispute in the main proceedings concerned the sale of a motor vehicle through a website. The general terms and conditions of sale, accessible on that website, contained an agreement conferring jurisdiction on a court in a Member State. The window containing those general terms and conditions of sale did not open automatically upon registration and upon every individual sale; instead the purchaser had to click a specific box to accept the terms and conditions.

The Landgericht Krefeld (Regional Court, Krefeld, Germany) asked the Court of Justice to determine whether the validity of a jurisdiction clause is affected if the click-wrapping technique is used.

In the first place, regarding the question of ensuring the real consent of the parties, which is one of the aims of Article 23(1) of Regulation (EC) No 44/2001, the Court held that the purchaser in the main proceedings had expressly accepted the general terms and conditions at issue, by clicking the relevant box on the seller's website. In the second place, it found that it follows from a literal interpretation of Article 23(2) of that regulation that it requires there to be the 'possibility' of providing a durable record of the agreement conferring jurisdiction, regardless of whether the text of the general terms and conditions has actually been durably recorded by the purchaser before or after he clicks the box indicating that he accepts those conditions.

The Court observed that the purpose of that provision is to treat certain forms of electronic communications in the same way as written communications in order to simplify the conclusion of contracts by electronic means, since the information concerned is also communicated if it is accessible on screen. In order for electronic communication to offer the same guarantees, in particular as regards evidence, it is sufficient that it is 'possible' to save and print the information before the conclusion of the contract. Consequently, since click-wrapping makes it possible to print and save the text of the terms and conditions before the conclusion of the contract, the fact that the web page containing that information does not open automatically upon registration on the website and during each purchase cannot call into question the validity of the agreement conferring jurisdiction. Click-wrapping therefore constitutes a

communication by electronic means within the meaning of Article 23(2) of Regulation (EC) No 44/2001.

Judgment of 25 January 2018, **Schrems** *(C-498/16, EU:C:2018:37)*

Mr Maximilian Schrems had been a private user of the social network Facebook since 2008. He brought class actions against the company Facebook Ireland Limited. Furthermore, in 2011, he opened a Facebook page registered and established by him, in order to report to internet users on his legal proceedings. He founded a non-profit organisation the purpose of which was to enforce the fundamental right to data protection and provide financial support for test cases.

In proceedings between Mr Maximilian Schrems and Facebook Ireland Limited concerning applications seeking declarations and an injunction, disclosure and production of Facebook accounts, the Oberster Gerichtshof (Supreme Court, Austria) enquired whether Article 15 of Regulation (EC) No 44/2001 must be interpreted as meaning that a person loses his consumer status if, after using a private Facebook account for several years, he publishes books, delivers lectures for remuneration or manages websites. The national court also asked whether Article 16 of that regulation must be interpreted as meaning that a consumer can also invoke at the same time as his own claims under a consumer contract similar claims of other consumers who are domiciled in the same Member State, in another Member State, or in a non-Member State.

The Court stated that the notion of 'consumer' must be independently and strictly construed. To determine whether Article 15 applies, the contract must have been concluded between the parties for the purpose of a use of the relevant goods or services that is other than a trade or professional use. As regards a person who concludes a contract for a purpose which is partly concerned with his trade or profession, the link between the contract and the trade or profession of the person concerned is so slight as to be marginal and, therefore, has only a negligible role in the context of the supply.

Next, the Court found that the consumer is protected only in so far as he is, in his personal capacity, the plaintiff or defendant in proceedings. Consequently, an applicant who is not himself a party to the consumer contract in question cannot enjoy the benefit of the jurisdiction relating to consumer contracts. The same considerations must also apply to a consumer to whom the claims of other consumers have been assigned. Indeed, Article 16(1) necessarily implies that a contract has been concluded by the consumer with the trader or professional concerned.

In addition, the assignment of claims cannot, in itself, have an impact on the determination of the court having jurisdiction. It follows that the jurisdiction of courts cannot be established through the concentration of several claims in the person of a

single applicant. The regulation does not apply to the proceedings brought by a consumer as in the instant case.

3. Consumer protection

Judgment of 16 October 2008,* Bundesverband der Verbraucherzentralen *(C-298/07, EU:C:2008:572)

DIV, an automobile insurance company, offered its services exclusively on the internet. On its web pages, it mentioned its postal and email addresses but not its telephone number. Its telephone number was communicated only after the conclusion of an insurance contract. However, persons interested in DIV's services were able to ask questions via an online enquiry template, the answers to which were sent by email. The Bundesverband der Verbraucherzentralen (the German Federation of Consumers' Associations) took the view that DIV had an obligation to mention its telephone number on its website. That would be the only means of guaranteeing direct communication.

The Bundesgerichtshof (Federal Court of Justice, Germany) decided to ask the Court of Justice whether Article 5(1)(c) of Directive 2000/31/EC [15] requires a telephone number to be given.

The Court held that Article 5(1)(c) of Directive 2000/31/EC must be interpreted as meaning that a service provider is required to supply to recipients of the service, before the conclusion of a contract with them, in addition to its email address, other information which allows the service provider to be contacted rapidly and communicated with in a direct and effective manner.

That information does not necessarily have to be a telephone number. It may be in the form of an electronic enquiry template through which the recipients of the service can contact the service provider via the internet, to whom the service provider replies by email except in situations where a recipient of the service, who, after contacting the service provider electronically, finds himself without access to the electronic network, requests the latter to provide access to another, non-electronic means of communication.

Judgment of 3 September 2009,* Messner *(C-489/07, EU:C:2009:502)

Ms Messner, a German consumer, withdrew from the purchase of a laptop computer over the internet. The seller of the computer had refused to repair free of charge a

[15] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (OJ 2000 L 178, p. 1).

defect that had appeared eight months after the purchase. Ms Messner subsequently stated that she was revoking the contract of sale and offered to return the laptop computer to the seller in return for a refund of the purchase price. That revocation was carried out within the period provided for in the BGB (German Civil Code) in so far as Ms Messner had not received effective notice, provided for in the provisions of that Code, such as to commence the period for withdrawal. Ms Messner claimed reimbursement of EUR 278 before the Amtsgericht Lahr (Local Court, Lahr, Germany). In opposition to that claim, the seller submitted that Ms Messner was, in any event, obliged to pay him compensation for value inasmuch as she had been using the laptop computer for approximately eight months.

In its judgment, the Court found that the provisions of the second sentence of Article 6(1) and Article 6(2) of Directive 97/7/EC [16] must be interpreted as precluding a provision of national law which provides in general that, in the case of withdrawal by a consumer within the withdrawal period, a seller may claim compensation for the value of the use of the consumer goods acquired under a distance contract.

If the consumer were required to pay such compensation merely because he had the opportunity to use the goods while they were in his possession, he would be able to exercise his right of withdrawal only against payment of that compensation. Such an outcome would be clearly at variance with the wording and purpose of the second sentence of Article 6(1) and Article 6(2) of Directive 97/7/EC and would, in particular, deprive the consumer of the opportunity to make completely free and independent use of the period for reflection granted to him by that directive.

Likewise, the efficiency and effectiveness of the right of withdrawal would be impaired if the consumer were obliged to pay compensation simply because he had examined and tested the goods. To the extent to which the right of withdrawal is intended precisely to give the consumer that opportunity, the fact of having made use of it cannot have the consequence that the consumer is able to exercise that right only if he pays compensation.

However, those provisions do not prevent the consumer from being required to pay compensation for the use of the goods in the case where he has made use of those goods in a manner incompatible with the principles of civil law, such as those of good faith or unjust enrichment, on condition that the purpose of that directive and, in particular, the efficiency and effectiveness of the right of withdrawal are not adversely affected, this being a matter for the national court to determine.

[16] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts (OJ 1997 L 144, p. 19).

Judgment of 15 April 2010, **Heinrich Heine** *(C-511/08, EU:C:2010:189)*

A mail-order undertaking, Heinrich Heine, provided in its general terms and conditions of sale that the consumer is to pay a flat-rate charge of EUR 4.95 for delivery. The supplier would not refund that amount even if the consumer were to exercise his right of withdrawal. The Verbraucherzentrale Nordrhein-Westfalen, a German consumer association, brought an action for an injunction to prevent Heinrich Heine from engaging in that practice, arguing that the delivery costs should not be charged to consumers in the event of withdrawal. According to the Bundesgerichtshof (Federal Court of Justice, Germany), German law does not explicitly grant the purchaser any right to reimbursement of the costs of delivering the goods ordered. Since the court was unsure about the compatibility with Directive 97/7/EC [17] of charging the costs of delivering the goods to the consumer, even where he has withdrawn from the contract, it asked the Court of Justice to interpret that directive.

In its judgment, the Court held that Article 6(1), first subparagraph, second sentence, and Article 6(2) of Directive 97/7/EC must be interpreted as precluding national legislation which allows the supplier under a distance contract to charge the costs of delivering the goods to the consumer where the latter exercises his right of withdrawal.

Those provisions authorise suppliers to charge consumers, in the event of their withdrawal, only the direct cost of returning the goods. If consumers also had to pay the delivery costs, such a charge, which would necessarily dissuade consumers from exercising their right of withdrawal, would run counter to the very objective of Article 6.

In addition, charging them in that way would compromise a balanced sharing of the risks between parties to distance contracts, by making consumers liable to bear all of the costs related to transporting the goods.

Judgment of 6 July 2017, **Air Berlin** *(C-290/16, EU:C:2017:523)*

The German airline Air Berlin introduced into its general terms and conditions of sale a term under which, if a passenger cancelled his flight booking at the economy rate or did not take the flight, he would be charged a handling fee of EUR 25 on the amount to be reimbursed to him. The Bundesverband der Verbraucherzentralen (German Federal Union of Consumer Organisations) argued that that term was invalid under German law because it unduly disadvantaged customers. Moreover, Air Berlin could not charge any separate fees for the fulfilment of a legal obligation. The Bundesverband therefore brought an action before the German courts seeking an injunction against Air Berlin.

In the same action, the Bundesverband challenged the practices of Air Berlin relating to the display of prices on its website. During a simulated online booking in 2010, the

[17] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts (OJ 1997 L 144, p. 19).

Bundesverband had found that the taxes and charges indicated were much lower those actually levied by the airports concerned. The Bundesverband submitted that the practice could mislead consumers and was contrary to the rules on price transparency laid down in EU law on the operation of air services. [18] The Bundesgerichtshof (Federal Court of Justice, Germany) asked the Court of Justice, first, whether Regulation (EC) No 1008/2008 is to be interpreted as meaning that, when publishing their air fares, air carriers must specify the actual amount of charges and therefore may not partially include them in their air fares, and, secondly, whether that regulation precludes the application of a national law on general terms and conditions of sale, which is based on EU law, according to which a separate handling fee cannot be imposed on customers who have not taken a flight or cancelled their booking.

The Court replied that the third sentence of Article 23(1) of Regulation (EC) No 1008/2008 must be interpreted as meaning that, when publishing their air fares, air carriers must specify separately the amounts payable by customers in respect of taxes, airport charges and other charges, surcharges or fees referred to in that regulation. Furthermore, they may not, as a consequence, include those items, even partially, in the air fare. Article 23(1) of Regulation (EC) No 1008/2008 seeks to ensure, in particular, that there is information and transparency with regard to prices for air services from an airport located in a Member State and accordingly to contribute to safeguarding protection of customers who use those services. Moreover, a different interpretation would deprive that provision of all practical effect.

Article 22(1) of Regulation (EC) No 1008/2008 must be interpreted as not precluding the application of national legislation transposing Directive 93/13/EEC from leading to a declaration of invalidity of a term in general terms and conditions of sale which allows separate flat-rate handling fees to be billed to customers who did not take a flight or who cancelled their booking. The Court found that the general rules protecting consumers against unfair terms also apply to contracts of carriage by air.

Thus, Regulation (EEC) No 2409/92, repealed by Regulation (EC) No 1008/2008, stated in its fifth recital that it was appropriate 'to complement price freedom with adequate safeguards for the interests of consumers and industry'.

Judgment of 10 July 2019,* Amazon EU *(C-649/17, EU:C:2019:576)

Amazon EU Sàrl, a company established in Luxembourg, offers online sales of various products. In the main proceedings, the Federal Union of Consumer Organisations and Associations, Germany ('The Federal Union') had brought an application for an injunction before a regional court relating to Amazon EU practices for the display of information on its website www.amazon.de and the possibility for consumers to contact that company.

[18] Regulation (EC) No 1008/2008 of the European Parliament and of the Council of 24 September 2008 on common rules for the operation of air services in the Community (OJ 2008 L 293, p. 3).

Since that Court dismissed that application, the Federal Union brought an appeal against that decision before a higher regional court, which was also dismissed. In those circumstances, the Federal Union brought an appeal on a point of law (Revision) before the referring court, the Bundesgerichtshof (Federal Court of Justice, Germany).

The request for a preliminary ruling concerned the interpretation of Article 6(1)(c) of Directive 2011/83/EU. [19]

First, the Court noted that the possibility, for consumers, to contact traders quickly and to communicate with them efficiently, as provided for in that provision, is of fundamental importance for ensuring and effectively implementing consumer rights and, in particular, the right of withdrawal, the detailed arrangements and conditions for the exercise of which are set out in Articles 9 to 16 of that directive. However, in interpreting that provision, it is necessary to ensure the right balance between a high level of consumer protection and the competitiveness of undertakings, as is stated in recital 4 of Directive 2011/83/EU, while respecting the undertaking's freedom to conduct a business, as set out in the Charter of Fundamental Rights of the European Union ('the Charter').

The Court held that it is for the national court to assess whether, in the light of all the circumstances in which consumers make contact with traders through a website and in particular of the presentation and functionality of that site, the means of communication made available to those consumers by those traders allow consumers to contact traders quickly and to communicate with them efficiently, in accordance with Article 6(1)(c) of Directive 2011/83/EU.

In that regard, the Court pointed out that an unconditional obligation to provide consumers, in all circumstances, with a telephone number, or even to put in place a telephone or fax line, or to create a new email address in order to allow consumers to contact traders seems to be disproportionate.

The Court thus held that it is necessary to interpret the words 'where available' provided for in Article 6(1)(c) of Directive 2011/83/EU as covering cases where traders have a telephone or fax number and do not use them solely for purposes other than contacting consumers. In the absence thereof, that provision does not impose on traders the obligation to inform consumers of that telephone number, to provide a telephone or fax line, or to create a new email address to allow consumers to contact them.

Secondly, having examined whether those traders may, in circumstances such as those in the main proceedings, make use of means of communication which are not mentioned in Article 6(1)(c) of Directive 2011/83/EU, such as instant messaging or a telephone callback system, the Court held that Article 6(1)(c) of Directive 2011/83/EU

[19] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (OJ 2011 L 304 p 64).

must be interpreted as meaning that, although that provision requires traders to make available to consumers a means of communication capable of satisfying the criteria of direct and effective communication, it does not preclude those traders from providing other means of communication than those listed in that provision in order to satisfy those criteria.

4. Protection of personal data

Judgment of 1 October 2015,* Weltimmo *(C-230/14, EU:C:2015:639)

Weltimmo, a company registered in Slovakia, ran a property dealing website concerning Hungarian properties. In that context, it processed the personal data of advertisers. The advertisements were free of charge for one month but thereafter a fee was payable. Many advertisers sent a request by email for the deletion of both their advertisements and their personal data at the end of the first month. However, Weltimmo did not delete those data and charged the interested parties for the price of its services. As the amounts charged were not paid, Weltimmo forwarded the personal data of the advertisers to debt collection agencies. The advertisers complained to the Hungarian data protection authority. That authority imposed on Weltimmo a fine of 10 million Hungarian forint (HUF) (approximately EUR 32 000) for having infringed the Hungarian law transposing Directive 95/46/EC. [20]

Weltimmo challenged the decision of the supervisory authority before the Hungarian courts. An appeal having been brought before it on a point of law, the Kúria (Supreme Court, Hungary) asked the Court of Justice whether that directive allowed the Hungarian supervisory authority to apply the Hungarian law adopted on the basis of the directive and impose the fine provided for in that law.

The Court pointed out that a flexible definition of the concept of 'establishment' follows from recital 19 of Directive 95/46/EC. Accordingly, in order to establish whether a company, the data controller, has an establishment in a Member State other than the Member State or third country where it is registered, both the degree of stability of the arrangements and the effective exercise of activities in that other Member State must be assessed. This is particularly true for undertakings offering services exclusively over the internet.

The Court found that Article 4(1)(a) of Directive 95/46/EC must be interpreted as permitting the application of the law on the protection of personal data of a Member State other than the Member State in which the controller with respect to the processing

[20] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).

of those data is registered, in so far as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity. By contrast, the issue of the nationality of the persons concerned by such data processing is irrelevant.

Where the supervisory authority of a Member State reaches the conclusion that the applicable law is not the law of that Member State, but the law of another Member State, Article 28(1), (3) and (6) of that directive must be interpreted as meaning that that supervisory authority will not be able to exercise the effective powers of intervention. Accordingly, it cannot impose penalties on the basis of the law of its own Member State on the controller with respect to the processing of those data who is not established in the territory of its own Member State. It follows from the requirements derived from the territorial sovereignty of the Member State concerned, the principle of legality and the concept of the rule of law that the exercise of the power to impose penalties cannot take place, as a matter of principle, outside the legal limits within which an administrative authority is authorised to act subject to the law of its own Member State.

Judgment of 6 October 2015 (Grand Chamber),* Schrems *(C-362/14, EU:C:2015:650)

Mr Maximillian Schrems, an Austrian citizen, had used Facebook since 2008. Some or all of the data provided by Mr Schrems to Facebook were transferred from Facebook's Irish subsidiary to servers located in the United States, where they were processed.
Mr Schrems lodged a complaint with the Irish supervisory authority arguing that in view of the revelations made in 2013 by Mr Edward Snowden concerning the activities of the United States intelligence services (in particular the National Security Agency or 'NSA'), the law and practices of the United States did not provide adequate protection against the surveillance by public authorities of data transferred to that country. The Irish authority rejected the complaint on the ground, inter alia, that in Decision 2000/520/EC, [21] the Commission had found that under the 'safe harbour' scheme, the United States ensured an adequate level of protection for transferred personal data.

Proceedings having been brought before it, the High Court (Ireland) sought to ascertain whether that decision of the Commission has the effect of preventing a national supervisory authority from investigating a complaint claiming that a third country does not ensure an adequate level of protection and, where appropriate, from suspending the disputed transfer of data.

The Court replied that the operation consisting in having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data

[21] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the Department of Commerce of the United States of America (OJ 2000 L 215, p. 7).

within the meaning of Article 2(b) of Directive 95/46/EC, [22] carried out in a Member State. The national authorities are therefore vested with the power to check whether a transfer of personal data from their own Member State to a third country complies with the requirements laid down by Directive 95/46/EC.

Thus, until such time as the Commission decision is declared invalid by the Court – which alone has jurisdiction to declare that an EU act is invalid – the Member States and their organs cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection. In a situation where a supervisory authority comes to the conclusion that the arguments put forward in support of a claim concerning the protection of rights and freedoms in regard to the processing of those personal data are unfounded and therefore rejects it, the person who lodged the claim must have access to judicial remedies enabling him to challenge such a decision adversely affecting him before the national courts. In the converse situation, where the national supervisory authority considers that the objections advanced by the person who has lodged with it such a claim are well founded, that authority must be able to engage in legal proceedings, in accordance with the third indent of the first subparagraph of Article 28(3) of Directive 95/46/EC, read in the light in particular of Article 8(3) of the Charter.

Article 25(6) of Directive 95/46/EC, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, by which the Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which have been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

The term 'adequate level of protection' in Article 25(6) of Directive 95/46/EC must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of that directive, read in the light of the Charter.

The safe harbour principles are applicable solely to self-certified United States organisations receiving personal data from the European Union, and United States public authorities are not required to comply with them. In addition, Decision 2000/520/EC enables interference, founded on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European

[22] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).

Union to the United States, without containing any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with those rights and without referring to the existence of effective legal protection against interference of that kind.

Furthermore, the Commission exceeded the power conferred upon it in Article 25(6) of Directive 95/46/EC, read in the light of the Charter, by adopting Article 3 of Decision 2000/520/EC, which is therefore invalid.

Judgment of 1 October 2019, **Planet49** *(Grand Chamber) (C-673/17, EU:C:2019:801)*

Planet49 is a company that organises a promotional lottery on the website www.dein-macbook.de. In order to take part, internet users were required to enter their names and addresses on a web page where there were checkboxes. The checkbox authorising the installation of cookies was pre-ticked.

In an appeal brought by the German Federation of Consumer Organisations, the Bundesgerichtshof (Federal Court of Justice, Germany) harboured doubts as to the validity of the consent obtained from internet users by means of the pre-ticked checkbox and as to the extent of the information obligation on the service provider.

The request for a preliminary ruling essentially concerned the interpretation of the concept of 'consent' referred to in the Directive on privacy and electronic communications, read in combination with Directive 95/46/EC and with the General Data Protection Regulation.

First, the Court observed that Article 2(h) of Directive 95/46/EC, to which Article 2(f) of the Directive on privacy and electronic communications refers, defines consent as being 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'. It noted that the requirement of an 'indication' of the data subject's wishes clearly points to active, rather than passive, behaviour. However, consent given in the form of a pre-ticked checkbox does not imply active behaviour on the part of a website user. In addition, the origins of Article 5(3) of the Directive on privacy and electronic communications, which, since its amendment by Directive 2009/136/EC, provides that the user must have 'given his or her consent' to the storage of cookies seems to indicate that henceforth user consent may no longer be presumed but must be the result of active behaviour on the part of the user. Lastly, active consent is now required under the General Data Protection Regulation since Article 4(11) of that regulation requires an indication of the data subject's wishes in the form of a 'clear affirmative action' and recital 32 thereof expressly precludes 'silence, pre-ticked boxes or inactivity' from constituting consent.

The Court therefore held that consent is not validly constituted if the storage of information, or access to information already stored in the website user's terminal

equipment, is permitted by way of a pre-ticked checkbox which the user must deselect to refuse giving consent.

Secondly, the Court found that Article 5(3) of the Directive on privacy and electronic communications aims to protect the user from interference with his or her private sphere, regardless of whether or not that interference involves personal data. It follows that the concept of 'consent' is not to be interpreted differently according to whether or not the information stored or accessed on a website user's terminal equipment is personal data.

Thirdly, the Court noted that Article 5(3) of the Directive on privacy and electronic communications requires that the user concerned has given his or her consent, having been provided with clear and comprehensive information, inter alia, about the purposes of the processing. Clear and comprehensive information implies that a user is in a position to be able to determine easily the consequences of any consent he or she might give and ensure that the consent given is well informed. In that regard, the Court held that the duration of the operation of the cookies and whether or not third parties may have access to those cookies form part of the clear and comprehensive information which must be provided to a website user by the service provider.

Judgment of 16 July 2020, **Facebook Ireland and Schrems** *(C-311/18, EU:C:2020:559)*

The General Data Protection Regulation [23] ('the GDPR') provides that the transfer of such data to a third country may, in principle, take place only if the third country in question ensures an adequate level of data protection. According to the GDPR, the Commission may find that a third country ensures, by reason of its domestic law or its international commitments, an adequate level of protection. [24] In the absence of an adequacy decision, such a transfer may take place only if the personal data exporter established in the European Union has provided appropriate safeguards, which may arise, in particular, from standard data protection clauses adopted by the Commission, and if data subjects have enforceable rights and effective legal remedies. [25]

Furthermore, the GDPR details the conditions under which such a transfer may take place in the absence of an adequacy decision or appropriate safeguards. [26]

Maximillian Schrems, an Austrian national residing in Austria, has been a Facebook user since 2008. As in the case of other users residing in the European Union, some or all of Mr Schrems's personal data are transferred by Facebook Ireland to servers belonging to Facebook Inc. that are located in the United States, where they undergo processing. Mr Schrems lodged a complaint with the Irish supervisory authority seeking, in essence,

[23] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ 2016 L 119, p. 1).
[24] Article 45 of the GDPR.
[25] Article 46(1) and (2)(c) of the GDPR.
[26] Article 49 of the GDPR.

to prohibit those transfers. He claimed that the law and practices in the United States do not offer sufficient protection against access by the public authorities to the data transferred to that country. That complaint was rejected on the ground, inter alia, that, in Decision 2000/520 [27] ('the Safe Harbour Decision'), the Commission had found that the United States ensured an adequate level of protection. In a judgment delivered on 6 October 2015, the Court of Justice, before which the High Court (Ireland) had referred questions for a preliminary ruling, declared that decision invalid ('the Schrems I judgment'). [28]

Following the Schrems I judgment and the subsequent annulment by the referring court of the decision rejecting Mr Schrems's complaint, the Irish supervisory authority asked Mr Schrems to reformulate his complaint in the light of the declaration by the Court that Decision 2000/520 was invalid. In his reformulated complaint, Mr Schrems claims that the United States does not offer sufficient protection of data transferred to that country. He seeks the suspension or prohibition of future transfers of his personal data from the European Union to the United States, which Facebook Ireland now carries out pursuant to the standard data protection clauses set out in the Annex to Decision 2010/87. [29] Taking the view that the outcome of Mr Schrems's complaint depends, in particular, on the validity of Decision 2010/87, the Irish supervisory authority brought proceedings before the High Court in order for it to refer questions to the Court for a preliminary ruling. After the initiation of those proceedings, the Commission adopted Decision 2016/1250 on the adequacy of the protection provided by the EU-US Privacy Shield [30] ('the Privacy Shield Decision').

By its request for a preliminary ruling, the referring court asks the Court whether the GDPR applies to transfers of personal data pursuant to the standard data protection clauses in Decision 2010/87, what level of protection is required by the GDPR in connection with such a transfer and what obligations are incumbent on supervisory authorities in those circumstances. The High Court also raises the question of the validity both of Decision 2010/87 and of Decision 2016/1250.

In its judgment, the Court finds that examination of Decision 2010/87 in the light of the Charter of Fundamental Rights has disclosed nothing to affect the validity of that decision. However, the Court declares Decision 2016/1250 invalid.

The Court considers, first of all, that EU law, and in particular the GDPR, applies to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, even if,

---

27 Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p. 7).

28 Judgment of 6 October 2015, *Schrems* (C-362/14, EU:C:2015:650).

29 Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ 2010 L 39, p. 5), as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344, p. 100).

30 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (OJ 2016 L 207, p. 1).

at the time of that transfer or thereafter, that data may be processed by the authorities of the third country in question for the purposes of public security, defence and State security. The Court adds that this type of data processing by the authorities of a third country cannot preclude such a transfer from the scope of the GDPR.

Regarding the level of protection required in respect of such a transfer, the Court holds that the requirements laid down for such purposes by the GDPR concerning appropriate safeguards, enforceable rights and effective legal remedies must be interpreted as meaning that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses must be afforded a level of protection essentially equivalent to that guaranteed within the European Union by the GDPR, read in the light of the Charter. In those circumstances, the Court specifies that the assessment of that level of protection must take into consideration both the contractual clauses agreed between the data exporter established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the data transferred, the relevant aspects of the legal system of that third country.

Regarding the supervisory authorities' obligations in connection with such a transfer, the Court holds that, unless there is a valid Commission adequacy decision, those competent supervisory authorities are required to suspend or prohibit a transfer of personal data to a third country where they take the view, in the light of all the circumstances of that transfer, that the standard data protection clauses are not or cannot be complied with in that country and that the protection of the data transferred that is required by EU law cannot be ensured by other means, where the data exporter established in the European Union has not itself suspended or put an end to such a transfer.

Next, the Court examines the validity of Decision 2010/87. The Court considers that the validity of that decision is not called into question by the mere fact that the standard data protection clauses in that decision do not, given that they are contractual in nature, bind the authorities of the third country to which data may be transferred. However, that validity, the Court adds, depends on whether the decision includes effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law and that transfers of personal data pursuant to such clauses are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them. The Court finds that Decision 2010/87 establishes such mechanisms. In that regard, the Court points out, in particular, that that decision imposes an obligation on a data exporter and the recipient of the data to verify, prior to any transfer, whether that level of protection is respected in the third country concerned and that the decision requires the recipient to inform the data exporter of any inability to comply with the standard data protection clauses, the latter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract with the former.

Lastly, the Court examines the validity of Decision 2016/1250 in the light of the requirements arising from the GDPR, read in the light of the provisions of the Charter guaranteeing respect for private and family life, personal data protection and the right to effective judicial protection. In that regard, the Court notes that that decision enshrines the position, as did Decision 2000/520, that the requirements of US national security, public interest and law enforcement have primacy, thus condoning interference with the fundamental rights of persons whose data are transferred to that third country. In the view of the Court, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to that third country, which the Commission assessed in Decision 2016/1250, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary. On the basis of the findings made in that decision, the Court pointed out that, in respect of certain surveillance programmes, those provisions do not indicate any limitations on the power they confer to implement those programmes, or the existence of guarantees for potentially targeted non-US persons. The Court adds that, although those provisions lay down requirements with which the US authorities must comply when implementing the surveillance programmes in question, the provisions do not grant data subjects actionable rights before the courts against the US authorities.

As regards the requirement of judicial protection, the Court holds that, contrary to the view taken by the Commission in Decision 2016/1250, the Ombudsperson mechanism referred to in that decision does not provide data subjects with any cause of action before a body which offers guarantees substantially equivalent to those required by EU law, such as to ensure both the independence of the Ombudsperson provided for by that mechanism and the existence of rules empowering the Ombudsperson to adopt decisions that are binding on the US intelligence services. On all those grounds, the Court declares Decision 2016/1250 invalid.

Judgment of 2 March 2021 (Grand Chamber),* Prokuratuur (Conditions of access to data relating to electronic communications) *(C-746/18, EU:C:2021:152)

Criminal proceedings were brought in Estonia against H. K. on counts of theft, use of another person's bank card and violence against persons party to court proceedings. A court of first instance convicted H. K. of those offences and imposed a custodial sentence of two years. That judgment was then upheld on appeal.

The reports relied upon in order to find H. K. guilty of those offences were drawn up, inter alia, on the basis of personal data generated in the context of the provision of electronic communications services. The Riigikohus (Supreme Court, Estonia), before which H. K. lodged an appeal on a point of law, expressed doubts as to whether the

conditions under which the investigating authority had access to those data were compatible with EU law. [31]

Those doubts concerned, first, whether the length of the period in respect of which the investigating authority has had access to the data is a criterion for assessing the seriousness of the interference, constituted by that access, with the fundamental rights of the persons concerned. Thus, the referring court raised the question whether, where that period is very short or the quantity of data gathered is very limited, the objective of combating crime in general, and not only combating serious crime, is capable of justifying such an interference. Second, the referring court had doubts as to whether it is possible to regard the Estonian public prosecutor's office, in the light of the various duties which are assigned to it by national legislation, as an 'independent' administrative authority, within the meaning of the judgment in *Tele2 Sverige and Watson and Others*, [32]that is capable of authorising access of the investigating authority to the data concerned.

By its judgment, delivered by the Grand Chamber, the Court holds that the directive on privacy and electronic communications, read in the light of the Charter, precludes national legislation that permits public authorities to have access to traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses and to allow precise conclusions to be drawn concerning his or her private life, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, without such access being confined to procedures and proceedings to combat serious crime or prevent serious threats to public security. According to the Court, the length of the period in respect of which access to those data is sought and the quantity or nature of the data available in respect of such a period are irrelevant in that regard. The Court further holds that that directive, read in the light of the Charter, precludes national legislation that confers upon the public prosecutor's office the power to authorise access of a public authority to traffic and location data for the purpose of conducting a criminal investigation.

As regards the circumstances in which access to traffic and location data retained by providers of electronic communications services may, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, be granted to public authorities, pursuant to a measure adopted under the directive on privacy and electronic communications, [33] the Court recalls the content of its ruling in *La Quadrature du Net and Others*. [34] Thus, that directive authorises the Member States to adopt, for

---

[31] To be more precise, with Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) ('the directive on privacy and electronic communications'), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union ('the Charter').

[32] Judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970, paragraph 120).

[33] Article 15(1) of Directive 2002/58.

[34] Judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/ 18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 166 to 169).

those purposes amongst others, legislative measures to restrict the scope of the rights and obligations provided for by the directive, inter alia the obligation to ensure the confidentiality of communications and traffic data, [35] only if the general principles of EU law – which include the principle of proportionality – and the fundamental rights guaranteed by the Charter [36] are observed. Within that framework, the directive precludes legislative measures which impose on providers of electronic communications services, as a preventive measure, an obligation requiring the general and indiscriminate retention of traffic and location data.

So far as concerns the objective of preventing, investigating, detecting and prosecuting criminal offences, which is pursued by the legislation at issue, in accordance with the principle of proportionality the Court holds that only the objectives of combating serious crime or preventing serious threats to public security are capable of justifying public authorities having access to a set of traffic or location data, that are liable to allow precise conclusions to be drawn concerning the private lives of the persons concerned, and other factors relating to the proportionality of a request for access, such as the length of the period in respect of which access to such data is sought, cannot have the effect that the objective of preventing, investigating, detecting and prosecuting criminal offences in general is capable of justifying such access.

As regards the power conferred upon the public prosecutor's office to authorise access of a public authority to traffic and location data for the purpose of conducting a criminal investigation, the Court points out that it is for national law to determine the conditions under which providers of electronic communications services must grant the competent national authorities access to the data in their possession. However, in order to satisfy the requirement of proportionality, such legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data are affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and must indicate in what circumstances and under which substantive and procedural conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary.

According to the Court, in order to ensure, in practice, that those conditions are fully observed, it is essential that access of the competent national authorities to retained data be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime. In cases of duly justified urgency, the review must take place within a short time.

---

[35] Article 5(1) of Directive 2002/58.

[36] In particular, Articles 7, 8 and 11 and Article 52(1) of the Charter.

In that regard, the Court states that one of the requirements for the prior review is that the court or body entrusted with carrying it out must have all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights at issue. As regards a criminal investigation in particular, it is a requirement of such a review that that court or body must be able to strike a fair balance between, on the one hand, the interests relating to the needs of the investigation in the context of combating crime and, on the other, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access. Where that review is carried out not by a court but by an independent administrative body, that body must have a status enabling it to act objectively and impartially when carrying out its duties and must, for that purpose, be free from any external influence.

According to the Court, it follows that the requirement of independence that has to be satisfied by the authority entrusted with carrying out the prior review means that that authority must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry out the review objectively and impartially and free from any external influence. In particular, in the criminal field the requirement of independence entails that the authority entrusted with the prior review, first, must not be involved in the conduct of the criminal investigation in question and, second, has a neutral stance vis-à-vis the parties to the criminal proceedings. That is not so in the case of a public prosecutor's office which, like the Estonian public prosecutor's office, directs the investigation procedure and, where appropriate, brings the public prosecution. It follows that the public prosecutor's office is not in a position to carry out the prior review.

Judgments of 6 October 2020 (Grand Chamber),* Privacy International *(C-623/17, EU:C:2020:790) and* La Quadrature du Net and Others *(C-511/18, C-512/18 and C-520/18, EU:C:2020:791)

In recent years, the Court of Justice has given rulings, in several judgments, on the retention of and access to personal data in the field of electronic communications. [37] The resulting case-law, in particular the judgment in *Tele2 Sverige and Watson and Others*, in

[37] Thus, in the judgment of 8 April 2014, *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2014:238), the Court declared Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54) invalid, on the ground that the interference with the rights to respect for private life and to the protection of personal data, recognised by the Charter of Fundamental Rights of the European Union ('the Charter'), which resulted from the general obligation to retain traffic and location data laid down by that directive was not limited to what was strictly necessary. In the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970), the Court then interpreted Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) ('the directive on privacy and electronic communications'). That article empowers the Member States – on grounds of the protection, inter alia, of national security – to adopt 'legislative measures' intended to restrict the scope of certain rights and obligations provided for in the directive. Lastly, in the judgment of 2 October 2018, *Ministerio Fiscal* (C-207/16, EU:C:2018:788), the Court interpreted Article 15(1) of that directive in a case which concerned public authorities' access to data relating to the civil identity of users of electronic communications systems.

which the Court held, inter alia, that Member States could not require providers of electronic communications services to retain traffic and location data in a general and indiscriminate way, has caused concerns on the part of certain States that they may have been deprived of an instrument which they consider necessary to safeguard national security and to combat crime.

It is against that background that proceedings were brought before the Investigatory Powers Tribunal (United Kingdom) (*Privacy International*, C-623/17), the Conseil d'État (Council of State, France) (*La Quadrature du Net and Others*, Joined Cases C-511/18 and C-512/18) and the Cour constitutionnelle (Constitutional Court, Belgium) (*Ordre des barreaux francophones et germanophone and Others*, C-520/18) concerning the lawfulness of legislation adopted by certain Member States in those fields, imposing in particular an obligation on providers of electronic communications services to forward users' traffic and location data to a public authority or to retain such data in a general or indiscriminate way.

By two Grand Chamber judgments delivered on 6 October 2020, the Court rules, first of all, that the directive on privacy and electronic communications is applicable to national legislation requiring providers of electronic communications services to carry out personal data processing operations, such as the transmission of that data to public authorities or its retention, for the purposes of safeguarding national security and combating crime. In addition, while confirming its case-law stemming from the judgment in *Tele2 Sverige and Watson and Others*, concerning the disproportionate nature of general and indiscriminate retention of traffic and location data, the Court provides clarification, inter alia, as to the scope of the powers conferred on the Member States by that directive in the field of the retention of such data for the purposes mentioned above.

First of all, the Court takes care to dispel the doubts raised in the present cases as to the applicability of the directive on privacy and electronic communications. Several Member States that submitted written observations to the Court differ in their opinions in that regard. They contended, inter alia, that the directive does not apply to the national legislation at issue, as the purpose of that legislation is to safeguard national security, which is the sole responsibility of the Member States, as attested to by, in particular, the third sentence of Article 4(2) TEU. The Court considers, however, that national legislation requiring providers of electronic communications services to retain traffic and location data or to forward that data to the national security and intelligence authorities for that purpose falls within the scope of that directive.

Next, the Court recalls that the directive on privacy and electronic communications [38] does not permit the exception to the obligation of principle to ensure the confidentiality of electronic communications and the related data and to the prohibition on storage of

[38] Article 15(1) and (3) of Directive 2002/58.

such data to become the rule. This means that the directive does not authorise the Member States to adopt, inter alia for the purposes of national security, legislative measures intended to restrict the scope of rights and obligations provided for in that directive, in particular the obligation to ensure the confidentiality of communications and traffic data [39], unless such measures comply with the general principles of EU law, including the principle of proportionality, and the fundamental rights guaranteed by the Charter. [40]

In that context, the Court holds, first, in the *Privacy International* case, that the directive on privacy and electronic communications, read in the light of the Charter, precludes national legislation requiring providers of electronic communications services to carry out the general and indiscriminate transmission of traffic and location data to the security and intelligence agencies for the purpose of safeguarding national security. Second, in Joined Cases *La Quadrature du Net and Others* and in *Ordre des barreaux francophones et germanophone and Others*, the Court finds that the directive precludes legislative measures requiring providers of electronic communications services to carry out the general and indiscriminate retention of traffic and location data as a preventive measure. Those obligations to forward and to retain such data in a general and indiscriminate way constitute particularly serious interferences with the fundamental rights guaranteed by the Charter, where there is no link between the conduct of the persons whose data is affected and the objective pursued by the legislation at issue. Similarly, the Court interprets Article 23(1) of the General Data Protection Regulation, [41] read in the light of the Charter, as precluding national legislation requiring providers of access to online public communication services and hosting service providers to retain, generally and indiscriminately, inter alia, personal data relating to those services.

By contrast, the Court holds that, in situations where the Member State concerned is facing a serious threat to national security that is shown to be genuine and present or foreseeable, the directive on privacy and electronic communications, read in the light of the Charter, does not preclude recourse to an order requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data. In that context, the Court specifies that the decision imposing such an order, for a period that is limited in time to what is strictly necessary, must be subject to effective review either by a court or by an independent administrative body whose decision is binding, in order to verify that one of those situations exists and that the conditions and safeguards laid down are observed. In those circumstances, that directive also does not preclude the automated analysis of the data, inter alia traffic and location data, of all users of means of electronic communication.

---

39 Article 5(1) of Directive 2002/58.

40 In particular, Articles 7, 8 and 11 and Article 52(1) of the Charter.

41 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1).

The Court adds that the directive on privacy and electronic communications, read in the light of the Charter, does not preclude legislative measures that allow recourse to the targeted retention, limited in time to what is strictly necessary, of traffic and location data, which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion. Likewise, that directive does not preclude legislative measures that provide for the general and indiscriminate retention of IP addresses assigned to the source of a communication, provided that the retention period is limited to what is strictly necessary, or measures that provide for such retention of data relating to the civil identity of users of electronic communications systems, the Member States not being required in the latter case to limit the retention period. Moreover, that directive does not preclude a legislative measure that allows recourse to the expedited retention of data available to service providers, where situations arise in which it becomes necessary to retain that data beyond statutory data retention periods in order to shed light on serious criminal offences or acts adversely affecting national security, where such offences or acts have already been established or where their existence may reasonably be suspected.

In addition, the Court rules that the directive on privacy and electronic communications, read in the light of the Charter, does not preclude national legislation which requires providers of electronic communications services to have recourse to real-time collection, inter alia, of traffic and location data, where that collection is limited to persons in respect of whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities and is subject to a prior review carried out either by a court or by an independent administrative body whose decision is binding, to ensure that such real-time collection is authorised only within the limits of what is strictly necessary. In urgent cases, the review must take place promptly.

Last, the Court addresses the issue of maintaining the temporal effects of national legislation held to be incompatible with EU law. In that regard, it rules that a national court may not apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality which it is bound to make in respect of national legislation imposing on providers of electronic communications services an obligation requiring the general and indiscriminate retention of traffic and location data that is incompatible with the directive on privacy and electronic communications, read in the light of the Charter.

That being said, in order to give a useful answer to the referring court, the Court of Justice recalls that, as EU law currently stands, it is for national law alone to determine the rules relating to the admissibility and assessment, in criminal proceedings against persons suspected of having committed serious criminal offences, of evidence obtained by the retention of data in breach of EU law. However, the Court specifies that the directive on privacy and electronic communications, interpreted in the light of the principle of effectiveness, requires national criminal courts to disregard evidence obtained by means of the general and indiscriminate retention of traffic and location

data in breach of EU law, in the context of such criminal proceedings, where those persons suspected of having committed criminal offences are not in a position to comment effectively on that evidence.

Judgment of 5 April 2022 (Grand Chamber),* Commissioner of An Garda Síochána and Others *(C-140/20, EU:C:2022:258)

In this case, the request for a preliminary ruling was submitted by the Supreme Court (Ireland) in the context of civil proceedings brought by a person sentenced to life imprisonment for a murder committed in Ireland. That person challenged the compatibility with EU law of certain provisions of national law on the retention of data generated in the context of electronic communications. [42] Pursuant to that law, [43] traffic and location data relating to the telephone calls of the person charged had been retained by providers of electronic communications services and made accessible to the police authorities. The referring court's doubts related in particular to the compatibility with the Directive on privacy and electronic communications, [44] read in the light of the Charter, [45] of a system of the general and indiscriminate retention of those data, in connection with combating serious crime.

In its judgment, the Court, sitting as the Grand Chamber, confirms, while also providing detail as to its scope, the case-law resulting from the judgment in *La Quadrature du Net and Others* by recalling that the general and indiscriminate retention of traffic and location data relating to electronic communications is not permitted for the purposes of combating serious crime and preventing serious threats to public security. It also confirms the case-law resulting from the judgment in *Prokuratuur (Conditions of access to data relating to electronic communications)*, [46] in particular as regards the obligation to make access by the competent national authorities to those retained data subject to a prior review carried out either by a court or by an administrative body that is independent in relation to a police officer.

The Court holds, in the first place, that the Directive on privacy and electronic communications, read in the light of the Charter, precludes legislative measures which, as a preventive measure, for the purposes of combating serious crime and preventing serious threats to public security, provide for the general and indiscriminate retention of traffic and location data. Having regard, first, to the dissuasive effect on the exercise of the fundamental rights [47] which is liable to result from the retention of those data, and,

---

42 Communications (Retention of Data) Act 2011. That law was adopted in order to transpose into Irish law Directive 2006/24 of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

43 The law permits, for reasons going beyond those inherent to the protection of national security, the preventative, general and indiscriminate retention of traffic and location data of all subscribers for a period of two years.

44 More specifically, Article 15(1) of Directive 2002/58.

45 In particular, Articles 7, 8, 11 and Article 52(1) of the Charter.

46 Judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152).

47 Enshrined in Articles 7 to 11 of the Charter.

second, to the seriousness of the interference entailed by such retention, it is necessary for that retention to be the exception and not the rule in the system established by that directive, such that those data should not be retained systematically and continuously.

Crime, even particularly serious crime, cannot be treated in the same way as a threat to national security, since to treat those situations in the same way would be likely to create an intermediate category between national security and public security for the purpose of applying to the latter the requirements inherent in the former.

However, the Directive on privacy and electronic communications, read in the light of the Charter, does not preclude legislative measures which provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended. It adds that such a retention measure covering places or infrastructures that regularly receive a very high volume of visitors, or strategic locations, such as airports, stations, maritime ports or tollbooth areas, may allow the competent authorities to obtain information as to the presence in those places or geographical areas of persons using a means of electronic communication within those areas and to draw conclusions as to their presence and activity in those places or geographical areas for the purposes of combating serious crime. In any event, the fact that it may be difficult to provide a detailed definition of the circumstances and conditions under which targeted retention may be carried out is no reason for the Member States, by turning the exception into a rule, to provide for the general retention of traffic and location data.

That directive, read in the light of the Charter, also does not preclude legislative measures that provide, for the same purposes, for the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary, as well as data relating to the civil identity of users of electronic communications systems. As regards that latter aspect, the Court holds more specifically that neither the Directive on privacy and electronic communications nor any other act of EU law precludes national legislation, which has the purpose of combating serious crime, pursuant to which the purchase of a means of electronic communication, such as a pre-paid SIM card, is subject to a check of official documents establishing the purchaser's identity and the registration, by the seller, of that information, with the seller being required, should the case arise, to give access to that information to the competent national authorities.

The same is the case for legislative measures which allow, also for the purposes of combating serious crime and preventing serious threats to public security, recourse to an instruction requiring providers of electronic communications services by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention (*quick freeze*) of traffic

and location data in their possession. Only actions to combat serious crime and, *a fortiori*, to safeguard national security are such as to justify that retention, on the condition that the measure and access to the retained data comply with the limits of what is strictly necessary. The Court recalls that such a retention measure may be extended to traffic and location data relating to persons other than those who are suspected of having planned or committed a serious criminal offence or acts adversely affecting national security, provided that those data can, on the basis of objective and non-discriminatory factors, shed light on such an offence or acts adversely affecting national security, such as data concerning the victim thereof, and his or her social or professional circle.

However, the Court indicates next that all the abovementioned legislative measures must ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against risks of abuse. The various measures for the retention of traffic and location data may, at the choice of the national legislature and subject to the limits of what is strictly necessary, be applied concurrently.

In addition, the Court states that to authorise, for the purposes of combating serious crime, access to those data retained generally and indiscriminately in order to address a serious threat to national security would be contrary to the hierarchy of objectives of public interest which may justify a measure taken pursuant to the Directive on privacy and electronic communications. [48] That would be to allow access to be justified for an objective of lesser importance than that which justified its retention, namely the safeguarding of national security, which would risk depriving of any effectiveness the prohibition on a general and indiscriminate retention for the purpose of combating serious crime.

In the second place, the Court holds that the Directive on privacy and electronic communications, read in the light of the Charter, precludes national legislation pursuant to which the centralised processing of requests for access to data retained by providers of electronic communications services, issued by the police in the context of the investigation or prosecution of serious criminal offences, is the responsibility of a police officer, who is assisted by a unit established within the police service which enjoys a degree of autonomy in the exercise of its duties, and whose decisions may subsequently be subject to judicial review. First, such a police officer does not fulfil the requirements of independence and impartiality which must be met by an administrative body carrying out the prior review of requests for access issued by the competent national authorities, as he or she does not have the status of a third party in relation to those authorities. Second, while the decision of that officer may be subject to subsequent judicial review,

[48] That hierarchy is set out in the case-law of the Court, and in particular in the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), paragraphs 135 and 136. Under that hierarchy, combating serious crime is of lesser importance than safeguarding national security.

that review cannot be substituted for a review which is independent and, except in duly justified urgent cases, undertaken beforehand.

In the third place, lastly, the Court confirms its case-law according to which EU law precludes a national court from limiting the temporal effects of a declaration of invalidity which, pursuant to national law, it is bound to make as regards national legislation requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data, owing to the incompatibility of that legislation with the Directive on privacy and electronic communications. However, the Court recalls that the admissibility of evidence obtained by means of such retention is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.

Judgment of 20 September 2022 (Grand Chamber),* SpaceNet and Telekom Deutschland *(C-793/19 and C-794/19, EU:C:2022:702)

In the present joined cases, two requests for a preliminary ruling were submitted by the Bundesverwaltungsgericht (Federal Administrative Court, Germany), before which the Federal Republic of Germany brought an appeal on a point of law against two judgments which had upheld the actions brought by two companies providing internet access services, *SpaceNet AG* (Case C-793/19) and *Telekom Deutschland GmbH* (Case C-794/19). By those actions, those companies challenged the obligation imposed by the German legislation [49] to retain traffic and location data relating to their customers' electronic communications.

The doubts expressed by the referring court concern, inter alia, the compatibility with the Directive on privacy and electronic communications, [50] read in the light of the Charter of Fundamental Rights of the European Union ('the Charter') [51] and of Article 4(2) TEU, of national legislation which requires providers of publicly available electronic communications services – inter alia for the purposes of prosecuting serious criminal offences or preventing a specific risk to national security – to retain, in a general and indiscriminate way, most of the traffic and location data of the end users of those services, laying down a retention period of several weeks and rules intended to ensure the effective protection of the retained data against the risks of abuse and against any unlawful access to those data.

By its judgment, the Court, sitting as a Grand Chamber, confirms its case-law arising from *La Quadrature du Net and Others*, and, more recently, the judgment in *Commissioner*

[49] Combined provisions of Paragraph 113a(1) and Paragraph 113b of the Telekommunikationsgesetz (Law on telecommunications) of 22 June 2004 (BGBl. 2004 I, p. 1190), in the version applicable to the dispute in the main proceedings.

[50] More specifically, Article 15(1) of Directive 2002/58.

[51] Articles 6 to 8, 11 and Article 52(1) of the Charter.

of An Garda Síochána and Others, [52] and clarifies the scope of that case-law. It recalls inter alia that the general and indiscriminate retention of traffic and location data relating to electronic communications is not permitted, on a preventative basis, for the purposes of combating serious crime and preventing serious threats to public security.

The Court begins by confirming the applicability of the Directive on privacy and electronic communications to the national legislation at issue, and then recalls the principles derived from its case-law, before carrying out a detailed examination of the characteristics of the national legislation at issue, highlighted by the referring court.

As regards, first of all, the extent of the data retained, the Court observes that the retention obligation laid down by the national legislation at issue covers a very broad set of traffic and location data and that it concerns practically the entire population without those persons being, even indirectly, in a situation liable to give rise to criminal prosecutions. It also notes that that legislation requires the general retention, without a reason, and without any distinction in terms of personal, temporal or geographical factors, of most traffic and location data, the scope of which corresponds, in essence, to that of the data retained in the cases which led to the judgment in *La Quadrature du net and Others*. Accordingly, in the light of that case-law, the Court considers that a data retention obligation such as that at issue in the main proceedings cannot be regarded as a targeted retention of data.

Next, as regards the data retention period, the Court notes that it is follows from the Directive on privacy and electronic communications [53] that the length of the retention period provided for by a national measure imposing a general and indiscriminate retention obligation is indeed a relevant factor, amongst others, in determining whether EU law precludes such a measure, since that sentence requires that that period be 'limited'. However, the seriousness of the interference stems from the risk, particularly in view of their number and variety, that the data retained, taken as a whole, may enable very precise conclusions to be drawn concerning the private life of the person or persons whose data have been retained and, in particular, provide the means of establishing a profile of the person or persons concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications. Accordingly, the retention of traffic or location data is in any event serious regardless of the length of the retention period and the quantity or nature of the data retained, when that set of data is liable to allow precise conclusions to be drawn concerning the private life of the person or persons concerned. [54]

Lastly, as regards the safeguards intended to protect the retained data against the risks of abuse and against any unlawful access, the Court points out, on the basis of its previous case-law, that the retention of and access to those data each constitute

[52] Judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others* (C-140/20, EU:C:2022:258).
[53] More specifically, from the second sentence of Article 15(1) of Directive 2002/58.
[54] See, as regards access to such data, judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152, paragraph 39).

separate interferences with the fundamental rights of the persons concerned, requiring a separate justification. It follows that national legislation ensuring full respect for the conditions established by the case-law as regards access to retained data cannot, by its very nature, be capable of either limiting or even remedying the serious interference with the rights of the persons concerned which results from the general retention of those data.

In addition, in order to respond to certain arguments raised before it, the Court notes, in the first place, that a threat to national security must be genuine and present, or, at the very least, foreseeable, which presupposes that sufficiently concrete circumstances have arisen to be able to justify a generalised and indiscriminate measure of retention of traffic and location data for a limited period of time. Such a threat is therefore distinguishable, by its nature, its seriousness, and the specific nature of the circumstances of which it is constituted, from the general and permanent risk of the occurrence of tensions or disturbances, even of a serious nature, that affect public security, or from that of serious criminal offences being committed. Thus, crime, even of a particularly serious nature, cannot be treated in the same way as a threat to national security.

It observes, in the second place, that authorising access, for the purpose of combating serious crime, to traffic and location data which have been retained in a general and indiscriminate way in order to confront a serious threat to national security, would be contrary to the hierarchy of public interest objectives which may justify a measure adopted under the Directive on privacy and electronic communications. [55] That would amount to allowing access to be justified for an objective of lesser importance than that which justified its retention, namely the safeguarding of national security, which would risk depriving of any effectiveness the prohibition on a general and indiscriminate retention for the purpose of combating serious crime.

The Court concludes, confirming its previous case-law, that the Directive on privacy and electronic communications, read in the light of the Charter, precludes national legislative measures which provide, on a preventative basis, for the purposes of combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of traffic and location data.

However, it does not preclude national legislative measures which allow, for the purposes of safeguarding national security, recourse to an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable. In that regard, the Court specifies that the decision imposing such an instruction must be subject to effective review, either by a court or by

[55] That hierarchy is set out in the case-law of the Court, in particular in *La Quadrature du Net and Others*, in paragraphs 135 and 136. In that hierarchy, combating serious crime is of lesser importance than safeguarding national security.

an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists.

That directive, read in the light of the Charter, also does not preclude national legislative measures providing, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended.

The same is true of national legislative measures providing, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of IP addresses assigned to the source of an internet connection, for a period that is limited in time to what is strictly necessary, and data relating to the civil identity of users of electronic communications systems, the retention of which may undisputedly contribute to the fight against serious crime, to the extent that those data make it possible to identify persons who have used those means in the context of planning or committing an act constituting serious crime.

That is also the case for national legislative measures that allow, for the purposes of combating serious crime and, *a fortiori*, safeguarding national security, recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers.

However, the Court states that all the abovementioned measures must ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse. Those various measures may, at the choice of the national legislature and subject to the limits of what is strictly necessary, be applied concurrently.

Judgment of 15 June 2021 (Grand Chamber),* Facebook Ireland and Others *(C-645/19, EU:C:2021:483)

On 11 September 2015, the President of the Belgian Privacy Commission ('the Privacy Commission') brought an action before the Nederlandstalige rechtbank van eerste aanleg Brussel (Dutch-language Court of First Instance, Brussels, Belgium), seeking an injunction against Facebook Ireland, Facebook Inc. and Facebook Belgium, aiming to put

an end to alleged infringements of data protection laws by Facebook. Those infringements consisted, inter alia, of the collection and use of information on the browsing behaviour of Belgian internet users, whether or not they were Facebook account holders, by means of various technologies, such as cookies, social plug-ins [56] or pixels.

On 16 February 2018, that court held that it had jurisdiction to give a ruling on that action and, on the substance, held that the Facebook social network had not adequately informed Belgian internet users of the collection and use of the information concerned. Further, the consent given by the internet users to the collection and processing of that data was held to be invalid.

On 2 March 2018, Facebook Ireland, Facebook Inc. and Facebook Belgium brought an appeal against that judgment before the Hof van beroep te Brussel (Court of Appeal, Brussels, Belgium), the referring court in the present case. Before that court, the Belgian Data Protection Authority ('the DPA') acted as the legal successor of the President of the Privacy Commission. The referring court held that it solely has jurisdiction to give a ruling on the appeal brought by Facebook Belgium.

The referring court was uncertain as to the effect of the application of the 'one-stop shop' mechanism provided for by the General Data Protection Regulation [57] on the competences of the DPA and, in particular, as to whether, with respect to the facts subsequent to the date of entry into force of the GDPR, namely 25 May 2018, the DPA may bring an action against Facebook Belgium, since it is Facebook Ireland which has been identified as the controller of the data concerned. Since that date, and in particular under the 'one-stop shop' rule laid down by the GDPR, only the Data Protection Commissioner (Ireland) is competent to bring injunction proceedings, subject to review by the Irish courts.

In its Grand Chamber judgment, the Court of Justice specifies the powers of national supervisory authorities within the scheme of the GDPR. Thus, it considers, inter alia, that that regulation authorises, under certain conditions, a supervisory authority of a Member State to exercise its power to bring any alleged infringement of the GDPR before a court of that State and to initiate or engage in legal proceedings in relation to an instance of cross-border data processing, [58] although that authority is not the lead supervisory authority with regard to that processing.

In the first place, the Court specifies the conditions governing whether a national supervisory authority, which does not have the status of lead supervisory authority in

---

[56] For example, the 'Like' or 'Share' buttons.

[57] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1) ('the GDPR'). Under Article 56(1) of the GDPR: 'Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor'.

[58] Within the meaning of Article 4(23) of the GDPR.

relation to an instance of cross-border processing, must exercise its power to bring any alleged infringement of the GDPR before a court of a Member State and, where necessary, to initiate or engage in legal proceedings in order to ensure the application of that regulation. Thus, the GDPR must confer on that supervisory authority a competence to adopt a decision finding that that processing infringes the rules laid down by that regulation and, in addition, that power must be exercised with due regard to the cooperation and consistency procedures provided for by that regulation. [59]

With respect to cross-border processing, the GDPR provides for the 'one-stop shop' mechanism, [60] which is based on an allocation of competences between one 'lead supervisory authority' and the other national supervisory authorities concerned. That mechanism requires close, sincere and effective cooperation between those authorities in order to ensure consistent and homogeneous protection of the rules for the protection of personal data, and thus preserve its effectiveness. As a general rule, the GDPR guarantees in this respect the competence of the lead supervisory authority for the adoption of a decision finding that an instance of cross-border processing is an infringement of the rules laid down by that regulation, [61] whereas the competence of the other supervisory authorities concerned for the adoption of such a decision, even provisionally, constitutes the exception to the rule. [62] However, in the exercise of its competences, the lead supervisory authority cannot eschew essential dialogue and sincere and effective cooperation with the other supervisory authorities concerned. Accordingly, in the context of that cooperation, the lead supervisory authority may not ignore the views of the other supervisory authorities concerned, and any relevant and reasoned objection made by one of the other supervisory authorities has the effect of blocking, at least temporarily, the adoption of the draft decision of the lead supervisory authority.

The Court also adds that the fact that a supervisory authority of a Member State which is not the lead supervisory authority with respect to an instance of cross-border data processing may exercise the power to bring any alleged infringement of the GDPR before a court of that State and to initiate or engage in legal proceedings only when that exercise complies with the rules on the allocation of competences between the lead supervisory authority and the other supervisory authorities [63] is compatible with Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, which guarantee data subjects the right to the protection of his or her personal data and the right to an effective remedy, respectively.

In the second place, the Court holds that, in the case of cross-border data processing, it is not a prerequisite for the exercise of the power of a supervisory authority of a

[59] Laid down in Articles 56 and 60 of the GDPR.
[60] Article 56(1) of the GDPR.
[61] Article 60(7) of the GDPR.
[62] Article 56(2) and Article 66 of the GDPR set out exceptions to the general rule that it is the lead supervisory authority that is competent to adopt such decisions.
[63] Laid down in Articles 55 and 56, read together with Article 60 of the GDPR.

Member State, other than the lead supervisory authority, to initiate or engage in legal proceedings [64] that the controller or the processor with respect to the cross-border processing of personal data to which that action relates has a main establishment or another establishment on the territory of that Member State. However, the exercise of that power must fall within the territorial scope of the GDPR, [65] which presupposes that the controller or the processor with respect to the cross-border processing has an establishment in the European Union.

In the third place, the Court rules that, in the event of cross-border data processing, the power of a supervisory authority of a Member State, other than the lead supervisory authority, to bring any alleged infringement of the GDPR before a court of that Member State and, where appropriate, to initiate or engage in legal proceedings, may be exercised both with respect to the main establishment of the controller which is located in that authority's own Member State and with respect to another establishment of that controller, provided that the object of the legal proceedings is a processing of data carried out in the context of the activities of that establishment and that that authority is competent to exercise that power.

However, the Court adds that the exercise of that power presupposes that the GDPR is applicable. In this instance, since the activities of the establishment of the Facebook group located in Belgium are inextricably linked to the processing of personal data at issue in the main proceedings, with respect to which Facebook Ireland is the controller within the European Union, that processing is carried out 'in the context of the activities of an establishment of the controller' and, therefore, does fall within the scope of the GDPR.

In the fourth place, the Court holds that, where a supervisory authority of a Member State which is not the 'lead supervisory authority' brought, before the date of entry into force of the GDPR, legal proceedings concerning an instance of cross-border processing of personal data, that action may be continued, under EU law, on the basis of the provisions of the Data Protection Directive, [66] which remains applicable in relation to infringements of the rules laid down in that directive committed up to the date when that directive was repealed. In addition, that action may be brought by that authority with respect to infringements committed after the date of entry into force of the GDPR, provided that that action is brought in one of the situations where, exceptionally, that regulation confers on that authority a competence to adopt a decision finding that the processing of data in question is in breach of the rules laid down by that regulation, and that the cooperation and consistency procedures provided for by the regulation are respected.

---

64 Pursuant to Article 58(5) of the GDPR.

65 Article 3(1) of the GDPR provides that that regulation is applicable to the processing of personal data 'in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not'.

66 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).

In the fifth and last place, the Court recognises the direct effect of the provision of the GDPR under which each Member State is to provide by law that its supervisory authority is to have the power to bring infringements of that regulation to the attention of the judicial authorities and, where appropriate, to initiate or engage otherwise in legal proceedings. Consequently, such an authority may rely on that provision in order to bring or continue a legal action against private parties, even where it has not been specifically implemented in the legislation of the Member State concerned.

Judgment of 30 April 2024 (Full Court*), La Quadrature du Net and Others (Personal data and action to combat counterfeiting) *(C-470/21, EU:C:2024:370)

In recent years, the Court of Justice has been called upon, on several occasions, to rule on the retention of and access to personal data in the field of electronic communications and has consequently established an extensive body of case-law in this area. [67] Ruling on a preliminary ruling from the Conseil d'État (Council of State, France), the Court, sitting as the full Court, develops that case-law by providing clarifications concerning (i) the conditions under which the general retention of IP addresses by providers of electronic communications services cannot be regarded as entailing a serious interference with the rights to respect for private life, to the protection of personal data and to freedom of expression guaranteed by the Charter [68] and (ii) the possibility, for a public authority, to access certain personal data retained in accordance with those conditions, in the context of combating infringements of intellectual property rights committed online.

In the present case, four associations submitted a request to the Premier ministre (Prime Minister, France) seeking the repeal of the decree relating to the automated processing of personal data. [69] As that request was not acted upon, those associations brought an action before the Conseil d'État (Council of State) seeking the annulment of that implicit rejection decision. In their view, that decree and the provisions which constitute its legal basis [70] infringe EU law.

Under French law, the Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (High Authority for the dissemination of works and the protection of rights on the internet) ('Hadopi') is authorised – in order to be able to identify those

---

[67] See, inter alia, judgments of 21 December 2016, *Tele2 Sverige et Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970), of 2 October 2018, *Ministerio Fiscal* (C-207/16, EU:C:2018:788), of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791), of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152), of 17 June 2021, *M.I.C.M.* (C-597/19, EU:C:2021:492), and of 5 April 2022, *Commissioner of An Garda Síochána and Others* (C-140/20, EU:C:2022:258).

[68] Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union ('the Charter').

[69] Décret no 2010-236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur internet » (Decree No 2010-236 of 5 March 2010 on the automated personal data processing system authorised by Article L. 331-29 of the code de la propriété intellectuelle (Intellectual Property Code), known as the 'System for the management of measures for the protection of works on the internet' (JORF No 56 of 7 March 2010, text No 19), as amended by décret no 2017-924, du 6 mai 2017, relatif à la gestion des droits d'auteur et des droits voisins par un organisme de gestion de droits et modifiant le code de la propriété intellectuelle (Decree No 2017-924 of 6 May 2017 on the management of copyright and related rights by a rights management organisation and amending the Intellectual Property Code) (JORF No 109 of 10 May 2017, text No 176).

[70] In particular, the third to fifth paragraphs of Article L. 331-21 of the Intellectual Property Code.

responsible for infringements of copyright or related rights committed online – to access certain data that providers of electronic communications services are required to retain. Those data relate to the civil identity of a person concerned associated with his or her IP address previously collected by rightholder organisations. Once the holder of the IP address used for activities constituting such infringements is identified, Hadopi follows the 'graduated response' procedure. Specifically, it is empowered to send that person two recommendations, which are similar to warnings, and, if the activities persist, a letter notifying him or her that those activities are subject to criminal prosecution. Finally, it is entitled to refer the matter to the public prosecution service with a view to the prosecution of that person. [71]

In that context, the Conseil d'État (Council of State) referred questions to the Court concerning the interpretation of the ePrivacy Directive, read in the light of the Charter. [72]

In the first place, as regards the retention of data relating to civil identity and the associated IP addresses, the Court states that the general and indiscriminate retention of IP addresses does not necessarily constitute, in every case, a serious interference with the rights to respect for private life, protection of personal data and freedom of expression guaranteed by the Charter.

The obligation to ensure such retention may be justified by the objective of combating criminal offences in general, where it is genuinely ruled out that that retention could give rise to serious interferences with the private life of the person concerned due to the possibility of drawing precise conclusions about that person by, inter alia, linking those IP addresses with a set of traffic or location data.

Accordingly, a Member State which intends to impose such an obligation on providers of electronic communications services must ensure that the arrangements for the retention of those data are such as to rule out the possibility that precise conclusions could be drawn about the private lives of the persons concerned.

The Court specifies that, to that end, the retention arrangements must relate to the very manner in which the retention is structured; in essence, that retention must be organised in such a way as to guarantee a genuinely watertight separation of the different categories of data retained. Accordingly, the national rules relating to those arrangements must ensure that each category of data, including data relating to civil identity and IP addresses, is kept completely separate from other categories of retained data and that that separation is genuinely watertight, by means of a secure and reliable computer system. In addition, in so far as those rules provide for the possibility of

---

71 With effect from 1 January 2022, Hadopi was merged with the Conseil supérieur de l'audiovisuel (Higher Council for the audiovisual sector) (CSA), another independent public authority, to form the Autorité de régulation de la communication audiovisuelle et numérique (Authority for the Regulation of Audiovisual and Digital Communications) (ARCOM). The graduated response procedure has, however, remained essentially unchanged.

72 Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) ('the ePrivacy Directive'), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.

linking the retained IP addresses with the civil identity of the person concerned for the purpose of combating infringements, they must permit such linking only through the use of an effective technical process which does not undermine the effectiveness of the watertight separation of those categories of data. The reliability of that separation must be subject to regular review by a third-party public authority. In so far as the applicable national legislation provides for such strict requirements, the interference resulting from that retention of IP addresses cannot be categorised as 'serious'.

Consequently, the Court concludes that, in the presence of a legislative framework ensuring that no combination of data will allow precise conclusions to be drawn about the private life of the persons whose data are retained, the ePrivacy Directive, read in the light of the Charter, does not preclude a Member State from imposing an obligation to retain IP addresses, in a general and indiscriminate manner, for a period not exceeding what is strictly necessary, for the purposes of combating criminal offences in general.

In the second place, as regards access to data relating to the civil identity associated with IP addresses, the Court holds that the ePrivacy Directive, read in the light of the Charter, does not preclude, in principle, national legislation which allows a public authority to access those data retained by providers of electronic communications services separately and in a genuinely watertight manner, for the sole purpose of enabling that authority to identify the holders of those addresses suspected of being responsible for infringements of copyright and related rights on the internet and to take measures against them. In that case, the national legislation must prohibit the officials having such access (i) from disclosing in any form whatsoever information concerning the content of the files consulted by those holders except for the sole purpose of referring the matter to the public prosecution service, (ii) from tracking in any way the clickstream of those holders and (iii) from using those IP addresses for purposes other than the adoption of those measures.

In that context, the Court notes inter alia that, even though the freedom of expression and the confidentiality of personal data are primary considerations, those fundamental rights are nevertheless not absolute. In balancing the rights and interests at issue, those fundamental rights must yield on occasion to other fundamental rights or public-interest imperatives, such as the maintenance of public order and the prevention of crime or the protection of the rights and freedoms of others. This is, in particular, the case where the weight given to those primary considerations is such as to hinder the effectiveness of a criminal investigation, in particular by making it impossible or excessively difficult to identify effectively the perpetrator of a criminal offence and to impose a penalty on him or her.

In the same context, the Court also refers to its case-law according to which, as regards the combating of criminal offences infringing copyright or related rights committed online, the fact that accessing IP addresses may be the only means of investigation enabling the person concerned to be identified tends to show that the retention of and

access to those addresses is strictly necessary for the attainment of the objective pursued and therefore meets the requirement of proportionality. Moreover, not to allow such access would carry a real risk of systemic impunity for criminal offences committed online or the commission or preparation of which is facilitated by the specific characteristics of the internet. The existence of such a risk constitutes a relevant factor for the purposes of assessing, when balancing the various rights and interests in question, whether an interference with the rights to respect for private life, protection of personal data and freedom of expression is a proportionate measure in the light of the objective of combating criminal offences.

In the third place, ruling on whether access by the public authority to data relating to the civil identity associated with an IP address must be subject to a prior review by a court or an independent administrative body, the Court considers that the requirement of such prior review applies where, within the framework of national legislation, that access carries the risk of a serious interference with the fundamental rights of the person concerned in that it could allow that public authority to draw precise conclusions about the private life of that person and, as the case may be, to establish a detailed profile of that person. Conversely, that requirement of prior review is not intended to apply where the interference with fundamental rights cannot be classified as serious.

In that regard, the Court states that, where a retention framework which ensures a watertight separation of the various categories of retained data is put in place, access by the public authority to the data relating to the civil identity associated with the IP addresses is not, in principle, subject to the requirement of a prior review. Such access for the sole purpose of identifying the holder of an IP address does not, as a general rule, constitute a serious interference with the abovementioned rights.

However, the Court does not rule out the possibility that, in atypical situations, there is a risk that, in the context of a procedure such as the graduated response procedure at issue in the main proceedings, the public authority may be able to draw precise conclusions about the private life of the person concerned, in particular where that person engages in activities infringing copyright or related rights on peer-to-peer networks repeatedly, or on a large scale, in connection with protected works of particular types, revealing potentially sensitive information about aspects of that person's private life.

In the present case, an IP address holder may be particularly exposed to such a risk when the public authority must decide whether or not to refer the matter to the public prosecution service with a view to the prosecution of that person. The intensity of the infringement of the right to respect for private life is likely to increase as the graduated response procedure, which is a sequential process, progresses through its various stages. The access of the competent authority to all of the data relating to the person concerned collected during the various stages of that procedure may enable precise conclusions to be drawn about the private life of that person. Accordingly, the national legislation must provide for a prior review which must take place before the public

authority can link the civil identity data and such a set of data, and before sending a notification letter declaring that that person has engaged in conduct subject to criminal prosecution. That review must, moreover, preserve the effectiveness of the graduated response procedure by making it possible, in particular, to identify cases where the unlawful conduct in question has been again repeated. To that end, that procedure must be organised and structured in such a way that the civil identity data of a person associated with IP addresses previously collected on the internet cannot automatically be linked, by the persons responsible for the examination of the facts within the competent public authority, with information which the latter already has and which could enable precise conclusions to be drawn about the private life of that person.

Furthermore, as regards the object of the prior review, the Court notes that, where the person concerned is suspected of having committed an offence which falls within the scope of criminal offences in general, the court or independent administrative body responsible for that review must refuse access where that access would allow the public authority to draw precise conclusions about the private life of that person. However, even access allowing such precise conclusions to be drawn should be authorised in cases where the person concerned is suspected of having committed an offence considered by the Member State concerned to undermine a fundamental interest of society and which thus constitutes a serious crime.

The Court also states that a prior review may in no case be entirely automated since, in the case of a criminal investigation, such a review requires that a balance be struck between, on the one hand, the legitimate interests relating to combating crime and, on the other hand, respect for private life and protection of personal data. That balancing requires the intervention of a natural person, all the more so where the automatic nature and large scale of the data processing in question poses privacy risks.

Thus, the Court concludes that the possibility, for the persons responsible for examining the facts within that public authority, of linking such data relating to the civil identity of a person associated with an IP address with files containing information that reveals the title of protected works the making available of which on the internet justified the collection of IP addresses by rightholder organisations is subject, in cases where the same person again repeats an activity infringing copyright or related rights, to review by a court or an independent administrative body. That review cannot be entirely automated and must take place before any such linking, as such linking is capable, in such circumstances, of enabling precise conclusions to be drawn about the private life of the person whose IP address has been used for activities that may infringe copyright or related rights.

In the fourth and last place, the Court notes that the data processing system used by the public authority must be subject, at regular intervals, to a review by an independent body acting as a third party in relation to that public authority. The purpose of that control is to verify the integrity of the system, including the effective safeguards against

the risks of abusive or unlawful access to or use of those data, and its effectiveness and reliability in detecting potential offending conduct.

In that context, the Court observes that, in the present case, the automated processing of personal data carried out by the public authority on the basis of the information relating to instances of counterfeiting detected by the rightholder organisations is likely to involve a certain number of false positives and, above all, the risk that a potentially very significant amount of personal data may be misused by third parties for unlawful or abusive purposes, which explains the need for such a review.

In addition, it adds that that processing must comply with the specific rules for the protection of personal data laid down by Directive 2016/680. [73] In the present case, even if the public authority does not have decision-making powers of its own in the context of the 'graduated response' procedure, it must be classified as a 'public authority' involved in the prevention and detection of criminal offences and therefore falls within the scope of that directive. Thus, the persons involved in such a procedure must enjoy a set of substantive and procedural safeguards referred to in Directive 2016/680; it is for the referring court to ascertain whether the national legislation provides for those safeguards.

5. Copyright

Judgment of 3 July 2012 (Grand Chamber),* UsedSoft *(C-128/11, EU:C:2012:407)

The company Oracle developed and distributed, in particular by downloading from the internet, what is known as 'client-server' software. The customer would download a copy of the software directly to his computer. The user right included the right to store a copy of the program permanently on a server and to allow 25 users to access it. The licence agreements provided that the customer would acquire, for an unlimited period, a non-transferable user right exclusively for internal business purposes. UsedSoft, a German undertaking, marketed licences purchased from customers of Oracle. Customers of UsedSoft not yet in possession of the software would download it directly, after acquiring a 'used' licence from Oracle's website. Customers who already had that software could purchase a further licence or part of a licence for additional users. In those circumstances, customers would download the software to the main memory of the workstation computers of those other users.

[73] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89).

Oracle brought proceedings against UsedSoft before the German courts seeking an order prohibiting that practice. The Bundesgerichtshof (Federal Court of Justice, Germany) asked the Court of Justice to interpret, against that background, Directive 2009/24/EC [74] on the legal protection of computer programs.

According to the Court, Article 4(2) of Directive 2009/24/EC must be interpreted as meaning that the right of distribution of a copy of a computer program is exhausted if the copyright holder who has authorised, even free of charge, the downloading of that copy from the internet onto a data carrier has also conferred, in return for payment of a fee intended to enable him to obtain a remuneration corresponding to the economic value of the copy of the work of which he is the proprietor, a right to use that copy for an unlimited period.

The downloading of a copy of a computer program and the conclusion of a user licence agreement for that copy form an indivisible whole. Those transactions involve a transfer of the right of ownership of the copy of the computer program. It makes no difference whether the copy of the computer program was made available to the customer by means of a download or by means of a material medium such as a CD-ROM or DVD

In addition, Articles 4(2) and 5(1) of Directive 2009/24/EC must be interpreted as meaning that, in the event of the resale of a user licence entailing the resale of a copy of a computer program downloaded from the copyright holder's website, that licence having originally been granted to the first acquirer, the second acquirer of the licence, as well as any subsequent acquirer of it, will be able to rely on the exhaustion of the distribution right under Article 4(2) of that directive and benefit from the right of reproduction

***Judgment of 10 November 2016*, Vereniging Openbare Bibliotheken *(C-174/15*, *EU:C:2016:856*)**

In the Netherlands, the lending of electronic books by public libraries was not covered by the rules on public lending applicable to paper books. Public libraries would make electronic books available to the public via the internet, on the basis of licensing agreements with rightholders. The Vereniging Openbare Bibliotheken, an association representing all public libraries in the Netherlands ('the VOB'), was of the view that the rules applying to paper books should also apply to digital lending. Against that background, it brought proceedings against Stichting Leenrecht, a foundation entrusted with collecting remuneration due to authors, seeking a declaratory judgment to that effect. The VOB's action concerned lending arrangements following the 'one copy, one user' model, namely the lending of a digital copy of a book by placing that copy on the server of a public library and allowing a user to reproduce that copy by downloading it

[74] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (OJ 2009 L 111, p. 16).

onto his own computer, bearing in mind that only one copy may be downloaded during the lending period and that, after that period has expired, the downloaded copy can no longer be used by that user. Proceedings having been brought before it, the Rechtbank Den Haag (District Court, The Hague, Netherlands) asked the Court of Justice whether Articles 1(1), 2(1)(b) and 6(1) of Directive 2006/115/EC [75] on rental right and lending right and on certain rights related to copyright in the field of intellectual property are to be construed as meaning that 'lending' covers the lending of a digital copy of a book and whether that directive precludes such a practice.

The Court held that Articles 1(1), 2(1)(b) and 6(1) of Directive 2006/115/EC must be interpreted as meaning that the concept of 'lending' as referred to in those provisions covers the 'one copy, one user' model.

It is necessary to interpret the concept of 'rental', in Article 2(1) (a) of Directive 2006/115/EC, as referring exclusively to tangible objects and to interpret the concept of 'copies', in Article 1(1) of that directive, as referring, as regards rental, exclusively to copies fixed in a physical medium. That conclusion is, moreover, borne out by the objective pursued by that directive. Recital 4 thereof states, inter alia, that copyright must adapt to new economic developments such as new forms of exploitation.

Furthermore, EU law must be interpreted as not precluding a Member State from making the application of Article 6(1) of Directive 2006/115/EC subject to the condition that the digital copy of a book made available by the public library must have been put into circulation by a first sale or other transfer of ownership of that copy in the European Union by the holder of the right of distribution to the public or with his consent, for the purposes of Article 4(2) of Directive 2001/29/EC. [76] The Member States cannot be prevented from setting, where appropriate, additional conditions such as to improve the protection of authors' rights beyond what is expressly laid down in that provision.

Article 6(1) of Directive 2006/115/EC must be construed as precluding the public lending exception laid down therein from applying to the making available by a public library of a digital copy of a book where that copy was obtained from an unlawful source.

Judgment of 8 September 2016,* GS Media *(C-160/15, EU:C:2016:644)

GS Media operated the website GeenStijl, which was one of the 10 most visited websites in the area of news in the Netherlands. In 2011, GS Media published an article and a hyperlink directing readers to an Australian site where photographs of Ms Dekker had been made available. Those photographs had been published on the Australian site

[75] Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (OJ 2006 L 376, p. 28).

[76] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ 2001 L 167, p. 10).

without the consent of Sanoma, the publisher of the monthly magazine Playboy which held the copyright over the photographs at issue. Despite receiving demands from Sanoma, GS Media refused to remove the hyperlink in question. When the Australian site removed the photographs at Sanoma's request, GeenStijl published a further article which also contained a hyperlink to another site where the photographs at issue could be viewed. That other site also complied with Sanoma's request to remove the photographs. On the GeenStijl forum, users then posted new links to other websites where the photographs could be viewed. Sanoma claimed that GS Media had infringed its copyright. Proceedings having been brought before it, the Hoge Raad der Nederlanden (Supreme Court of the Netherlands) submitted a question to the Court of Justice on that point. Under Directive 2001/29/EC, [77] every act of communication of a work to the public has to be authorised by the copyright holder.

According to the Court, Article 3(1) of Directive 2001/29/EC must be interpreted as meaning that, in order to establish whether the fact of posting, on a website, hyperlinks to protected works, which are freely available on another website without the consent of the copyright holder, constitutes a 'communication to the public' within the meaning of that provision, it is to be determined whether those links are provided without the pursuit of financial gain by a person who did not know or could not reasonably have known the illegal nature of the publication of those works on that other website or whether, on the contrary, those links are provided for such a purpose, a situation in which that knowledge must be presumed.

Where it is established that a person knew or ought to have known that the hyperlink he posted provides access to a work illegally placed on the internet, for example owing to the fact that he was notified thereof by the copyright holders, it is necessary to consider that the provision of that link constitutes a 'communication to the public' within the meaning of Article 3(1) of Directive 2001/29/EC. When the posting of hyperlinks is carried out for profit, it can be expected that the person who posted such a link carries out the necessary checks to ensure that the work concerned is not illegally published on the website to which those hyperlinks lead. In such circumstances, and in so far as that rebuttable presumption is not rebutted, the act of posting a hyperlink to a work which was illegally placed on the internet constitutes a 'communication to the public' within the meaning of Article 3(1) of Directive 2001/29/EC.

Judgment of 14 June 2017,* Stichting Brein *(C-610/15, EU:C:2017:456)

Ziggo and XS 4ALL were internet access providers. A significant number of their subscribers used the online sharing platform 'The Pirate Bay'. That platform allowed users to share and download, in segments ('torrents'), works present on their own computers. The files at issue were mainly copyright-protected works, without the

[77] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ 2001 L 167, p. 10).

rightholders having given their consent to the operators or users of that platform to carry out the sharing acts. Stichting Brein, a Netherlands foundation which protects the interests of copyright holders, brought proceedings before the Netherlands courts seeking an order directing Ziggo and XS4ALL to block the domain names and IP addresses of 'The Pirate Bay'.

The Hoge Raad der Nederlanden (Supreme Court of the Netherlands) essentially enquired whether a sharing platform such as 'The Pirate Bay' makes a 'communication to the public' within the meaning of Directive 2001/29/EC [78] and may therefore infringe copyright.

The Court held that the concept of 'communication to the public', within the meaning of Article 3(1) of Directive 2001/29/EC, must be interpreted as covering the making available and management, on the Internet, of a sharing platform which, by means of indexation of metadata referring to protected works and the provision of a search engine, allows users of that platform to locate those works and to share them in the context of a peer-to-peer network.

It must be noted, as recital 23 of Directive 2001/29/EC states, that the author's right of communication to the public, provided for in Article 3(1), covers any transmission or retransmission of a work to the public by wire or wireless means, including broadcasting.

The Court has already held that the provision, on a website, of clickable links to protected works published without any access restrictions on another site, affords users of the first site direct access to those works. The same is true as regards the sale of a multimedia player on which there are pre-installed add-ons, available on the internet, containing hyperlinks to websites – that are freely accessible to the public – on which copyright-protected works have been made available without the consent of the rightholders. It can therefore be inferred from that case-law that, as a rule, any act by which a user, with full knowledge of the relevant facts, provides its clients with access to protected works is liable to constitute an 'act of communication' for the purposes of Article 3(1) of Directive 2001/29/EC.

In order to be categorised as a 'communication to the public', within the meaning of Article 3(1) of Directive 2001/29/EC, the protected works must also in fact be communicated to a 'public'. The concept of 'public' involves a certain *de minimis* threshold. Thus, it is necessary to know not only how many persons have access to the same work at the same time, but also how many of them have access to it in succession.

[78] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ 2001 L 167, p. 10).

Judgment of 29 July 2019 (Grand Chamber), **Funke Medien NRW** *(C-469/17, EU:C:2019:623)*

The company Funke Medien operated the internet portal of the German daily newspaper Westdeutsche Allgemeine Zeitung. The Federal Republic of Germany, taking the view that Funke Medien had infringed its copyright over certain reports concerning military status that were 'classified for restricted access' and had been drawn up by the German Government, brought an action for an injunction against the latter. That action was upheld by a regional court and confirmed on appeal by a higher regional court. In its appeal on a point of law (Revision), brought before the referring court, the Bundesgerichtshof (Federal Court of Justice, Germany), Funke Medien maintained its contention that the action for an injunction should be dismissed.

As a preliminary point, the Court recalled that military status reports can be protected by copyright only if those reports constitute an intellectual creation of their author which reflect the author's personality and are expressed by free and creative choices made by that author in drafting those reports, which must be ascertained by the national court in each case.

The Court noted that the provisions of Directive 2001/29/EC providing for the exclusive rights of authors over reproduction and communication to the public of their work constitute measures of full harmonisation of the corresponding substantive law. On the other hand, the Court considered that the provisions of Directive 2001/29/EC allowing derogation from those rights in relation to the reporting of current events or quotations do not constitute measures of full harmonisation of the scope of the relevant exceptions or limitations. Nevertheless, the Member States' discretion in the implementation of those provisions must be exercised within the limits imposed by EU law in order to maintain a fair balance between, on the one hand, the interest of rights holders in the protection of their intellectual property rights, as guaranteed by the Charter, and, on the other hand, the rights and interests of users of protected works or subject matter, in particular their freedom of expression and information, which is also guaranteed by the Charter, as well as of the public interest.

Next, the Court clarified that freedom of expression and information is not capable of justifying, beyond the exceptions and limitations provided for in Directive 2001/29/EC, a derogation from the authors' exclusive rights over the reproduction and communication to the public of their works, other than that provided for by the said directive. In that regard, the Court reiterated that the list of exceptions and limitations provided for in Directive 2001/29/EC is exhaustive.

Lastly, the Court stated that, in the context of striking the balance, which is to be carried out by the national court, having regard to all the circumstances of the case before it, between, on the one hand, the exclusive rights of authors over the reproduction and communication to the public of their works and, on the other hand, the rights of users of protected subject matter referred to in the derogating provisions of Directive 2001/29/EC concerning the reporting of current events or quotations, a national court

must rely on an interpretation of those provisions which, whilst consistent with their wording and safeguarding their effectiveness, fully adheres to the fundamental rights enshrined in the Charter.

Judgment of 29 July 2019 (Grand Chamber), **Spiegel Online** *(C-516/17, EU:C:2019:625)*

The company Spiegel Online operated the internet news portal named Spiegel Online. Mr Volker Beck, who was a member of the Bundestag (Federal Parliament, Germany), brought an action before a regional court, challenging the making available of complete texts of one of his manuscripts and an article on Spiegel Online's website. Mr Beck considered that publication to be an infringement of his copyright. That court upheld Mr Beck's action. After its appeal was dismissed, Spiegel Online brought an appeal on a point of law (Revision) before the referring court, the Bundesgerichtshof (Federal Court of Justice, Germany).

The Court held that the provisions of Directive 2001/29/EC allowing derogation from the exclusive rights of the author in relation to the reporting of current events or quotations allow the Member States discretion in their transposition into national law but do not constitute measures of full harmonisation. Nevertheless, the Member States' discretion in the implementation of those provisions must be exercised within the limits imposed by EU law in order to maintain a fair balance between, on the one hand, the interest of rights holders in the protection of their intellectual property rights, as guaranteed by the Charter, and, on the other hand, the rights and interests of users of protected works or subject matter, in particular their freedom of expression and information, which is also guaranteed by the Charter, as well as of the public interest.

As regards the freedom of expression and information, the Court noted that it is not capable of justifying, beyond the exceptions and limitations provided for in Directive 2001/29/EC, a derogation from the authors' exclusive rights over the reproduction and communication to the public of their works, other than that provided for by the said directive. In that regard, the Court reiterated that the list of exceptions and limitations provided for in that directive is exhaustive.

Furthermore, the Court stated that, in the context of striking the balance, which is to be carried out by the national court, having regard to all the circumstances of the case before it, between, on the one hand, the exclusive rights of authors over the reproduction and communication to the public of their works and, on the other hand, the rights of users of protected subject matter referred to in the derogating provisions of Directive 2001/29/EC concerning the reporting of current events or quotations, a national court must rely on an interpretation of those provisions which, whilst consistent with their wording and safeguarding their effectiveness, fully adheres to the fundamental rights enshrined in the Charter.

In the first place, the Court held that the derogating provision of Directive 2001/29/EC concerning the reporting of current events precludes a national rule restricting the

application of the exception or limitation provided for in that provision in cases where it is not reasonably possible to make a prior request for authorisation with a view to the use of a protected work for the purposes of reporting current events. When a current event occurs, it is necessary, as a general rule, particularly in the information society, for the information relating to that event to be diffused rapidly, which is difficult to reconcile with a requirement for the author's prior consent, which would be likely to make it excessively difficult for relevant information to be provided to the public in a timely fashion, and might even prevent it altogether.

In the second place, the Court held, first, that the concept of 'quotations', referred to in the derogating provision of Directive 2001/29/EC concerning quotations, covers a reference made by means of a hyperlink to a file which can be downloaded independently. In that context, the Court recalled the case-law according to which hyperlinks contribute to the sound operation of the internet, which is of particular importance to freedom of expression and of information, enshrined in the Charter, as well as to the exchange of opinions and information in that network characterised by the availability of incalculable amounts of information. Secondly, the Court held that a work has already been lawfully made available to the public where that work, in its specific form, was previously made available to the public with the rightholder's authorisation or in accordance with a non-contractual licence or statutory authorisation. It is for the national court to decide whether a work has been lawfully made available to the public, in the light of the particular case before it and by taking into account all the circumstances of the case.

Judgment of 9 March 2021 (Grand Chamber),* VG Bild-Kunst *(C-392/19, EU:C:2021:181)

Stiftung Preußischer Kulturbesitz ('SPK'), a German foundation, is the operator of the Deutsche Digitale Bibliothek, a digital library devoted to culture and knowledge, which networks German cultural and scientific institutions. The website of that library contains links to digitised content stored on the internet portals of participating institutions. As a 'digital showcase', the Deutsche Digitale Bibliothek itself stores only thumbnails, that is to say smaller versions of original images.

VG Bild-Kunst, a visual arts copyright collecting society in Germany, maintains that the conclusion with SPK of a licence agreement for the use of its catalogue of works in the form of thumbnails should be subject to the condition that the agreement include a provision whereby SPK undertakes, when using the works covered by the agreement, to implement effective technological measures against the framing, [79] by third parties, of the thumbnails of such works on the website of the Deutsche Digitale Bibliothek.

[79] The technique of framing consists in dividing a website page into several frames and posting within one of them, by means of a clickable link or an embedded internet link (inline linking), an element coming from another site in order to hide from the users of that site the original environment to which that element belongs.

SPK considers that such a term in the agreement is not reasonable in the light of copyright, and brought an action before the German courts seeking a declaration that VG Bild-Kunst is required to grant SPK that licence without any condition requiring the implementation of such measures to prevent framing. [80]

Against that background, the Bundesgerichtshof (Federal Court of Justice, Germany) asks the Court for a determination of whether that framing must be held to be a communication to the public within the meaning of Directive 2001/29, [81] which, if that is the case, would permit VG Bild-Kunst to require SPK to implement such measures.

The Grand Chamber of the Court holds that the embedding by means of framing, in a third party website page, of works protected by copyright and made freely accessible to the public with the authorisation of the copyright holder on another website constitutes a communication to the public where that embedding circumvents protection measures against framing adopted or imposed by the copyright holder.

First, the Court states that the alteration in the size of the works in framing is not a factor in the assessment of whether there is an act of communication to the public, so long as the original elements of those works are perceptible.

Next, the Court states that the technique of framing constitutes an act of communication to a public, since the effect of that technique is to make the posted element available to all the potential users of a website. Further, the Court states that, provided that the technical means used by the technique of framing are the same as those previously used to communicate the protected work to the public on the original website, namely the internet, that communication does not satisfy the condition of being made to a new public and that communication accordingly does not fall within the scope of a communication 'to the public', within the meaning of Directive 2001/29.

However, the Court adds that that consideration is applicable only in a situation where access to the works concerned on the original website is not subject to any restrictive measure. In that situation, the right holder has authorised from the outset the communication of his or her works to all internet users.

Conversely, the Court states that, where the right holder has established or imposed from the outset restrictive measures linked to the publication of his or her works, he or she has not agreed to third parties being able to communicate his or her works freely to the public. On the contrary, his or her intention was to restrict the public having access to his or her works solely to the users of a particular website.

---

80 Under German law, collecting societies are obliged to grant to any person who so requests, on reasonable terms, a licence to use the rights whose management is entrusted to them. However, according to German case-law, collecting societies may, exceptionally, refuse to grant a licence, provided that that refusal is not an abuse of monopoly power and that the licence application is objectionable by reference to overriding legitimate interests.

81 Under Article 3(1) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ 2001 L 167, p. 10), Member States are to provide authors with the exclusive right to authorise or prohibit any communication to the public of their works.

Consequently, the Court holds that, where the copyright holder has adopted or imposed measures to restrict framing, the embedding of a work in a website page of a third party, by means of the technique of framing, constitutes an act of 'making available that work to a new public'. That communication to the public must, therefore, be authorised by the right holders concerned.

The opposite approach would amount to creating a rule on exhaustion of the right of communication. Such a rule would deprive the copyright holder of the opportunity to claim an appropriate reward for the use of his or her work. Accordingly, the consequence of such an approach would be that the need to safeguard a fair balance in the digital environment, between, on the one hand, the interest of the holders of copyright and related rights in the protection of their intellectual property, and, on the other, the protection of the interests and fundamental rights of users of protected subject matter, would be disregarded.

Last, the Court makes clear that a copyright holder may not limit his or her consent to framing by means other than effective technological measures. In the absence of such measures, it might prove difficult to ascertain whether that right holder intended to oppose the framing of his or her works.

Judgment of 22 June 2021 (Grand Chamber), **YouTube and Cyando** *(C-682/18 and C-683/18, EU:C:2021:503)*

In the dispute giving rise to the first case (C-682/18), Frank Peterson, a music producer, is bringing an action against YouTube and its legal representative Google before the German courts in respect of the posting online, on YouTube, in 2008, of a number of recordings over which he claims to hold various rights. Those recordings were posted by users of that platform without his permission. They are songs from the album *A Winter Symphony* by Sarah Brightman and private audio recordings made during concerts on her *'Symphony Tour'*.

In the dispute giving rise to the second case (C-683/18), the publisher Elsevier is bringing an action against Cyando before the German courts in respect of the posting online, on the 'Uploaded' file-hosting and -sharing platform, in 2013, of various works over which Elsevier holds exclusive rights. Those works were posted by users of that platform without its permission. They are *Gray's Anatomy for Students*, *Atlas of Human Anatomy* and *Campbell-Walsh Urology*, which could be consulted on Uploaded via the link collections rehabgate.com, avaxhome.ws and bookarchive.ws.

The Bundesgerichtshof (Federal Court of Justice, Germany), which is hearing the two cases, referred a number of questions to the Court for a preliminary ruling so that the latter can provide clarification on, inter alia, the liability of the operators of online platforms as regards copyright-protected works illegally posted online on such platforms by platform users.

The Court has examined that liability under the set of rules, applicable at the material time, under Directive 2001/29 on copyright, [82] Directive 2000/31 on electronic commerce, [83] and Directive 2004/48 on the enforcement of copyright. [84] The questions referred do not concern the set of rules established by Directive 2019/790 relating to copyright and related rights in the Digital Single Market, which came into force subsequently. [85]

In its Grand Chamber judgment, the Court finds, inter alia, that, as EU law currently stands, operators of online platforms do not themselves make a communication to the public of copyright-protected content illegally posted online by users of those platforms unless those operators contribute, beyond merely making those platforms available, to giving access to such content to the public in breach of copyright. Moreover, the Court finds that such operators may benefit from the exemption from liability under Directive 2000/31 on electronic commerce unless they play an active role of such a kind as to give them knowledge of or control over the content uploaded to their platform.

In the first place, the Court examines the question whether the operator of a video-sharing platform or a file-hosting and -sharing platform on which users can illegally make protected content available to the public itself carries out, in circumstances such as those at issue in the present cases, a 'communication to the public' of that content within the meaning of Directive 2001/29 on copyright. [86] At the outset, the Court states the objectives and definition of the concept of a 'communication to the public' as well as the associated criteria which must be taken into account when making an individual assessment of what that concept means.

Amongst those criteria, the Court emphasises the indispensable role played by the platform operator and the deliberate nature of its intervention. That platform operator makes an 'act of communication' when it intervenes, in full knowledge of the consequences of its action, to give its customers access to a protected work, particularly where, in the absence of that intervention, those customers would not, in principle, be able to enjoy the broadcast work.

In that context, the Court finds that the operator of a video-sharing platform or a file-hosting and -sharing platform, on which users can illegally make protected content available to the public, does not make a 'communication to the public' of that content,

---

82 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ 2001 L 167, p. 10).

83 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ 2000 L 178, p. 1).

84 Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ 2004 L 157, p. 45, and corrigendum OJ 2004 L 195, p. 16).

85 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (OJ 2019 L 130, p. 92). That directive establishes, for operators of online platforms, a new specific liability regime in respect of works illegally posted online by users of those platforms. That directive, which must be transposed by each Member State into its national law by 7 June 2021 at the latest, requires, inter alia, those operators to seek permission from rightholders – for example, by concluding a licencing agreement – for works posted online by users of their platform.

86 Article 3(1) of Directive 2001/29 on copyright. Under that provision, Member States are to provide authors with the exclusive right to authorise or prohibit any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them.

within the meaning of Directive 2001/29 on copyright, unless it contributes, beyond merely making that platform available, to giving access to such content to the public in breach of copyright.

That is the case, inter alia, where that operator has specific knowledge that protected content is available illegally on its platform and refrains from expeditiously deleting it or blocking access to it, or where that operator, despite the fact that it knows or ought to know, in a general sense, that users of its platform are making protected content available to the public illegally via its platform, refrains from putting in place the appropriate technological measures that can be expected from a reasonably diligent operator in its situation in order to counter credibly and effectively copyright infringements on that platform, or where that operator participates in selecting protected content illegally communicated to the public, provides tools on its platform specifically intended for the illegal sharing of such content or knowingly promotes such sharing, which may be attested by the fact that that operator has adopted a financial model that encourages users of its platform illegally to communicate protected content to the public via that platform.

In the second place, the Court looks at the question whether the operator of online platforms may benefit from the exemption from liability, provided for in Directive 2000/31 on electronic commerce, [87] in respect of protected content which users illegally communicate to the public via its platform. In that context, the Court examines whether the role played by that operator is neutral, that is to say, whether its conduct is merely technical, automatic and passive, which means that it has no knowledge of or control over the content it stores, or whether, on the contrary, that operator plays an active role that gives it knowledge of or control over that content. In that regard, the Court finds that such an operator can benefit from the exemption from liability provided that it does not play an active role of such a kind as to give it knowledge of or control over the content uploaded to its platform. On that point, the Court specifies that, for such an operator to be excluded from the exemption from liability provided for in that directive, it must have knowledge of or awareness of specific illegal acts committed by its users relating to protected content that was uploaded to its platform.

In the third place, the Court clarifies the circumstances in which, under Directive 2001/29 on copyright, [88] rightholders can obtain injunctions against operators of online platforms. It finds that that directive does not preclude a situation under national law whereby a copyright holder or the holder of a related right may not obtain an injunction against an operator whose service has been used by a third party to infringe his or her

[87] Article 14(1) of Directive 2000/31 on electronic commerce. Under that provision, where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States are to ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that 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 the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

[88] Article 8(3) of Directive 2001/29 on copyright. Under that provision, Member States are to ensure that right holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.

right, that operator having had no knowledge or awareness of that infringement, within the meaning of Directive 2000/31 on electronic commerce, [89] unless, before court proceedings are commenced, that infringement has first been notified to that operator and the latter has failed to intervene expeditiously in order to remove the content in question or to block access to it and to ensure that such infringements do not recur.

It is, however, for the national courts to satisfy themselves, when applying such a condition, that that condition does not result in the actual cessation of the infringement being delayed in such a way as to cause disproportionate damage to the rightholder.

II. Legal framework governing electronic commerce

1. Advertising

Judgment of 23 March 2010 (Grand Chamber),* Google France *(C-236/08 to C-238/08, EU:C:2010:159)

Google operated an internet search engine and offered, among other things, a paid referencing service called 'AdWords'. That service enabled any economic operator, by means of the reservation of one or more keywords, to obtain the placing of an advertising link to its site, together with an advertising message. Vuitton, the proprietor of the Community trade mark 'Vuitton' and other proprietors of French trade marks became aware that the entry, by internet users, of terms constituting its trade marks into Google triggered the display of links to sites offering imitation versions of Vuitton's products and to sites of competitors of other proprietors of trade marks. The Cour de cassation (Court of Cassation, France) asked the Court of Justice whether it was lawful to use signs corresponding to trade marks as keywords in an internet referencing service, without consent having been given by the proprietors of those trade marks.

The Court held that an internet referencing service provider does not use that sign within the meaning of Article 5(1) and (2) of Directive 89/104/EEC [90] or Article 9(1) of Regulation (EC) No 40/94, [91] even if it permits advertisers to select, as keywords, signs identical with trade marks, stores those signs and displays its clients' ads on the basis thereof. The use, by a third party, of a sign identical with, or similar to, the proprietor's trade mark implies that that third party uses the sign in its own commercial

[89] Article 14(1)(a) of Directive 2000/31 on electronic commerce.
[90] Council Directive 89/104/EEC of 21 December 1988 to approximate the laws of the Member States relating to trade marks (OJ 1989 L 40, p. 1).
[91] Council Regulation (EC) No 40/94 of 20 December 1993 on the Community trade mark (OJ 1994 L 11, p. 1).

communication and amounts to use for the purposes of that directive, where the display seeks to mislead internet users as to the origin of its goods or services.

The proprietor of a trade mark is entitled to prohibit an advertiser from advertising where such advertising makes it difficult for an internet user to ascertain whether the goods or services referred to therein originate from the proprietor of the trade mark or a third party. The essential function of the trade mark is, in particular, to enable internet users to distinguish the goods or services of the proprietor of that mark from those which have a different origin.

Nevertheless, repercussions of use by third parties of a sign identical with the trade mark do not of themselves constitute an adverse effect on the advertising function of the trade mark. Article 14 of Directive 2000/31/EC [92] must be interpreted as meaning that the rule laid down therein applies to an internet referencing service provider in the case where that service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored. If the conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores, that provider cannot be held liable.

Judgment of 11 July 2013,* Belgian Electronic Sorting Technology *(C-657/11, EU:C:2013:516)

The undertakings Belgian Electronic Sorting Technology (BEST) and Visys were producers, manufacturers and distributors of sorting machines and sorting systems incorporating laser-technology. Visys had been established by Mr Peelaers, a former employee of BEST. Mr Peelaers registered, on behalf of Visys, the domain name 'www.bestlasersorter.com'. The content of the website hosted under that domain name was identical to that of Visys' usual websites, accessible under the domain names 'www.visys.be' and 'www.visysglobal.be'. When the words 'Best Laser Sorter' were entered in the search engine google.be, the second search result to appear, directly after BEST's website, was a link to Visys' website. Visys used for its websites the following metatags, among others: 'Best+Helius, Best+Genius'. The referring court, the Hof van Cassatie (Court of Cassation, Belgium), asked the Court of Justice whether the registration and use of a domain name and the use of metatags in a website's metadata could be regarded as falling within the concept of advertising within the meaning of Directives 84/450/EEC [93] and 2006/114/EC. [94]

The Court found that Article 2(1) of Directive 84/450/EEC and Article 2(a) of Directive 2006/114/EC must be interpreted as meaning that the term advertising, as defined by those provisions, covers the use of a domain name and that of metatags in a website's

[92] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (OJ 2000 L 178, p. 1).

[93] Council Directive 84/450/EEC of 10 September 1984 relating to the approximation of the laws, regulations and administrative provisions of the Member States concerning misleading advertising, as amended by Directive 2005/29/EC (OJ 1984 L 250, p. 17).

[94] Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising (OJ 2006 L 376, p. 21).

metadata, where the domain name or the metatags consisting of keywords ('keyword metatags') make reference to certain goods or services or to the trade name of a company and constitute a form of representation that is made to potential consumers and suggests to them that they will find a website relating to those goods or services, or relating to that company.

The term advertising cannot be interpreted and applied in such a way that steps taken by a trader to promote the sale of his products or services that are capable of influencing the economic behaviour of consumers and, therefore, of affecting the competitors of that trader, are not subject to the rules of fair competition imposed by those directives.

By contrast, the registration of a domain name, as such, is not encompassed by that term. That is a purely formal act which, in itself, does not necessarily imply that potential consumers can become aware of the domain name, and which is therefore not capable of influencing the choice of those potential consumers.

Judgment of 4 May 2017, **Luc Vanderborght** *(C-339/15, EU:C:2017:335)*

Mr Luc Vanderborght, a dentist established in Belgium, advertised the provision of dental care services. He installed a sign stating his name, his designation as a dentist, the address of his website and the telephone number of his practice. In addition, he created a website informing patients of the various types of treatment offered at his practice. Finally, he placed some advertisements in local newspapers. As a result of a complaint made by the Verbond der Vlaamse tandartsen, a professional association of dentists, criminal proceedings were brought against Mr Vanderborght. Belgian law prohibited all advertising for the provision of oral and dental care services and imposed requirements of discretion. Proceedings having been brought before it, the Nederlandstalige rechtbank van eerste aanleg te Brussel (Brussels Court of First Instance (Dutch-speaking), Belgium) decided to submit a question to the Court of Justice on the matter.

According to the Court, Directive 2000/31/EC [95] must be interpreted as precluding national legislation such as that at issue in the main proceedings.

Recital 18 of Directive 2000/31/EC states that the concept of 'information society services' spans a wide range of economic activities which take place online. Furthermore, Article 2(f) of that directive stipulates that the concept of 'commercial communication' covers, inter alia, any form of communication designed to promote the services of a person practising a regulated profession. It follows that advertising relating to the provision of oral and dental care services by means of a website constitutes such a service. The EU legislature has not excluded regulated professions from the principle

[95] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (OJ 2000 L 178, p. 1).

of the permissibility of online commercial communications laid down in Article 8(1) of that directive. Although that provision makes it possible to take into account the particularities of health professions when the relevant professional rules are drawn up, by supervising the form and manner of the online commercial communications with a view, in particular, to ensuring that the confidence which patients have in those professions is not undermined, the fact remains that those professional rules cannot impose a general and absolute prohibition of any form of online advertising designed to promote the activity of a person practising such a profession.

Article 56 TFEU must be interpreted as precluding national legislation, such as that at issue in the main proceedings, which imposes a general and absolute prohibition of any advertising relating to the provision of oral and dental care services.

As regards the need for a restriction on the freedom to provide services such as that at issue in the main proceedings, account must be taken of the fact that the health and life of humans rank foremost among the assets and interests protected by the Treaty and that it is, in principle, for the Member States to determine the level of protection which they wish to afford to public health.

All the advertising messages prohibited by that legislation are not, in themselves, likely to produce effects that are contrary to the objectives referred to. In those circumstances, it must be held that the objectives pursued by the legislation at issue in the main proceedings could be attained through the use of less restrictive measures.

Judgment of 30 March 2017, **Verband Sozialer Wettbewerb eV** *(C-146/16, EU:C:2017:243)*

The subject matter of the dispute was an advertisement published in a newspaper by DHL Paket, which operated the online sales platform 'MeinPaket.de' on which commercial sellers offered products for sale. The goods presented in that advertisement, which each had a code, could be purchased from third-party sellers through that platform. Once connected to the site, the user could enter the corresponding code to be redirected to a page providing further details on the product in question and mentioning the seller, whose relevant particulars could be consulted under a heading for that purpose.

According to the Verband Sozialer Wettbewerb (VSW), an association whose members include suppliers of electric and electronic products and mail-order companies, which sell all sorts of products, the published advertisement constituted an unfair business practice. According to VSW, DHL Paket did not meet its obligation to state the identity and geographical address of the suppliers using its sales platform. VSW brought an action seeking the cessation of that advertising activity.

In reply to a question referred for a preliminary ruling by the Bundesgerichtshof (Federal Court of Justice, Germany), the Court of Justice held that Article 7(4) of Directive 2005/29/EC [96] must be interpreted as meaning that an advertisement, such as that at issue in the main proceedings, which falls within the definition of an 'invitation to purchase' within the meaning of that directive, may satisfy the obligation regarding information laid down in that provision.

It is for the referring court to examine, on a case-by-case basis, first, whether the limitations of space in the advertisement warrant information on the supplier being provided only upon access to the online sales platform and, secondly, whether, so far as the online sales platform is concerned, the information required by Article 7(4)(b) of that directive is communicated simply and quickly.

Judgment of 3 March 2016, **Daimler AG** *(C-179/15, EU:C:2016:134)*

Együd Garage, a Hungarian company specialising in the sale and repair of Mercedes cars, was bound by an after-sales service contract with Daimler, the German manufacturer of Mercedes cars and proprietor of the international trade mark 'Mercedes-Benz'. The Hungarian company was entitled to use that trade mark and to describe itself as an 'authorised Mercedes-Benz dealer' in its own advertisements. Following the termination of that contract, Együd Garage tried to remove all internet advertisements on the basis of which the public might assume that there was still a contractual relationship between it and Daimler. Despite taking those steps, advertisements referring to such a relationship continued to be distributed online and displayed by search engines. The Fővárosi Törvényszék (Budapest High Court, Hungary) asked the Court of Justice whether Directive 2008/95/EC on trade marks [97] entitled Daimler to require a previous contractual partner to take extensive steps to prevent detriment to its trade mark.

The Court held that the use of a trade mark by a third party, without the proprietor's authorisation, in order to inform the public that that third party carries out repairs and maintenance of goods covered by that trade mark or that he has specialised in such goods constitutes a use of that mark for the purposes of Article 5(1)(a) of Directive 2008/95/EC. That may be prohibited by the trade mark proprietor unless Article 6, concerning the limitation of the effects of the trade mark, or Article 7, concerning exhaustion of the rights conferred by it, are applicable. Such use, where it is made without the consent of the proprietor of the mark, is liable to affect the origin function of the mark.

---

[96] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (OJ 2005 L 149, p. 22).

[97] Directive 2008/95/EC of the European Parliament and of the Council of 22 October 2008 to approximate the laws of the Member States relating to trade marks (OJ 2008 L 299, p. 25).

Article 5(1)(a) and (b) of that directive must be interpreted as meaning that use does not occur where that advertisement has not been placed by that third party or on his behalf or, if that advertisement has been placed by that third party or on his behalf with the consent of the proprietor, where that third party has expressly requested the operator of that website, from whom the third party ordered the advertisement, to remove the advertisement or the reference to the mark contained therein. Furthermore, an advertiser cannot be held liable for the independent actions of other economic operators, such as those of referencing website operators, which do not act by order but on their own initiative and in their own name.

In both situations, the proprietor of the mark is not entitled, under Article 5(1)(a) or (b) of Directive 2008/95/EC, to take action against the advertiser in order to prevent him from publishing online the advertisement containing the reference to its trade mark.

Judgment of 22 December 2022 (Grand Chamber),* Louboutin (Use of an infringing sign on an online marketplace) *(C-148/21 and C-184/21, EU:C:2022:1016)

Since 2016, Mr Louboutin, a French designer of luxury footwear and handbags, has registered the colour red, applied to the outer sole of a high-heeled shoe, as an EU trade mark.

Amazon operates websites selling various goods which it offers both directly, in its own name and on its own behalf, and indirectly, by providing a sales platform for third-party sellers. That operator also offers third-party sellers the additional services of stocking and shipping their goods.

Mr Louboutin stated that those websites regularly display advertisements for red-soled shoes which, in his view, relate to goods which have been placed on the market without his consent. Then, alleging an infringement of the exclusive rights conferred by the mark at issue, he brought two actions for infringement against Amazon before the tribunal d'arrondissement de Luxembourg (District Court, Luxembourg, Luxembourg) [98] and the tribunal de l'entreprise francophone de Bruxelles (Brussels Companies Court (French-speaking), Belgium). [99]

Each of those courts then decided to refer a number of questions to the Court of Justice for a preliminary ruling.

In essence, they asked the Court whether the EU trade mark regulation [100] must be interpreted as meaning that the operator of an online sales website incorporating, as well as that operator's own sales offerings, an online marketplace may be regarded as itself using a sign which is identical with an EU trade mark of another person for goods

[98] Case C-148/21.
[99] Case C-184/21.
[100] More specifically, Article 9(2)(a) of Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark (OJ 2017 L 154, p. 1).

which are identical with those for which that trade mark is registered where third-party sellers offer goods bearing that sign for sale on that marketplace without the consent of the trade mark proprietor.

They are unsure, inter alia, whether the following are relevant in that regard: the fact that that operator uses a uniform method of presenting the offers published on its website, displaying both the advertisements relating to the goods which it sells in its own name and on its own behalf and those relating to goods offered by third-party sellers on that marketplace; the fact that it places its own logo as a renowned distributor on all those advertisements; and the fact that it offers third-party sellers, in connection with the marketing of their goods, additional services consisting in providing them support in the presentation of their advertisements and in storing and shipping goods offered on the same marketplace. In that context, the referring courts also ask whether it is necessary to take into consideration, where appropriate, the perception of the users of the website in question.

The Court, sitting as the Grand Chamber, had the opportunity to provide important clarifications on the issue of the direct liability of the operator of an online sales website incorporating an online marketplace for infringements of the rights of the proprietor of an EU trade mark resulting from the fact that a sign which is identical with that mark appears in advertisements from third-party sellers on that marketplace.

It must be recalled that, under the EU trade mark regulation, [101] the registration of an EU trade mark confers on its proprietor the right to prevent all third parties from using, in the course of trade, any sign which is identical with that trade mark in relation to goods or services which are identical with those for which the mark is registered.

The Court notes at the outset that the concept of 'using' is not defined by the EU trade mark regulation. Nevertheless, that expression involves active behaviour and direct or indirect control of the act constituting the use. Only a third party which has such control is effectively able to stop the use of a trade mark without the consent of its proprietor.

The use, by a third party, of a sign which is identical with or similar to the proprietor's trade mark also implies, at the very least, that that third party uses the sign in its own commercial communication. A person may thus allow its clients to use signs which are identical with or similar to trade marks without itself using those signs. The Court thus considered that, with regard to the operator of an online marketplace, the use of signs which are identical with or similar to trade marks in offers for sale displayed on that marketplace is made only by the sellers which are customers of that operator and not by the operator itself, since the latter does not use that sign in its own commercial communication.

[101] Article 9(2)(a) of Regulation (EU) No 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark (OJ 2017 L 154, p. 1).

The Court observes, however, that, in its earlier case-law, it was not asked about the impact of the fact that the online sales website in question incorporates, as well as the online marketplace, sales offers of the operator of that site itself, whereas the present cases specifically raise the issue of that impact. Accordingly, in the present case, the referring courts are uncertain whether, in addition to the third-party seller, the operator of an online sales website incorporating an online marketplace, such as Amazon, also uses, in its own commercial communication, a sign which is identical with a trade mark of another person for goods which are identical with those for which that trade mark is registered, and may thus be held liable for the infringement of the rights of the proprietor of that trade mark where that third-party seller offers goods bearing that sign for sale on that marketplace.

The Court finds that that issue arises irrespective of the fact that the role of that operator may, where appropriate, also be examined from the point of view of other rules of law and that, although the assessment of such use by the operator is ultimately a matter for the national court, it may provide elements of interpretation under EU law which may be useful in that regard.

In that connection, as regards commercial communication, the Court states that the use of a sign which is identical with another person's trade mark by the operator of a website incorporating an online marketplace in its own commercial communication presupposes that that sign appears, in the eyes of third parties, to be an integral part of that communication and, consequently, a part of its activity.

In that context, the Court notes that, in a situation in which the operator of a service uses a sign which is identical with or similar to the trade mark of another person in order to promote goods which one of its customers is marketing with the assistance of that service, that operator does itself make use of that sign if it uses it in such a way that it establishes a link between the sign and the services provided by that operator.

Accordingly, the Court has held that such an operator does not itself make use of a sign which is identical with or similar to a trade mark of another person when the service it provides is not comparable to a service aimed at promoting the marketing of goods bearing that sign and does not imply the creation of a link between the service and that sign, since the operator in question is not apparent to the consumer, which excludes any association between its services and the sign at issue.

On the other hand, the Court has held that such a link does exist where the operator of an online marketplace, by means of an internet referencing service and on the basis of a keyword which is identical with a trade mark of another person, advertises goods bearing that trade mark which are offered for sale by its customers on its online marketplace. For internet users carrying out a search on the basis of a keyword, such advertising creates an obvious association between those trade-marked goods and the possibility of buying them through that marketplace. That is why the proprietor of that trade mark is entitled to prohibit that operator from such use, where that advertising

infringes the trade mark right owing to the fact that it does not enable well-informed and reasonably observant internet users, or enables them only with difficulty, to ascertain whether those goods originate from the proprietor of that trade mark or from an undertaking economically linked to that proprietor or, on the contrary, from a third party.

The Court concluded from this that, in order to determine whether the operator of an online sales website incorporating an online marketplace does itself make use of a sign which is identical with a trade mark of another person, which appears in the advertisements relating to goods offered by third-party sellers on that marketplace, it is necessary to assess whether a well-informed and reasonably observant user of that website establishes a link between that operator's services and the sign in question.

From that point of view, in order to determine whether an advertisement, published on that marketplace by a third-party seller active on that marketplace, using a sign which is identical with a trade mark of another person may be regarded as forming part of the commercial communication of the operator of that website, it is necessary to ascertain whether it is capable of establishing a link between the services offered by that operator and the sign in question, on the ground that a user might believe that the operator is marketing, in its own name and on its own behalf, the goods for which the sign in question is being used.

The Court highlights that, in the overall assessment of the circumstances of the present case, the method of presenting the advertisements, both individually and as a whole, on the website in question and the nature and scope of the services provided by the operator of the website are particularly important.

As regards, first, the method of presenting the advertisements, EU law requires transparency in the display of advertisements on the internet, so that a well-informed and reasonably observant user can distinguish easily between offers originating from the operator of the website and from third-party sellers active on the online marketplace. However, the Court considers that the operator's use of a uniform method of presenting the offers published, displaying both its own advertisements and those of third-party sellers and placing its own logo as a renowned distributor on its own website and on all of the advertisements may make it difficult to draw such a distinction and thus give the impression that that operator is marketing, in its own name and on its own behalf, the goods offered for sale by those third-party sellers.

Second, the nature and scope of the services provided by the operator of an online marketplace to sellers, and in particular the services consisting of the storage, shipping and management of returns of those goods, are also likely to give the impression, to a well-informed and reasonably observant user, that those same goods are being marketed by that operator and thus establish a link, in the eyes of those users, between those services and the signs placed on those goods and in the advertisements of third-party sellers.

In conclusion, the Court rules that the operator of an online sales website incorporating, as well as that operator's own sales offers, an online marketplace may be regarded as itself using a sign which is identical with an EU trade mark of another person for goods which are identical with those for which that trade mark is registered, where third-party sellers offer for sale, on that marketplace, without the consent of the proprietor of that trade mark, such goods bearing that sign, if a well-informed and reasonably observant user of that site establishes a link between the services of that operator and the sign at issue, which is in particular the case where, in view of all the circumstances of the situation in question, such a user may have the impression that that operator itself is marketing, in its own name and on its own behalf, the goods bearing that sign. The Court adds that the following are relevant in that regard:

– the fact that that operator uses a uniform method of presenting the offers published on its website, displaying both the advertisements relating to the goods which it sells in its own name and on its own behalf and those relating to goods offered by third-party sellers on that marketplace;
– the fact that it places its own logo as a renowned distributor on all those advertisements; and
– the fact that it offers third-party sellers, in connection with the marketing of goods bearing the sign at issue, additional services consisting inter alia in the storing and shipping of those goods.

Judgment of 22 December 2022 (Grand Chamber),* EUROAPTIEKA *(C-530/20, EU:C:2022:1014)

'EUROAPTIEKA' SIA is a company operating a pharmaceutical business in Latvia. It is part of a group that owns a network of pharmacies and companies distributing medicinal products for retail in that country. In 2016, the Veselības inspekcijas Zāļu kontroles nodaļa (Medicinal Product Control Section of the Health Inspectorate, Latvia) banned EUROAPTIEKA from the dissemination of advertising relating to a promotional sale offering a reduction of 15% off the purchase price of any medicinal product when at least three articles were purchased. That decision was taken on the basis of a national provision that prohibited the inclusion in advertising to the general public of a medicinal product, which is neither subject to medical prescription nor reimbursed, of any information which encourages the purchase of the medicinal product by justifying the need to purchase that medicinal product on the basis of its price, by announcing a special sale, or by indicating that the medicinal product is sold as a bundle together with other medicinal products (including at a reduced price) or other types of product. [102]

[102] Subparagraph 18.12 of the Ministru kabineta noteikumi Nr. 378 « Zāļu reklamēšanas kārtība un kārtība, kādā zāļu ražotājs ir tiesīgs nodot ārstiem bezmaksas zāļu paraugus » (Decree No 378 of the Council of Ministers on 'the detailed rules for the advertising of medicinal products and detailed rules pursuant to which a medicinal product manufacturer may give free samples of medicinal products to medical practitioners'), of 17 May 2011 (Latvijas Vēstnesis, 2011, No 78).

In 2020, hearing an appeal brought by EUROAPTIEKA against that provision, the Latvijas Republikas Satversmes tiesa (Constitutional Court, Latvia) made a request to the Court of Justice for a preliminary ruling on the interpretation of Directive 2001/83. [103]

By its judgment, the Court of Justice, sitting as the Grand Chamber, clarifies the scope of the concept of 'advertising of medicinal products', within the meaning of that directive, in particular as regards content that refers not to a specific medicinal product but to unspecified medicinal products. Furthermore, it rules on the compatibility with that directive of a national provision providing for prohibitions such as those at issue in the main proceedings, including as to whether those prohibitions seek to promote the rational use of medicinal products, within the meaning of that same directive.

In the first place, the Court rules that the dissemination of information that encourages the purchase of medicinal products by justifying the need for that purchase on the basis of price, by announcing a special sale, or by indicating that the medicinal products are sold together with other medicinal products, including at a reduced price, or with other products, falls within the concept of 'advertising of medicinal products', within the meaning of Directive 2001/83, even where that information does not refer to a specific medicinal product, but to unspecified medicinal products.

First of all, from a textual perspective, the Court recalls that Article 86(1) of that directive, which contains the concept of 'advertising of medicinal products' systematically refers to 'medicinal products' in the plural. In addition, that provision defines that concept broadly, as covering 'any form' of door-to-door information, canvassing activity or inducement, including, inter alia 'advertising of medicinal products to the general public'.

Next, from a contextual perspective, the Court finds that the provisions of Title VIII of Directive 2001/83, of which Article 86 is part, set out the general and fundamental rules relating to advertising of medicinal products and that, therefore, they apply to any activity seeking to promote the prescription, supply, sale or consumption of medicinal products.

Finally, as regards the objectives pursued by Directive 2001/83, the Court considers that the essential aim of safeguarding public health pursued by that directive would be greatly compromised if an activity of door-to-door information, canvassing or inducement seeking to promote the prescription, supply, sale or consumption of medicinal products without making reference to a specific medicinal product did not fall within the concept of 'advertising of medicinal products' and therefore escaped the prohibitions, conditions and restrictions laid down by that directive as regards advertising.

[103] More specifically, the provisions referred to are Articles 86(1), 87(3) and 90 of Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (OJ 2001 L 311, p. 67), as amended by Directive 2004/27/EC of the European Parliament and of the Council of 31 March 2004 (OJ 2004 L 136, p. 34).

To the extent that advertising for non-specified medicinal products, such as the advertising of an entire class of medicinal products intended to treat the same pathology, may relate equally to medicinal products subject to medical prescription and to medicinal products the cost of which may be reimbursed, to exclude that advertising from the scope of the provisions of Directive 2001/83 on the subject of advertising would result in the prohibitions laid down by that directive [104] being deprived of their effectiveness to a large extent, by allowing any advertising that does not refer to a specific medicinal product within that class to escape those prohibitions.

In addition, the Court considers that advertising made with regard to a set of unspecified medicinal products that are neither subject to medical prescription nor reimbursed may, in the same way as advertising in respect of a single specific medicinal product, be excessive and ill-considered and, therefore, harmful to public health, by inducing the irrational use or overconsumption by consumers of the medicinal products concerned.

The Court concludes that, notwithstanding the decision in the judgment *A (Advertising and sale of medicinal products online)* [105] and the judgment in *DocMorris*, [106] the concept of 'advertising of medicinal products', for the purposes of Directive 2001/83, covers any form of door-to-door information, canvassing activity or inducement designed to promote the prescription, supply, sale or consumption of specified or unspecified medicinal products.

The Court adds that, since the purpose of the message constitutes the fundamental defining characteristic of that concept and the decisive factor for distinguishing advertising from mere information and that the activities of disseminating information covered by the national provision, such as that at issue in the main proceedings, appear to have such a promotional purpose, those activities fall within that concept.

In the second place, the Court holds that the provisions of Directive 2001/83 [107] do not preclude a national provision that imposes restrictions not laid down by that directive but which meet the essential aim of safeguarding public health pursued by that directive, by prohibiting the inclusion, in advertising to the general public of medicinal products not subject to medical prescription and not reimbursed, of information that encourages the purchase of medicinal products by justifying the need for such a purchase on the basis of the price of those medicinal products, by announcing a special sale or by indicating that those medicinal products are sold together with other medicinal products, including at a reduced price, or with other products.

In support of that interpretation, the Court recalls, first, that, as regards the relationship between the requirement that that advertising promotes the rational use of medicinal

[104] Article 88(1)(a) and (3) of Directive 2001/83.
[105] Judgment of 1 October 2020, *A (Advertising and sale of medicinal products online)*, (C-649/18, EU:C:2020:764, paragraph 50).
[106] Judgment of 15 July 2021, *DocMorris* (C-190/20, EU:C:2021:609, paragraph 20).
[107] More specifically, Articles 87(3) and 90 of Directive 2001/83.

products [108] and the restrictions referred to in Directive 2001/83 in the form of a list of banned advertising methods, [109] the fact that that directive does not contain any specific rules concerning certain advertising material does not preclude that, with the aim of preventing any excessive and ill-considered advertising of medicinal products which could affect public health, Member States may prohibit [110] that material to the extent that it encourages the irrational use of medicinal products.

Consequently, and notwithstanding the fact that Directive 2001/83 permits advertising of medicinal products not subject to medical prescription, in order to prevent risks to public health in accordance with the essential aim of safeguarding public health, Member States must prohibit the inclusion, in advertising to the public of medicinal products which are neither subject to medical prescription nor reimbursed, of material which is of such a nature as to promote the irrational use of such medicinal products.

Secondly, as regards whether that is the case for the material covered by prohibitions such as those at issue in the main proceedings, the Court observes that, as regards medicinal products that are not subject to medical prescription and not reimbursed, it is frequently the case that the end consumer himself or herself evaluates, without the assistance of a doctor, the usefulness or need to purchase such medicinal products. However, that consumer does not necessarily have the specific and objective knowledge enabling him or her to evaluate their therapeutic value. Advertising may therefore exercise a particularly strong influence on the evaluation and choice made by that consumer, both as regards the quality of the medicinal product and the amount to purchase.

In that context, advertising methods such as those referred to in the national provision at issue in the main proceedings are of such a nature as to encourage consumers to purchase medicinal products which are neither subject to medical prescription nor reimbursed according to an economic criterion connected with the price of those medicinal products and, therefore, are likely to lead consumers to purchase and consume those medicinal products without carrying out an objective evaluation based on the therapeutic properties of those products and on specific medical needs.

According to the Court, advertising that distracts the consumer from an objective evaluation of the need to take such medicine encourages the irrational and excessive use of that medicinal product. Such irrational and excessive use of medicinal products may also arise as a result of advertising material that, like that referring to promotional offers or bundled sales of medicinal products and other products, treats medicinal products in the same way as other consumer goods, which are in general the subject of discounts and price reductions where a certain level of expenditure is exceeded.

---

[108] Requirement laid down by Article 87(3) of Directive 2001/83.
[109] Restrictions set out in Article 90 of Directive 2001/83.
[110] On the basis of Article 87(3) of Directive 2001/83.

The Court concludes that, by prohibiting the dissemination of advertising material that encourages the irrational and excessive use of medicinal products that are neither subject to medical prescription nor reimbursed – without prejudice to the possibility for pharmacies to grant discounts and price reductions when selling medicinal products and other health products – a national provision such as that at issue in the main proceedings meets the essential aim of safeguarding public health and is therefore compatible with Directive 2001/83.

2. Liability of intermediary service providers

Judgment of 3 October 2019,* Glawischnig-Piesczek *(C-18/18, EU:C:2019:821)

Facebook Ireland operates a global social media platform ('Facebook Service') for users located outside of the United States of America and Canada. Ms Glawischnig-Piesczek was a member of the Nationalrat (National Council, Austria), chair of the parliamentary party 'die Grünen' (The Greens) and federal spokesperson for that party. On 3 April 2016, a Facebook Service user shared on that user's personal page an article from the Austrian online news magazine oe24.at entitled 'Greens: Minimum income for refugees should stay', which had the effect of generating on that page a 'thumbnail' of the original site, containing the title and a brief summary of the article, and a photograph of Ms Glawischnig-Piesczek. That user also published, in connection with that article, a comment which the referring court found to be harmful to the reputation of the applicant in the main proceedings, and which insulted and defamed her. This post could be accessed by any Facebook user.

In a letter of 7 July 2016, Ms Glawischnig-Piesczek, inter alia, asked Facebook Ireland to delete that comment. Because Facebook Ireland did not withdraw the comment in question, Ms Glawischnig-Piesczek brought an action before a commercial court which directed Facebook Ireland, with immediate effect and until the proceedings relating to the action for a prohibitory injunction have been finally concluded, to cease and desist from publishing and/or disseminating photographs showing the applicant in the main proceedings. Facebook Ireland disabled access in Austria to the content initially published.

On appeal, a higher regional court upheld the order made at first instance as regards the identical allegations. However, it also held that the dissemination of allegations of equivalent content had to cease only as regards those brought to the knowledge of Facebook Ireland by the applicant in the main proceedings, by third parties or otherwise. Each of the parties in the main proceedings lodged appeals on a point of law at the Oberster Gerichtshof (Supreme Court, Austria).

The request for a preliminary ruling mainly concerned the interpretation of Article 15(1) of Directive 2000/31/EC.

As a preliminary point, the Court noted that, in order to ensure that the host provider at issue prevents any further impairment of the interests involved, it is legitimate for the court having jurisdiction to be able to require that host provider to block access to the information stored, the content of which is identical to the content previously declared to be illegal, or to remove that information, irrespective of who requested the storage of that information.

Further, according to the Court, a court of a Member State is authorised to order a host provider to remove information which it stores, the content of which is identical to the content of information which was previously declared to be illegal, or to block access to that information, provided that the monitoring of and search for the information concerned by such an injunction are limited to information conveying a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality and containing the elements specified in the injunction, and provided that the differences in the wording of that equivalent content, compared with the wording characterising the information which was previously declared to be illegal, are not such as to require the host provider to carry out an independent assessment of that content.

Lastly, a court of a Member State may order a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law.

Judgment of 8 December 2022 (Grand Chamber)*, Google (De-referencing of allegedly inaccurate content) *(C-460/20, EU:C:2022:962)

The applicants in the main proceedings, TU, who occupies leadership positions and holds shares in various companies, and RE, who was his cohabiting partner and, until May 2015, held general commercial power of representation in one of those companies, were the subject of three articles published on a website in 2015 by G-LLC, the operator of that website. Those articles, one of which was illustrated by four photographs of the applicants and suggested that they led a life of luxury, criticised the investment model of a number of their companies. It was possible to access those articles by entering into the search engine operated by Google LLC ('Google') the surnames and forenames of the applicants, both on their own and in conjunction with certain company names. The list of results provided a link to those articles and to photographs in the form of thumbnails.

The applicants in the main proceedings requested Google, as the controller of personal data processed by its search engine, first, to de-reference the links to the articles at issue from the list of search results, on the ground that they contained inaccurate claims and defamatory opinions, and, second, to remove the thumbnails from the list of search results. Google refused to accede to that request.

Since they were unsuccessful at first instance and on appeal, the applicants in the main proceedings brought an appeal on a point of law before the Bundesgerichtshof (Federal Court of Justice, Germany), in the context of which the Bundesgerichtshof (Federal Court of Justice) made a request to the Court of Justice for a preliminary ruling on the interpretation of the GDPR [111] and Directive 95/46. [112]

By its judgment, delivered by the Grand Chamber, the Court develops its case-law on the conditions which apply to requests for de-referencing addressed to the operator of a search engine based on rules regarding the protection of personal data. [113] It examines, in particular, first, the extent of the obligations and responsibilities incumbent on the operator of a search engine in processing a request for de-referencing based on the alleged inaccuracy of the information in the referenced content and, second, the burden of proof imposed on the data subject as regards that inaccuracy. The Court also gives a ruling on the need, for the purposes of examining a request to remove photographs displayed in the form of thumbnails in the list of results of an image search, to take account of the original context of the publication of those photographs on the internet.

In the first place, the Court rules that, in the context of striking a balance between, on the one hand, the right to respect for private life and the protection of personal data, and on the other hand, the right to freedom of expression and information, [114] for the purposes of examining a request for de-referencing made to the operator of a search engine seeking the removal from the list of search results of a link to content containing allegedly inaccurate information, such de-referencing is not subject to the condition that the question of the accuracy of the referenced content has been resolved, at least provisionally, in an action brought by the person making that request against the content provider.

As a preliminary point, in order to examine the conditions in which the operator of a search engine is required to accede to a request for de-referencing and thus to remove from the list of results displayed following a search on the basis of the data subject's name, the link to an internet page on which allegations appear which that person regards as inaccurate, the Court stated, in particular, as follows:

– inasmuch as the activity of a search engine is liable to affect significantly, and additionally compared with that of the publishers of websites, the fundamental rights to privacy and to the protection of personal data, the operator of that search engine, as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the

[111] Article 17(3)(a) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1).

[112] Article 12(b) and point (a) of the first paragraph of Article 14 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).

[113] Judgments of 13 May 2014, *Google Spain and Google* (C-131/12, EU:C:2014:317), and of 24 September 2019, *GC and Others (De-referencing of sensitive data)* (C-136/17, EU:C:2019:773) and *Google (Territorial scope of de-referencing)* (C-507/17, EU:C:2019:772).

[114] Fundamental rights guaranteed by Articles 7, 8 and 11, respectively, of the Charter of Fundamental Rights of the European Union.

guarantees laid down by Directive 95/46 and the GDPR may have full effect and that effective and complete protection of data subjects may actually be achieved;

– where the operator of a search engine receives a request for de-referencing, it must ascertain whether the inclusion of the link to the internet page in question in the list of results is necessary for exercising the right to freedom of information of internet users potentially interested in accessing that internet page by means of such a search, a right protected by the right to freedom of expression and of information;

– the GDPR expressly lays down the requirement to strike a balance between the fundamental rights to privacy and protection of personal data, on the one hand, and the fundamental right of freedom of information on the other.

First of all, the Court finds that while the data subject's rights to respect for private life and the protection of personal data override, as a general rule, the legitimate interest of internet users who may be interested in accessing the information in question, that balance may, however, depend on the relevant circumstances of each case, in particular on the nature of that information and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.

The question of whether or not the referenced content is accurate also constitutes a relevant factor when making that assessment. Accordingly, in certain circumstances, the right of internet users to information and the content provider's freedom of expression may override the rights to private life and to protection of personal data, in particular where the data subject plays a role in public life. However, that relationship is reversed where, at the very least, a part – which is not minor in relation to the content as a whole – of the information referred to in the request for de-referencing proves to be inaccurate. In such a situation, the right to inform and the right to be informed cannot be taken into account, since they cannot include the right to disseminate and have access to such information.

Next, as regards, first, the obligations relating to establishing whether or not the information found in the referenced content is accurate, the Court clarifies that the person requesting the de-referencing on account of the inaccuracy of such information is required to establish the manifest inaccuracy of such information or, at the very least, of a part – which is not minor in relation to the content as a whole – of that information. However, in order to avoid imposing on that person an excessive burden which is liable to undermine the practical effect of the right to de-referencing, that person has to provide only evidence that, in the light of the circumstances of the particular case, can reasonably be required of him or her to try to find. In principle, that person cannot be required to produce, as from the pre-litigation stage, in support of his or her request for de-referencing, a judicial decision made against the publisher of the website, even in the form of a decision given in interim proceedings.

Second, as regards the obligations and responsibilities imposed on the operator of the search engine, the Court points out that the operator of a search engine must, in order to determine whether content may continue to be included in the list of search results carried out using its search engine following a request for de-referencing, take into account all the rights and interests involved and all the circumstances of the case. However, that operator cannot be obliged to investigate the facts and, to that end, to organise an adversarial debate with the content provider seeking to obtain missing information concerning the accuracy of the referenced content. An obligation to contribute to establishing whether or not the referenced content is accurate would impose on that operator a burden in excess of what can reasonably be expected of it in the light of its responsibilities, powers and capabilities. That solution would entail a serious risk that content meeting the public's legitimate and compelling need for information would be de-referenced and would thereby become difficult to find on the internet. There would, accordingly, be a real risk of a deterrent effect on the exercise of freedom of expression and of information if such an operator undertook such de-referencing quasi-systematically, in order to avoid having to bear the burden of investigating the relevant facts for the purpose of establishing whether or not the referenced content was accurate.

Therefore, where the person who has made a request for de-referencing submits evidence establishing the manifest inaccuracy of the information found in the referenced content or, at the very least, of a part – which is not minor in relation to the content as a whole – of that information, the operator of the search engine is required to accede to that request. The same applies where the person making that request submits a judicial decision made against the publisher of the website, which is based on the finding that information found in the referenced content – which is not minor in relation to that content as a whole – is, at least prima facie, inaccurate. By contrast, where the inaccuracy of such information is not obvious, in the light of the evidence provided by the person making the request, the operator of the search engine is not required, where there is no such judicial decision, to accede to such a request for de-referencing. Where the information in question is likely to contribute to a debate of public interest, it is appropriate, in the light of all the circumstances of the case, to place particular importance on the right to freedom of expression and of information.

Lastly, the Court adds that, where the operator of a search engine does not grant a request for de-referencing, the data subject must be able to bring the matter before the supervisory authority or the judicial authority so that it carries out the necessary checks and orders that controller to adopt the necessary measures. In that regard, the judicial authorities must ensure a balance is struck between competing interests, since they are best placed to carry out a complex and detailed balancing exercise, which takes account of all the criteria and all the factors established by the relevant case-law.

In the second place, the Court rules that, within the context of weighing up fundamental rights mentioned above, for the purposes of examining a request for de-referencing

seeking the removal from the results of an image search carried out on the basis of the name of a natural person of photographs displayed in the form of thumbnails representing that person, account must be taken of the informative value of those photographs regardless of the original context of their publication on the internet page from which they are taken. However, it is necessary to take into consideration any text element which accompanies directly the display of those photographs in the search results and which is capable of casting light on the informative value of those photographs.

In reaching that conclusion, the Court notes that image searches carried out by means of an internet search engine on the basis of a person's name are subject to the same principles as those which apply to internet page searches and the information contained in them. It states that displaying, following a search by name, photographs of the data subject in the form of thumbnails, is such as to constitute a particularly significant interference with the data subject's rights to private life and that person's personal data.

Consequently, when the operator of a search engine receives a request for de-referencing which seeks the removal, from the results of an image search carried out on the basis of the name of a person, of photographs displayed in the form of thumbnails representing that person, it must ascertain whether displaying the photographs in question is necessary for exercising the right to freedom of information of internet users who are potentially interested in accessing those photographs by means of such a search.

In so far as the search engine displays photographs of the data subject outside the context in which they are published on the referenced internet page, most often in order to illustrate the text elements contained in that page, it is necessary to establish whether that context must nevertheless be taken into consideration when striking a balance between the competing rights and interests. In that context, the question whether that assessment must also include the content of the internet page containing the photograph displayed in the form of a thumbnail, the removal of which is sought, depends on the purpose and nature of the processing at issue.

As regards, first, the purpose of the processing at issue, the Court notes that the publication of photographs as a non-verbal means of communication is likely to have a stronger impact on internet users than text publications. Photographs are, as such, an important means of attracting internet users' attention and may encourage an interest in accessing the articles they illustrate. Since, in particular, photographs are often open to a number of interpretations, displaying them in the list of search results as thumbnails may result in a particularly serious interference with the data subject's right to protection of his or her image, which must be taken into account when weighing-up competing rights and interests. A separate weighing-up exercise is required depending on whether the case concerns, on the one hand, articles containing photographs which are published on an internet page and which, when placed into their original context, illustrate the information provided in those articles and the opinions expressed in them,

or, on the other hand, photographs displayed in the list of results in the form of thumbnails by the operator of a search engine outside the context in which they were published on the original internet page.

In that regard, the Court recalls that not only does the ground justifying the publication of a piece of personal data on a website not necessarily coincide with that which is applicable to the activity of search engines, but also, even where that is the case, the outcome of the weighing-up of the rights and interests at issue may differ according to whether the processing carried out by the operator of a search engine or that carried out by the publisher of that internet page is at issue. The legitimate interests justifying such processing may be different and, also, the consequences of the processing for the data subject, and in particular for his or her private life, are not necessarily the same. [115]

As regards, second, the nature of the processing carried out by the operator of the search engine, the Court observes that, by retrieving the photographs of natural persons published on the internet and displaying them separately, in the results of an image search, in the form of thumbnails, the operator of a search engine offers a service in which it carries out autonomous processing of personal data which is distinct both from that of the publisher of the internet page from which the photographs are taken and from that, for which the operator is also responsible, of referencing that page.

Therefore, an autonomous assessment of the activity of the operator of the search engine, which consists of displaying results of an image search, in the form of thumbnails, is necessary, as the additional interference with fundamental rights resulting from such activity may be particularly intense owing to the aggregation, in a search by name, of all information concerning the data subject which is found on the internet. In the context of that autonomous assessment, account must be taken of the fact that that display constitutes, in itself, the result sought by the internet user, regardless of his or her subsequent decision to access the original internet page or not.

The Court observes, however, that such a specific weighing-up exercise, which takes account of the autonomous nature of the data processing performed by the operator of the search engine, is without prejudice to the possible relevance of text elements which may directly accompany the display of a photograph in the list of search results, since such elements are capable of casting light on the informative value of that photograph for the public and, consequently, of influencing the weighing-up of the rights and interests involved.

[115] See judgment *Google Spain and Google* (C-131/12, EU:C:2014:317, paragraph 86).

3. Competition law

Judgment of 13 October 2011, **Pierre Fabre** *(C-439/09, EU:C:2011:649)*

The company Pierre Fabre Dermo-Cosmétique ('PFDC') manufactured and marketed cosmetics through pharmacists on the European market. The products at issue were not classified as medicines. However, the distribution contracts for those products stipulated that sales had to be made exclusively in a physical space and in the presence of a qualified pharmacist, thereby limiting, in practice, all forms of selling by internet. The French competition authority decided that, owing to the de facto ban on all internet sales, PFDC's distribution contracts constituted anticompetitive agreements of the kind contrary to French law and EU competition law. PFDC challenged that decision before the cour d'appel de Paris (Court of Appeal, Paris, France), which asked the Court of Justice whether a general and absolute ban on internet sales constitutes a restriction of competition 'by object', whether such an agreement could be eligible for a block exemption, and whether, if the block exemption does not apply, it could be eligible for an individual exemption under Article 101(3) TFEU.

The Court replied that Article 101(1) TFEU must be interpreted as meaning that, in the context of a selective distribution system, a contractual clause amounts to a restriction by object within the meaning of that provision where, following an individual examination, that clause is not objectively justified. Such a contractual clause considerably reduces the ability of an authorised distributor to sell the contractual products to customers outside its contractual territory or area of activity. It is therefore liable to restrict competition in that sector.

However, there are legitimate requirements, such as the maintenance of a specialist trade capable of providing specific services as regards high-quality and high-technology products, which may justify a reduction of price competition in favour of competition relating to factors other than price. In that regard, the organisation of a selective distribution system is not prohibited by Article 101(1) TFEU, to the extent that resellers are chosen on the basis of objective criteria of a qualitative nature, laid down uniformly for all potential resellers and not applied in a discriminatory fashion, that the characteristics of the product in question necessitate such a network in order to preserve its quality and ensure its proper use and, finally, that the criteria laid down do not go beyond what is necessary. As regards, in particular, the sale of cosmetics and personal care products, the aim of maintaining a prestigious image is not a legitimate aim for restricting competition.

Article 4(c) of Regulation (EC) No 2790/1999 [116] must be interpreted as meaning that the block exemption provided for in Article 2 of that regulation does not apply to vertical

[116] Commission Regulation (EC) No 2790/1999 of 22 December 1999 on the application of Article 81(3) of the Treaty to categories of vertical agreements and concerted practices (OJ 1999 L 336, p. 21).

agreements which have as their object the restriction of active or passive sales to end users by members of a selective distribution system operating at the retail level of trade, without prejudice to the possibility of prohibiting a member of the system from operating out of an unauthorised place of establishment.

Judgment of 6 December 2017, **Coty Germany** *(C-230/16, EU:C:2017:941)*

Coty Germany sold luxury cosmetics in Germany. In order to preserve its luxury image, it marketed certain brands through a selective distribution network, namely through authorised distributors. The sales locations of those authorised distributors had to satisfy a number of requirements relating to their environment, decor and furnishing. Furthermore, the authorised distributors were permitted to sell the goods in issue online provided they used their own electronic shop window or unauthorised third-party platforms where the use of such platforms was not discernible to the consumer. On the other hand, they were expressly prohibited from selling the goods online through third-party platforms operating in a discernible manner towards consumers.

Coty Germany brought an action before the German courts against one of its authorised distributors, Parfümerie Akzente, seeking an order prohibiting it, in accordance with that contractual clause, from distributing Coty goods through the platform 'amazon.de'. Being unsure whether that clause was lawful under EU competition law, the Oberlandesgericht Frankfurt am Main (Higher Regional Court, Frankfurt am Main, Germany) submitted a question to the Court of Justice for a preliminary ruling in that regard.

According to the Court, Article 101(1) TFEU must be interpreted as meaning that such a selective distribution system designed to preserve the luxury image of those goods complies with that provision to the extent that resellers are chosen on the basis of objective criteria of a qualitative nature that are laid down uniformly for all potential resellers and applied in a non-discriminatory fashion and that the criteria laid down do not go beyond what is necessary.

Furthermore, Article 4 of Regulation (EU) No 330/2010 [117] must be interpreted as meaning that the prohibition imposed on the members of a selective distribution system for luxury goods, which operate as distributors at the retail level of trade, of making use, in a discernible manner, of third-party undertakings for internet sales does not constitute a restriction of customers, within the meaning of Article 4(b), or a restriction of passive sales to end users, within the meaning of Article 4(c) of that regulation.

[117] Commission Regulation (EU) No 330/2010 of 20 April 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices (OJ 2010 L 102, p. 1).

Judgment of 4 July 2023 (Grand Chamber),* Meta Platforms and Others (General terms of use of a social network) *(C-252/21, EU:C:2023:537)

Meta Platforms owns the online social network Facebook, which is free of charge for private users. The business model of that social network is based on financing through online advertising, which is tailored to its individual users. That advertising is made possible in technical terms by the automated production of detailed profiles in respect of the network users and the users of the online services offered at the level of the Meta group. In order to be able to use that social network, when they register, users must accept the general terms drawn up by Meta Platforms, which refer to the data and cookies policies set by that company. Under those policies, in addition to the data which those users provide directly when they register, Meta Platforms also collects data about user activities on and off the social network and links the data with the Facebook accounts of the users concerned. The latter data, also known as 'off-Facebook data', are data concerning visits to third-party webpages and apps as well as data concerning the use of other online services belonging to the Meta group (including Instagram and WhatsApp). The aggregate view of the data thus collected allows detailed conclusions to be drawn about those users' preferences and interests.

By decision of 6 February 2019, the Bundeskartellamt (Federal Cartel Office, Germany), prohibited Meta Platforms, first, from making, in the general terms in force at the time, [118] the use of the social network Facebook by private users resident in Germany subject to the processing of their off-Facebook data and, second, from processing those data without their consent. In addition, the Federal Cartel Office required Meta Platforms to adapt those general terms in such a way that it is made clear that those data will neither be collected nor linked with Facebook user accounts nor used without the consent of the users concerned. Last, the office clarified that such a consent was not valid if it was a condition for using the social network. It based its decision on the fact that the processing of the data at issue, which it found to be inconsistent with the GDPR, [119] constitutes an abuse of Meta Platforms' dominant position on the market for online social networks.

Meta Platforms brought an action against that decision before the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany). Having doubts as to (i) whether national competition authorities may review whether the processing of personal data complies with the requirements set out in the GDPR and (ii) the interpretation and application of certain provisions of that regulation, the Higher Regional Court, Düsseldorf, referred the matter to the Court of Justice for a preliminary ruling.

---

[118] On 31 July 2019, Meta Platforms introduced new general terms expressly stating that the user agrees to be shown advertisements instead of paying to use Facebook products.

[119] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1, and corrigendum OJ 2018 L 127, p. 2) ('the GDPR').

By its judgment, the Court, sitting as the Grand Chamber, rules on the powers of a national competition authority to find that the processing of personal data is not consistent with the GDPR as well as on how to reconcile this with the powers of the national data protection supervisory authorities. [120] Moreover, it provides clarification on whether users' 'sensitive' personal data may be processed by the operator of a social network, on the conditions for lawful data processing by such an operator and on whether consent given for the purposes of such processing by those users to an undertaking holding a dominant position on the national market for online social networks is valid.

In the first place, with regard to the powers of a competition authority to find that the processing of personal data is not consistent with the GDPR, the Court holds that, subject to compliance with its duty of sincere cooperation [121] with the data protection supervisory authorities, such an authority can find, in the context of the examination of an abuse of a dominant position by an undertaking, [122] that that undertaking's general terms of use relating to the processing of personal data and the implementation thereof are not consistent with that regulation, where that finding is necessary to establish the existence of such an abuse. Nevertheless, where a competition authority identifies an infringement of the GDPR in the context of the finding of an abuse of a dominant position, it does not replace the supervisory authorities.

Thus, in the light of the principle of sincere cooperation, when competition authorities are called upon, in the exercise of their powers, to examine whether an undertaking's conduct is consistent with the provisions of the GDPR, they are required to consult and cooperate sincerely with the national supervisory authorities concerned or with the lead supervisory authority. All of these authorities are then bound to observe their respective powers and competences, in such a way as to ensure that the obligations arising from the GDPR and the objectives of that regulation are complied with while their effectiveness is safeguarded. It follows that, where, in the context of the examination seeking to establish whether there is an abuse of a dominant position by an undertaking, a competition authority takes the view that it is necessary to examine whether that undertaking's conduct is consistent with the provisions of the GDPR, that authority must ascertain whether that conduct or similar conduct has already been the subject of a decision by the competent national supervisory authority or the lead supervisory authority or the Court. If that is the case, the competition authority cannot depart from it, although it remains free to draw its own conclusions from the point of view of the application of competition law.

Where it has doubts as to the scope of the assessment carried out by the competent national supervisory authority or the lead supervisory authority, where the conduct in question or similar conduct is, simultaneously, under examination by those authorities,

[120] Within the meaning of Articles 51 to 59 of the GDPR.
[121] Enshrined in Article 4(3) TEU.
[122] Within the meaning of Article 102 TFEU.

or where, in the absence of investigation by those authorities, it takes the view that an undertaking's conduct is not consistent with the provisions of the GDPR, the competition authority must consult these authorities and seek their cooperation in order to dispel its doubts or to determine whether it must wait for the supervisory authority concerned to take a decision before starting its own assessment. In the absence of any objection from them or of a reply within a reasonable time, the competition authority may continue its own investigation.

In the second place, with regard to the processing of special categories of personal data, [123] the Court finds that, where the user of an online social network visits websites or apps to which one or more of those categories relate and, as the case may be, enters information into them when registering or when placing online orders, the processing of personal data by the operator of that online social network [124] must be regarded as 'processing of special categories of personal data' within the meaning of Article 9(1) of the GDPR, where it allows information falling within one of those special categories to be revealed, irrespective of whether that information concerns a user of that network or any other natural person. Such data processing is in principle prohibited, subject to certain derogations. [125]

In the latter regard, the Court states that, where the user of an online social network visits websites or apps to which one or more of those special categories relate, the user does not manifestly make public [126] the data relating to those visits collected by the operator of that online social network via cookies or similar storage technologies. Moreover, where he or she enters information into such websites or apps or where he or she clicks or taps on buttons integrated into those sites and apps, such as the 'Like' or 'Share' buttons or buttons enabling the user to identify himself or herself on those sites or apps using login credentials linked to his or her social network user account, his or her telephone number or email address, that user manifestly makes public the data thus entered or resulting from the clicking or tapping on those buttons only in the circumstance where he or she has explicitly made the choice beforehand, as the case may be on the basis of individual settings selected with full knowledge of the facts, to make the data relating to him or her publicly accessible to an unlimited number of persons.

---

123 Referred to in Article 9(1) of the GDPR. Under this provision, 'processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited'.

124 That processing entails the collection – by means of integrated interfaces, cookies or similar storage technologies – of data from visits to those sites and apps and of the information entered by the user, the linking of all those data with the user's social network account and the use of those data by that operator.

125 Provided for in Article 9(2) of the GDPR. That article provides that 'paragraph 1 shall not apply if one of the following applies:
(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
...
(e) processing relates to personal data which are manifestly made public by the data subject;
(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
...'.

126 Within the meaning of Article 9(2)(e) of the GDPR.

In the third place, as regards more generally the conditions for the lawful processing of personal data, the Court recalls that, under the GDPR, data processing is lawful if and to the extent that the data subject has given consent for one or more specific purposes. [127] In the absence of such a consent, or where that consent was not freely given, specific, informed and unambiguous, such processing is nevertheless justified if it meets one of the requirements of necessity, [128] which must be interpreted strictly. The processing of the personal data of its users by the operator of an online social network can be regarded as necessary for the performance of a contract to which those users are party only on condition that the processing is objectively indispensable for a purpose that is integral to the contractual obligation intended for those users, such that the main subject matter of the contract cannot be achieved if that processing does not occur.

In addition, according to the Court, the data processing at issue can be regarded as necessary for the purposes of the legitimate interests pursued by the controller or by a third party only on condition that the operator has informed the users from whom the data have been collected of a legitimate interest that is pursued by the data processing, that such processing is carried out only in so far as is strictly necessary for the purposes of that legitimate interest and that it is apparent from a balancing of the opposing interests, having regard to all the relevant circumstances, that the interests or fundamental freedoms and rights of those users do not override that legitimate interest of the controller or of a third party. The Court finds, inter alia, that in the absence of consent on their part, the interests and fundamental rights of those users override the interest of the operator of an online social network in personalised advertising through which it finances its activity.

Last, the Court specifies that the processing of personal data at issue is justified where it is actually necessary for compliance with a legal obligation to which the controller is subject, pursuant to a provision of EU law or the law of the Member State concerned, where that legal basis meets an objective of public interest and is proportionate to the legitimate aim pursued and where that processing is carried out only in so far as is strictly necessary.

In the fourth and last place, as regards the validity of the consent of the users concerned to the processing of their data under the GDPR, the Court holds that the fact that the operator of an online social network holds a dominant position on the market for online social networks does not, as such, preclude the users of such a network from being able validly to consent to the processing of their personal data by that operator. However, since that position is liable to affect the freedom of choice of those users and to create a clear imbalance between them and the controller, it is an important factor in

[127] Within the meaning of point (a) of the first subparagraph of Article 6(1) of the GDPR.

[128] Referred to in points (b) to (f) of the first subparagraph of Article 6(1) of the GDPR. Under those provisions, processing is lawful only if and to the extent that it is, inter alia, necessary for the performance of a contract to which the data subject is party (point (b) of the first subparagraph of Article 6(1) of the GDPR), for compliance with a legal obligation to which the controller is subject (point (c) of the first subparagraph of Article 6(1) of the GDPR) or for the purposes of the legitimate interests pursued by the controller or by a third party (point (f) of the first subparagraph of Article 6(1) of the GDPR).

determining whether the consent was in fact validly and, in particular, freely given, which it is for that operator to prove. [129]

In particular, the users of the social network in question must be free to refuse individually, in the context of the contractual process, to give their consent to particular data processing operations not necessary for the performance of the contract, without being obliged to refrain entirely from using that online social network, which means that those users are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations. Moreover, it must be possible to give separate consent for the processing of off-Facebook data.

4. Online sales of medicinal products and medical devices

Judgment of 11 December 2003 (Grand Chamber),* Deutscher Apothekerverband *(C-322/01, EU:C:2003:664)

The main proceedings involved a dispute between Deutscher Apothekerverband eV, an association for the protection of the economic and social interests of pharmacists, and 0800 DocMorris NV, a Dutch pharmacy established in the Netherlands. Mr Jacques Waterval was a pharmacist and one of the legal representatives of DocMorris. Since June 2000, DocMorris and Mr Waterval had been offering medicinal products for sale at the internet address www.0800DocMorris.com. The medicinal products in issue were authorised either in Germany or the Netherlands. This type of medicinal product was supplied only on production of the original prescription. The Apothekerverband challenged, before the Landgericht Frankfurt am Main (Regional Court, Frankfurt am Main, Germany), the offer of medicinal products for sale over the internet and their delivery by international mail order. It argued that the provisions of the German law on medicinal products did not permit the pursuit of a business of that kind. The national court asked the Court of Justice whether such prohibitions infringe the principle of the free movement of goods. Next, assuming that there is an infringement of Article 28 EC, the national court sought to ascertain whether the German legislation at issue in the main action is necessary for the effective protection of the health and life of humans for the purposes of Article 30 EC.

The Court held that the national prohibition was a measure having equivalent effect within the meaning of Article 28 EC. It has a greater impact on pharmacies established outside national territory and could impede access to the market for products from other Member States more than it impedes access for domestic products.

[129] Pursuant to Article 7(1) of the GDPR.

Article 30 EC may justify such a national prohibition in so far as it covers medicinal products subject to prescription. Given that there may be risks attaching to the use of those medicinal products, it is necessary to be able to check effectively and responsibly the authenticity of doctors' prescriptions and thus to ensure that the medicine is handed over either to the customer himself, or to a person to whom its collection has been entrusted by the customer. However, Article 30 EC cannot be relied on to justify an absolute prohibition on the sale by mail order of medicinal products.

Furthermore, Article 88(1) of Directive 2001/83/EC [130] precludes a national prohibition on advertising the sale by mail order of medicinal products which may be supplied only in pharmacies in the Member State concerned, in so far as the prohibition covers medicinal products which are not subject to prescription.

Article 88(2) of Directive 2001/83/EC, which allows medicinal products not subject to prescription to be advertised to the general public, cannot be interpreted as precluding advertising for the sale by mail order of medicinal products on the basis of the alleged need for a pharmacist to be physically present.

Judgment of 2 December 2010,* Ker-Optika *(C-108/09, EU:C:2010:725)

Under Hungarian law, contact lenses could only be sold in a specialist shop with a minimum area of 18 m² or in premises separated from the workshop. Furthermore, the sale of those goods required the services of an optometrist or an ophthalmologist qualified in the field of contact lenses to be used. However, the Hungarian company Ker-Optika sold contact lenses on its website. The Hungarian health authorities prohibited it from pursuing that business. Ker-Optika challenged that prohibition before the courts. The Baranya megyei bíróság (County Court, Baranya, Hungary), before which the case was brought, asked the Court of Justice whether EU law precluded the Hungarian legislation.

The Court replied that the national rules relating to the selling of contact lenses fall within the scope of Directive 2000/31/EC [131] in so far as they relate to the online offer and the conclusion of the contract by electronic means. On the other hand, the national rules relating to the supply of contact lenses are not covered by that directive. Articles 34 TFEU and 36 TFEU and Directive 2000/31/EC must be interpreted as precluding national legislation which authorises the selling of contact lenses only in shops which specialise in medical devices.

That legislation constitutes a measure having an effect equivalent to a quantitative restriction, as prohibited by Article 34 TFEU, since the prohibition concerns the sale of

[130] Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (OJ 2001 L 311, p. 67).

[131] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (OJ 2000 L 178, p. 1).

contact lenses via the internet by mail order and the delivery to the home of customers resident in national territory and deprives traders from other Member States of a particularly effective means of selling those products, thus significantly impeding access of those traders to the market of the Member State concerned.

The national legislature exceeded the limits of the discretion it enjoys to determine the level of protection which it wishes to afford to public health and the legislation at issue must be held to go beyond what is necessary to attain the objective pursued. That objective may be achieved by less restrictive measures, namely measures which subject to certain restrictions only the first supply of lenses and which require the economic operators concerned to make available a qualified optician to the customer. For the same reasons, that legislation cannot be held to be proportionate to the objective of ensuring the protection of public health, for the purposes of Article 3(4) of Directive 2000/31/EC.

Judgment of 19 October 2016, **Deutsche Parkinson Vereinigung** *(C-148/15, EU:C:2016:776)*

The Deutsche Parkinson Vereinigung, a German self-help organisation aiming to improve the lives of patients suffering from Parkinson's disease, agreed upon a bonus system with the Dutch mail-order pharmacy DocMorris. Its members were eligible for the bonus system if they purchased prescription-only medicinal products for Parkinson's disease available only from pharmacies. A German association for protection against unfair competition considered that the bonus system infringed German law, which provided for uniform pharmacy retail prices for prescription-only medicinal products.

The Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany) asked the Court of Justice whether the setting of uniform prices is compatible with the free movement of goods.

The Court held that Article 34 TFEU must be interpreted as meaning that the national legislation constitutes a measure having equivalent effect to a quantitative restriction on imports. That legislation has a greater impact on the sale of prescription-only medicinal products by pharmacies established in other Member States than on the sale of the same medicinal products by pharmacies established within the national territory.

Traditional pharmacies are better placed than mail-order pharmacies to provide patients with individually tailored advice and to ensure a supply of medicinal products in cases of emergency. It must be held that price competition is capable of providing a more important factor of competition for mail-order pharmacies than for traditional pharmacies.

Article 36 TFEU must be interpreted as meaning that national legislation cannot be justified on grounds of the protection of health and life of humans, inasmuch as that legislation is not appropriate for attaining the objectives pursued. The objective of ensuring a safe and high-quality supply of medicinal products throughout a Member

State comes within the ambit of Article 36 TFEU. However, such legislation can be properly justified only if it is appropriate for securing the attainment of the legitimate objective pursued and does not go beyond what is necessary in order to attain it.

Increased price competition between pharmacies would be conducive to a uniform supply of medicinal products and does not adversely affect traditional pharmacies in performing certain activities in the general interest, such as producing prescription medicinal products or maintaining a given stock and selection of medicinal products. Lastly, price competition could be capable of benefiting the patient in so far as it would allow for prescription-only medicinal products to be offered at more attractive prices.

Judgment of 29 February 2024, **Doctipharma** *(C-606/21, EU:C:2024:179)*

Hearing a reference for a preliminary ruling from the Cour d'appel de Paris (Court of Appeal, Paris, France), the Court of Justice clarifies the concept of an 'information society service' and provides a basis for assessing whether a Member State's prohibition of a service provided by means of a website and consisting of connecting pharmacists and customers for the online sale of non-prescription medicinal products ('the service provided') complies with EU law.

Doctipharma set up the www.doctipharma.fr website, where internet users could buy pharmaceutical products and medicinal products not subject to prescription from pharmacy websites.

On that website, pharmacists subscribed to the online sales platform through a monthly subscription paid to Doctipharma, and customers had to create a customer account in order to access the websites of the pharmacists of their choice.

Since the Union des Groupements de pharmaciens d'officine (UDGPO) considers that that practice involved Doctipharma in the e-commerce of medicinal products, it brought an action against Doctipharma before the Tribunal de commerce de Nanterre (Commercial Court, Nanterre, France), which found that the website was unlawful and ordered Doctipharma to cease its activity. The Cour de cassation (Court of Cassation, France) set aside the decision of the Cour d'appel de Versailles (Court of Appeal, Versailles, France), which had overturned the lower court's judgement. It held that, by connecting dispensing pharmacists with potential patients, Doctipharma had acted as an intermediary in the sale of non-prescription medicinal products and participated in the e-commerce of medicinal products, without, however, having the status of pharmacist required by national legislation. It referred the case back to the Cour d'appel de Paris (Court of Appeal, Paris), the referring court in this case.

Confronted with the different approaches adopted by the French courts, the referring court decided to refer several questions to the Court of Justice for a preliminary ruling. It

asks the Court to interpret Directive 98/34, [132] in order to determine whether the service provided falls within the concept of an 'information society service', and Article 85c of Directive 2001/83, [133] in order to determine whether the Member States may, on the basis of that provision, prohibit the provision of the service in question.

In the first place, as regards the conditions to be satisfied in order to classify a service as falling within the concept of an 'information society service' for the purposes of Directives 98/34 and 2015/1535, [134] the Court considers, first of all, that it is irrelevant, first, whether Doctipharma was remunerated by the pharmacists who subscribed to its platform on the basis of a flat-rate fee and, secondly, whether the service provided by Doctipharma was subject to a monthly subscription fee paid to it by pharmacists and to a retrocession of a percentage of the amount of sales, deducted by the platform, since those circumstances, if proven, imply that the service in question must be regarded as fulfilling the condition of being provided in return for payment. Next, the classification of the service in question as an 'information society service' also follows from the fact that it is provided via a website that does not require the simultaneous presence of the service provider and the customer or pharmacist, and from the fact that the service is provided at the individual request of pharmacists and customers.

The Court concludes that a service provided on a website, connecting pharmacists and customers for the sale, via the websites of pharmacies which have subscribed to the service, of medicinal products not subject to medical prescription, falls within the concept of an 'information society service'.

In the second place, as regards the possibility for the Member States to prohibit such an intermediation service under Article 85c of Directive 2001/83, the Court points out that the Member States alone are competent to determine the natural or legal persons authorised or entitled to supply medicinal products to the public at a distance by means of information society services.

It considers that Article 85c(1)(a) of Directive 2001/83 requires the referring court to determine whether the provider of the service in question must be regarded as merely connecting sellers and customers by means of a service which is specific to and distinct from the sale, or whether that provider must be regarded as itself providing the sale.

In that regard, in the present case, if, following that analysis, Doctipharma were to be regarded as itself providing the service, Article 85c(1)(a) would not preclude the prohibition of that service by the Member State in whose territory it is established. A

[132] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services (OJ 1998 L 204, p. 37), as amended by Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 (OJ 1998 L 217, p. 18) ('Directive 98/34').

[133] Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (OJ 2001 L 311, p. 67), as amended by Directive 2011/62/EU of the European Parliament and of the Council of 8 June 2011 (OJ 2011 L 174, p. 74).

[134] Article 1(2) of Directive 98/34 and Article 1(1)(b) of Directive 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ 2015 L 241, p. 1) are worded identically. Those articles define the concept of 'information society service' on the basis of four conditions: 'any service normally provided for remuneration, at a distance, by electronic means, and at the individual request of a recipient of services'.

Member State may restrict the distance selling of non-prescription medicinal products to the public by means of information society services to persons who are qualified pharmacists.

Conversely, if Doctipharma were found to be providing a service of its own distinct from selling, then the service provided could not be prohibited on the basis of Article 85c(2) of Directive 2001/83 and would not fall within the concept of 'conditions for the retail supply' of medicinal products offered for distance selling to the public. The service provided must be classified as an 'information society service'. Article 85c(1) explicitly provides that, without prejudice to national legislation prohibiting the offer for distance selling to the public of medicinal products subject to prescription, Member States are to ensure that medicinal products are offered for distance selling to the public by means of information society services. It would therefore be inconsistent to hold that the use of such a service could be prohibited by the Member States.

5. Games of chance

Judgment of 6 November 2003 (Grand Chamber), **Gambelli** *(C-243/01, EU:C:2003:597)*

Mr Piergiorgio Gambelli and 137 other individuals ran data transmission centres in Italy which collected sporting bets in that Member State on behalf of an English bookmaker to which they were linked by the internet. The bookmaker, Stanley International Betting Ltd, carried on its business under a licence granted by the City of Liverpool pursuant to English law. In Italy, that business was reserved to the State or its licensees. Any infringement of that rule was liable to result in a criminal penalty of up to one year's imprisonment. Criminal proceedings were brought against Mr Gambelli. He argued that the provisions of Italian law were contrary to the Community principles of freedom of establishment and freedom to provide services. The Tribunale di Ascoli Piceno (District Court, Ascoli Piceno, Italy), before which the case had been brought, asked the Court of Justice how to interpret the relevant provisions of the EC Treaty.

The Court held that such national legislation constitutes a restriction on the freedom of establishment and the freedom to provide services provided for in Articles 43 EC and 49 EC respectively. In order to be justified, it must be based on imperative requirements in the general interest, be suitable for achieving the objective pursued, not go beyond what is necessary in order to attain that objective and be applied without discrimination.

It is for the national courts to determine whether such legislation, having regard to the detailed rules for its application, actually serves the aims which might justify it, and whether the restrictions it imposes are disproportionate in the light of those aims.

The Court also found that in so far as the authorities of a Member State incite and encourage consumers to participate in lotteries, games of chance and betting to the

financial benefit of the public purse, the authorities of that State cannot invoke public order concerns relating to the need to reduce opportunities for betting in order to justify measures such as those at issue in the main proceedings.

Judgment of 8 September 2009 (Grand Chamber), **Liga Portuguesa and Bwin International** *(C-42/07, EU:C:2009:519)*

Bwin, an online gambling undertaking which has its registered office in Gibraltar (United Kingdom) and has no establishment in Portugal, offered games of chance on a website. Its servers were in Gibraltar and Austria. La Liga, a private-law legal person, made up of all the clubs taking part in football competitions at professional level in Portugal, changed its name to Bwin Liga, as Bwin had become the main institutional sponsor of the First Football Division in Portugal. La Liga's website included references and a link to Bwin's website.

The directors of the Gaming Department of Santa Casa subsequently adopted decisions imposing fines on La Liga and Bwin for promoting games of a social nature and also for advertising such gambling. La Liga and Bwin brought actions before the Tribunal de Pequena Instância Criminal do Porto (Local Criminal Court, Oporto, Portugal) seeking the annulment of those decisions on the basis of, inter alia, Articles 43 EC, 49 EC and 56 EC.

The Court held that where a national measure relates to several fundamental freedoms at the same time, the Court will in principle examine the measure in relation to only one of those freedoms if it appears, in the circumstances of the case, that the other freedoms are entirely secondary in relation to the first and may be considered together with it.

Next, it found that such legislation gives rise to a restriction on the freedom to provide services enshrined in Article 49 EC, by also imposing a restriction on the freedom of the residents of the Member State concerned to enjoy, via the internet, services which are offered in other Member States. However, the restriction may be regarded as justified by the objective of combating fraud and crime.

The sector involving games of chance offered via the internet has not been the subject of Community harmonisation. A Member State is therefore entitled to take the view that the mere fact that a private operator lawfully offers services via the internet in another Member State, in which it is established, cannot be regarded as amounting to a sufficient assurance that national consumers will be protected. In addition, because of the lack of direct contact between consumer and operator, games of chance accessible via the internet involve different risks of fraud. Moreover, the possibility cannot be ruled out that an operator which sponsors some of the sporting competitions on which it accepts bets might be in a position to influence their outcome and thus increase its profits. Article 49 EC does not preclude legislation of a Member State which prohibits private operators established in other Member States, in which they lawfully provide

similar services, from offering games of chance via the internet within the territory of that Member State.

Judgment of 22 June 2017, **Unibet International** *(C-49/16, EU:C:2017:491)*

The Maltese company Unibet International organised online games of chance. In 2014, Unibet, which held licences issued by several Member States, provided online games of chance on Hungarian-language websites although it did not have the necessary licence in Hungary. The Hungarian authorities ordered the temporary closure of access to Unibet's websites from Hungary and imposed a fine on Unibet. It was theoretically possible for operators established in other Member States to be granted a licence for the organisation of online games of chance in so far as the provision of such services was not reserved to a State monopoly. However, it was, in practice, impossible for them to secure such a licence. Against that background, the Fővárosi Közigazgatási és Munkaügyi Bíróság (Budapest Administrative and Labour Court, Hungary) asked the Court of Justice whether the Hungarian legislation at issue was compatible with the principle of the freedom to provide services.

The Court held that Article 56 TFEU must be interpreted as precluding domestic legislation which introduces a system of concessions for the organisation of online games of chance, if it contains discriminatory rules with regard to operators established in other Member States or if it lays down rules which are not discriminatory but which are applied in an manner which is not transparent in such a way as to prevent or hinder an application from tenderers established in other Member States.

A rule according to which trustworthy operators must have carried out, for a period of at least 10 years, an activity of organisation of games of chance in the territory of that Member State puts operators established in other Member States at a disadvantage. The mere fact of putting forward an objective of general interest cannot suffice to justify such a difference in treatment.

The national requirement to have carried out an activity of organising games of chance for three years in a Member State does not create an advantage for operators established in the host Member State and could be justified by a general interest objective. However, it is important that the rules in question are applied transparently to all tenderers. That requirement is not satisfied by national legislation whose conditions governing the exercise of the powers of the Minister for the Economy which it sets in such a procedure and technical conditions having to be fulfilled by operators of games of chance when submitting their tenders are not defined with sufficient precision.

Article 56 TFEU must be interpreted as precluding penalties imposed for the infringement of national legislation introducing a system of concessions and licences for the organisation of games of chance, if such national legislation proves to be contrary to that article.

6. Sharing economy

Judgment of 20 December 2017 (Grand Chamber),* Asociación Profesional Élite Taxi *(C-434/15, EU:C:2017:981)

The electronic platform Uber provided, by means of an application, a paid service consisting of connecting non-professional drivers using their own vehicle. In 2014, a professional taxi drivers' association in Barcelona (Spain) brought an action before the Juzgado de lo Mercantil no 3 de Barcelona (Commercial Court No 3, Barcelona, Spain). It argued that Uber's activities amounted to misleading practices and acts of unfair competition. The Commercial Court considered it necessary to ascertain whether Uber required prior administrative authorisation. If the service was covered by the Directive on services in the internal market [135] or Directive 98/34/EC, [136] Uber's practices could not be regarded as unfair practices.

The Court held that the questions submitted by the national court concerned the legal classification of the service at issue and that it therefore had jurisdiction to reply to them.

Thus, such a service could be classified as an 'information society service', within the meaning of Article 1(2) of Directive 98/34/EC, to which Article 2(a) of Directive 2000/31/EC refers. That service is a 'service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services'.

It is more than an intermediation service consisting of connecting, by means of a smartphone application, a non-professional driver using his or her own vehicle with a person who wishes to make an urban journey. In a situation such as that with which the referring court is concerned, the provider simultaneously offers urban transport services, which it renders accessible through the application and whose general operation it organises.

Without the application, drivers would not be led to provide transport services and passengers would not use the services of those drivers. In addition, Uber exercises decisive influence over the conditions under which the service is provided by those drivers and determines at least the maximum fare by means of the eponymous application, which it receives from the client before paying part of it to the non-professional driver of the vehicle. It also exercises a certain control over the quality of the vehicles, the drivers and their conduct, which can, in some circumstances, result in

[135] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market (OJ 2006 L 376, p. 36).

[136] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services (OJ 1998 L 204, p. 37).

their exclusion. That intermediation service must thus be regarded as a 'service in the field of transport', within the meaning of Article 2(2)(d) of Directive 2006/123/EC, with the result that it is excluded from the scope of that directive.

Judgment of 10 April 2018 (Grand Chamber), **Uber France** *(C-320/16, EU:C:2018:221)*

The French company Uber France, the operator of a service called UberPop through which it put non-professional drivers using their own vehicle in contact with persons who wished to make urban journeys, by means of a smartphone application, was prosecuted for having organised that service. It argued that the French legislation under which it had been prosecuted was a technical rule concerning an information society service within the meaning of the Directive on technical standards and regulations. [137] That directive requires Member States to communicate to the Commission any draft law or regulation laying down technical rules relating to information society goods and services. In the instant case, the French authorities had not notified the Commission of the criminal legislation at issue prior to its enactment. Proceedings having been brought before it, the tribunal de grande instance de Lille (Regional Court, Lille, France) asked the Court of Justice whether or not the French authorities were required to give prior notice of the draft law to the Commission.

The Court held that Article 1 of Directive 98/34/EC, as amended by Directive 98/48/EC, and Article 2(2)(d) of Directive 2006/123/EC must be interpreted as meaning that a provision of national law that lays down criminal penalties for the organisation of such a system concerns a 'service in the field of transport', in so far as it applies to an intermediation service that is provided by means of a smartphone application and forms an integral part of an overall service the principal element of which is the transport service. Such a service is excluded from the scope of those directives.

The Court recalled its finding in *Asociación Profesional Élite Taxi*, C-434/15 (see above), that the UberPop service fell within the field of transport and did not amount to an information society service within the meaning of Directive 98/34/EC. According to the Court, the UberPop service offered in France is essentially the same as that provided in Spain. It follows that the French authorities were not required to give prior notice of the draft criminal law in issue to the Commission.

Judgment of 19 December 2019 (Grand Chamber), **Airbnb Ireland** *(C-390/18, EU:C:2019:1112)*

By its judgment of 19 December 2019, *Airbnb Ireland* (C-390/18), the Grand Chamber of the Court held, first, that an intermediation service which, by means of an electronic platform, is intended to connect, for remuneration, potential guests with professional or

[137] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services (JO 1998, L 204, p. 37).

non-professional hosts offering short-term accommodation services, while also providing a certain number of services ancillary to that intermediation service, must be classified as an 'information society service' under Directive 2000/31 on electronic commerce. [138] Second, the Court found that, in criminal proceedings with an ancillary civil action, an individual may oppose the application to him or her of measures of a Member State restricting the freedom to provide such a service which that individual provides from another Member State, where those measures were not notified in accordance with the second indent of Article 3(4)(b) of that directive.

The dispute in the main proceedings concerns criminal proceedings brought in France following a complaint, together with an application to be joined as a civil party to the proceedings, lodged against Airbnb Ireland by the Association pour un hébergement et un tourisme professionnels (Association for professional tourism and accommodation). Airbnb Ireland is an Irish company that manages an electronic platform which, in return for payment of a commission, makes it possible to establish contact, particularly in France, between professional hosts and private individuals offering short-term accommodation services and people looking for such accommodation. In addition, Airbnb Ireland offers those hosts ancillary services, such as a format for setting out the content of their offer, civil liability insurance, a tool for estimating their rental price or payment services for the provision of those services.

The association which lodged the complaint against Airbnb Ireland maintained that that company did not merely connect two parties through its platform of the same name; it also acted as an estate agent without holding a professional licence, in breach of the act known as the Hoguet Law, which applies to the activities of real estate professionals in France. For its part, Airbnb Ireland claimed that, on any view, Directive 2000/31 precluded that legislation.

Asked, in the first place, about the classification of the intermediation service provided by Airbnb Ireland, the Court pointed out, referring to the judgment in *Asociación Profesional Elite Taxi*, [139] that if an intermediation service satisfies the conditions laid down in Article 1(1)(b) of Directive 2015/1535, [140] to which Article 2(a) of Directive 2000/31 refers, then, in principle, it is an 'information society service', distinct from the subsequent service to which it relates. However, this will not be the case if it appears that that intermediation service forms an integral part of an overall service whose main component is a service coming under another legal classification.

In the present case, the Court found that an intermediation service such as that provided by Airbnb Ireland satisfied those conditions, and the nature of the links between the intermediation service and the provision of accommodation did not justify

[138] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ('Directive on electronic commerce') (OJ 2000 L 178, p. 1).

[139] Judgment of 20 December 2017, *Asociación Profesional Elite Taxi* (C-434/15, EU:C:2017:981), paragraph 40.

[140] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ 2015 L 241, p. 1)

departing from the classification of that intermediation service as an 'information society service' and thus the application of Directive 2000/31 to that service.

To underline the separate nature of such an intermediation service in relation to the accommodation services to which it relates, the Court noted, first, that that service is not aimed only at providing immediate accommodation services, but rather it consists essentially of providing a tool for presenting and finding accommodation for rent, thereby facilitating the conclusion of future rental agreements. Therefore, that type of service cannot be regarded as being merely ancillary to an overall accommodation service. Second, the Court pointed out that an intermediation service, such as the one provided by Airbnb Ireland, is in no way indispensable to the provision of accommodation services, since the guests and hosts have a number of other channels in that respect, some of which are long-standing. Finally, third, the Court stated that there was nothing in the file to indicate that Airbnb sets or caps the amount of the rents charged by the hosts using that platform.

The Court further stated that the other services offered by Airbnb Ireland do not call that finding into question, since the various services provided are merely ancillary to the intermediation service provided by that company. In addition, it stated that, unlike the intermediation services at issue in the judgments in *Asociación Profesional Elite Taxi* and *Uber France*, [141] neither that intermediation service nor the ancillary services offered by Airbnb Ireland make it possible to establish the existence of a decisive influence exercised by that company over the accommodation services to which its activity relates, with regard both to determining the rental price charged and selecting the hosts or accommodation for rent on its platform.

In the second place, the Court examined whether Airbnb Ireland may, in the main proceedings, oppose the application to that company of a law restricting the freedom to provide information society services provided by an operator from another Member State, such as the Hoguet Law, on the ground that that law was not notified by France in accordance with the second indent of Article 3(4) of Directive 2000/31. The Court stated that the fact that that law predates the entry into force of Directive 2000/31 cannot have had the consequence of freeing the French Republic of its notification obligation. Next, drawing on the reasoning followed in the judgment in *CIA Security International* [142] it found that that obligation, which constitutes a substantial procedural requirement, must be recognised as having direct effect. It therefore concluded that a Member State's failure to fulfil its obligation to give notification of such a measure may be relied on by an individual, not only in criminal proceedings brought against that individual, but also in a claim for damages brought by another individual who has been joined as civil party.

[141] Judgment of 10 April 2018, *Uber France* (C-320/16, EU:C:2018:221).
[142] Judgment of 30 April 1996, *CIA Security International* (C-194/94, EU:C:1996:172).

Judgment of 9 November 2023,* Google Ireland and Others *(C-376/22, EU:C:2023:835)

Google Ireland Limited, Meta Platforms Ireland Limited and Tik Tok Technology Limited are companies established in Ireland which provide, inter alia in Austria, communication platform services.

By its decisions, adopted in 2021, the Kommunikationsbehörde Austria (KommAustria) (the Austrian communications regulatory authority) declared that the three companies referred to above were subject to Austrian law. [143]

Taking the view that that Austrian law, which imposes a set of obligations on providers of communication platform services, whether established in Austria or elsewhere, relating to the monitoring and notification of allegedly unlawful content, should not be applied to them, those companies brought actions against the KommAustria decisions. Those actions were dismissed at first instance.

Following that dismissal, those companies lodged appeals on a point of law before the Verwaltungsgerichtshof (Supreme Administrative Court, Austria). In support of those appeals, they submit in particular that the obligations introduced by the Austrian law are disproportionate and incompatible with the free movement of information society services and with the principle of control of those services by the home Member State, in other words, by the State on whose territory the service provider is established, as laid down in the Directive on electronic commerce. [144]

Having doubts as to the compatibility of the Austrian law and the obligations it imposes on service providers with the Directive on electronic commerce, which allows a Member State other than the home Member State to derogate, under certain conditions, from the principle of free movement of information society services, the Supreme Administrative Court made a reference to the Court of Justice on the interpretation of that directive.

In its judgment, the Court rules on the question whether a Member State of destination of information society services may derogate from the free movement of those services by taking not only individual and specific measures, but also general and abstract measures aimed at a category of given services and, specifically, whether those measures are likely to fall within the concept of 'measures taken against a given information society service' within the meaning of the Directive on electronic commerce. [145]

First of all, the Court notes that the possibility of derogating from the principle of free movement of information society services concerns, according to the wording of the

---

[143] Namely, the Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen (Kommunikationsplattformen-Gesetz) (Federal Law on measures for the protection of users of communications platforms) (BGBl. I, 151/2020).

[144] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ 2000 L 178, p. 1) ('the Directive on electronic commerce').

[145] Article 3(4) of the Directive on electronic commerce.

Directive on electronic commerce, a 'given information society service'. In this context, the use of the word 'given' tends to indicate that the service referred to must be understood as an individualised service. Consequently, Member States cannot adopt general and abstract measures aimed at a category of given information society services described in general terms and applying without distinction to any provider of that category of services.

That assessment is not called into question by the fact that the Directive on electronic commerce uses the concept of 'measures'. By using such a broad and general term, the EU legislature has left to the discretion of the Member States the nature and form of the measures they may adopt to derogate from the principle of free movement of information society services. However, the use of that term in no way prejudges the substance or material content of those measures.

Next, the Court notes that that literal interpretation is corroborated by the contextual analysis of the Directive on electronic commerce.

The possibility of derogating from the principle of free movement of information society services is subject to the condition that the Member State of destination of those services must first ask the Member State of their origin to take measures, [146] which presupposes the possibility of identifying the service providers and, consequently, the Member States concerned. If Member States were authorised to restrict the free movement of such services by means of measures of a general and abstract nature applying without distinction to any provider of a category of such services, such identification would be, if not impossible, at least excessively difficult, so that Member States would not be able to comply with such a condition.

Finally, the Court points out that the Directive on electronic commerce is based on the application of the principles of home Member State control and mutual recognition, so that, within the coordinated field, [147] information society services are regulated solely in the Member State on whose territory the providers of those services are established. However, if Member States of destination were authorised to adopt measures of a general and abstract nature applying without distinction to any provider of a category of such services, whether established in the latter Member State or not, the principle of control in the Member State of origin would be called into question. That principle results in a division of regulatory powers between the Member State of origin and the Member State of destination. To authorise the latter State to adopt such measures would encroach on the regulatory powers of the Member State of origin and would have the effect of subjecting such providers to the legislation of both that State and the Member State or Member States of destination. Calling into question that principle would undermine the system and objectives of the Directive on electronic commerce. Furthermore, to allow the Member State of destination to adopt such measures would

[146] Article 3(4)(b) of the Directive on electronic commerce.
[147] Within the meaning of Article 2(h) of the Directive on electronic commerce.

undermine mutual trust between Member States and would be in conflict with the principle of mutual recognition.

In addition, the Court states that the Directive on electronic commerce seeks to eliminate legal obstacles to the proper functioning of the internal market arising from divergences in legislation and from the legal uncertainty as to which national rules apply to such services. However, the possibility of adopting the abovementioned measures would ultimately amount to subjecting the service providers concerned to different laws and, consequently, reintroducing the legal obstacles to freedom to provide services which that directive seeks to eliminate.

Thus, the Court concludes that general and abstract measures aimed at a category of given information society services described in general terms and applying without distinction to any provider of that category of services do not fall within the concept of 'measures taken against a given information society service' within the meaning of the Directive on electronic commerce.

7. VAT

Judgments of 5 March 2015,* Commission *v* France *(C-479/13, EU:C:2015:141) and* Commission *v* Luxembourg *(C-502/13, EU:C:2015:143)

In France and Luxembourg, the supply of electronic books was subject to a reduced rate of VAT. Thus, since 1 January 2012, France and Luxembourg had respectively applied a VAT rate of 5.5% and 3% to the supply of electronic books.

The electronic (or digital) books at issue in this case covered books in electronic format supplied for consideration by download or streaming from a website to be viewed on a computer, smartphone, electronic book reader or other reading system. The European Commission asked the Court of Justice to declare that, by applying a reduced rate of VAT to the supply of electronic books, France and Luxembourg had failed to fulfil their obligations under the VAT directive. [148]

The Court held that a Member State which applies a reduced rate of VAT to the supply of digital or electronic books fails to fulfil its obligations under Articles 96 and 98 of Directive 2006/112/EC and Regulation (EU) No 282/2011. [149]

It is apparent from the wording of point 6 of Annex III to Directive 2006/112/EC that the reduced VAT rate is applicable to a transaction consisting of the supply of a book on a physical medium. Admittedly, in order to be able to read an electronic book, physical

[148] Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax (OJ 2006 L 347, p. 1).

[149] Council Implementing Regulation (EU) No 282/2011 of 15 March 2011 laying down implementing measures for Directive 2006/112/EC on the common system of value added tax (OJ 2011 L 77, p. 1).

support, such as a computer, is required. However, such support is not included in the supply of electronic books. Furthermore, as is clear from the second subparagraph of Article 98(2) of that directive, the EU legislature decided to exclude any possibility of a reduced rate of VAT being applied to electronically supplied services. The supply of electronic books constitutes such a service, since it cannot be regarded as a supply of goods within the meaning of Article 14(1) of that directive because an electronic book cannot qualify as tangible property. Similarly, the supply of electronic books meets the definition of electronically supplied services set out in Article 7(1) of Regulation (EU) No 282/2011.

That interpretation is not undermined by the principle of fiscal neutrality, since that principle cannot extend the scope of reduced rates of VAT in the absence of clear wording to that effect.

Judgment of 7 March 2017 (Grand Chamber),* RPO *(C-390/15, EU:C:2017:174)

Under the VAT directive, [150] Member States were able to apply a reduced rate of VAT to print publications such as books, newspapers and periodicals. By contrast, digital publications had to be subject to the standard rate of VAT, except digital books supplied on a physical support (for instance, CD-ROM). Proceedings having been brought before it by the Polish Commissioner for Civic Rights, the Trybunał Konstytucyjny (Constitutional Court, Poland) expressed doubts about the validity of that difference in tax treatment. It asked the Court of Justice whether that difference was compatible with the principle of equal treatment and whether the European Parliament had been sufficiently involved in the legislative procedure.

According to the Court, the obligation to consult the Parliament during the legislative procedure in the cases laid down by the Treaty means that the Parliament is consulted afresh whenever the text finally adopted, taken as a whole, differs in essence from the text on which the Parliament has already been consulted, except in cases where the amendments substantially correspond to a wish of the Parliament itself.

The text of point 6 of Annex III to Directive 2006/112/EC as amended is nothing other than a simplification of the drafting of the text which was set out in the proposal for a directive and the substance of which has been fully preserved.

In addition, the examination of the questions referred for a preliminary ruling disclosed no factor of such a kind as to affect the validity of point 6 of Annex III to Directive 2006/112/EC or of Article 98(2) of that directive, read in conjunction with point 6 of Annex III thereto.

[150] Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax (OJ 2006 L 347, p. 1), as amended by Council Directive 2009/47/EC of 5 May 2009 amending Directive 2006/112/EC as regards reduced rates of value added tax (OJ 2009 L 116, p. 18).

The supply of digital books on all physical means of support and the supply of digital books electronically amount to comparable situations. Those provisions must be regarded as establishing a difference in treatment between two situations that are, however, comparable in the light of the objective pursued by the EU legislature. Where such a difference is found, the principle of equal treatment is not infringed in so far as that difference is duly justified. That is the case where the difference in treatment relates to a legally permitted objective pursued by the measure having the effect of giving rise to such a difference and is proportionate to that objective.

In that respect, it is understood that, when the EU legislature adopts a tax measure, it is called upon to make political, economic and social choices, and to rank divergent interests or to undertake complex assessments. Consequently, it should, in that context, be accorded a broad discretion, so that judicial review must be limited to review as to manifest error. Indeed, it is apparent from the explanations provided by the Council and the Commission that it was considered necessary to make electronically supplied services subject to clear, simple and uniform rules in order that the VAT rate applicable to those services may be established with certainty and, thus, that the administration of VAT by taxable persons and national tax authorities is facilitated. The possibility of applying a reduced rate of VAT to the supply of digital books electronically would effectively compromise the overall coherence of the measure intended by the EU legislature.

COURT OF JUSTICE
OF THE EUROPEAN UNION

Research and Documentation Directorate

July 2024