FRICoRe

Judicial Training Project

Fundamental Rights In Courts and Regulation

CASEBOOK

EFFECTIVE CONSUMER PROTECTION AND FUNDAMENTAL RIGHTS

SSM

Scuola Superiore della Magistratura

University of Trento

THIS PUBLICATION IS FUNDED BY THE EUROPEAN UNION'S JUSTICE PROGRAMME (2014-2020)

Effective Consumer Protection and Fundamental Rights

Edited by Paola Iamiceli, Fabrizio Cafaggi and Mireia Artigot i Golobardes

Publisher: Scuola Superiore della Magistratura, Rome – 2022

ISBN 9791280600240

Published in the framework of the project:

Fundamental Rights In Courts and Regulation (FRICoRe)

Coordinating Partner:

University of Trento (*Italy*)

Partners:

Scuola Superiore della Magistratura (*Italy*)

Institute of Law Studies of the Polish Academy of Sciences (INP-PAN) (*Poland*)

University of Versailles Saint Quentin-en-Yvelines (*France*)

University of Gröningen (*The Netherlands*)

Pompeu Fabra University (*Spain*)

University of Coimbra (*Portugal*)

Fondazione Bruno Kessler (*Italy*)

The present Casebook builds upon the *RE-Jus Casebook. Effective Justice in Consumer protection.* Particularly, chapters 1 through 7 are based on RE-Jus training materials, subject to revision, integration, and updating.

Edition: May 2022

Scientific Coordinator of the FRICoRe Project:

Paola Iamiceli

Coordinator of the team of legal experts on Effective Consumer Protection:

Paola Iamiceli; Fabrizio Cafaggi

Project Manager:

Chiara Patera

Co-editors and co-authors of this Casebook:

Co-editors: Paola Iamiceli (Project Coordinator), Fabrizio Cafaggi and Mireia Artigot i Golobardes
Introduction: Fabrizio Cafaggi and Paola Iamiceli
Appendix: The Status of consumer: Chiara Angiolini
Ch. 1: Chiara Angiolini, Paola Iamiceli and Charlotte Pavillon
Ch. 2: Kati Cseres and Gianmatteo Sabatino
Ch. 3: Mateusz Grochowski, Chiara Patera and Federico Pistelli
Ch. 4: Chiara Angiolini, Sébastien Fassiaux and Cèlia Roig
Ch. 5: Chiara Angiolini, Charlotte Pavillon and Paola Iamiceli
Ch. 6: Chiara Angiolini and Paola Iamiceli
Ch. 7: Sandrine Clavel and Fabienne Jault-Seseke
Ch. 8: Mireia Artigot, Fernando Gómez and Sébastien Fassiaux
Ch. 9: Chiara Angiolini and Sébastien Fassiaux
Ch. 10: Tomàs Garcia-Micó, Carlos Gómez, Rosa Milà and Sonia Ramos

Note on national experts and collaborators:

The FRICoRe team would like to thank: Cèlia Roig and Federico Pistelli for their support in chapters' editing, and all the judges, experts and collaborators who contributed to the project and to the Casebook by suggesting instances of national and European case law, and particularly the following members of the *European Network of Judges and Legal Experts* who supported the FRICoRe project (in alphabetical order):

José Mª Blanco Saralegui
Aurelia Colombi Ciacchi
Silvia Ciacchi
Marta Fernandez De Frutos
Maud Lagelée Heymann
Federica De Gottardo
Ksenija Dimec
Rossana Ducato
Giuseppe Fiengo
Stéphanie Gargoullaud
Ilaria Gentile
Petri Helander
Thomas Horvath
Mareike Hoffmann
Pamela Ilieva
Monika Jozon
Meeli Kaur
Sil Van Kordelaan
Madalina Moraru
Viola Nobili
Michal Notovny
Sandra Passinhas
Charlotte Pavillon
Tobias Nowak
Valentina Rustja
José Mª Fernández Seijo
Markus Thoma

Table of contents

9. Effective consumer and data protection: the intersections

9.1. Collective redress in data protection. The (possible) role of consumer protection associations

Relevant CJEU cases

- Judgement of the Court (Second Chamber) of 29 July 2019, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, Case C-40/17 ("**Fashion ID**")
- Judgement of the Court (Third Chamber) of 25 January 2018, *Maximilian Schrems v Facebook Ireland Limited*, Case C-498/16 ("**Schrems**")
- Judgement of the Court (Third Chamber) of 28 April 2022, *Meta Platforms Ireland Limited contre Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V.,* Case C-319/20 ("**Meta**")

Main questions addressed

Question 1 In light of the principle of effectiveness and of Article 47 of the Charter of Fundamental Rights, can a consumer protection association seek an action in the event of violations of data protection law?

Question 2 What is the impact of Article 80 GDPR on the role of associations in data protection collective redress? How should Article 80 GDPR be interpreted in light of Article 47 of the Charter of Fundamental Rights and of the principles of proportionality, effectiveness and dissuasiveness?

9.1.1. Question 1 – consumer protection associations and data protection law violations

In light of the principle of effectiveness and of Article 47 of the Charter of Fundamental Rights, can a consumer protection association seek an action in the event of violations of data protection law?

The analysis is mainly based on the *Fashion ID* case (C-40/17).

Judgement of the Court (Third Chamber) of 25 January 2018, *Maximilian Schrems v Facebook Ireland Limited*, Case C-498/16 ("Schrems")

The case

Fashion ID, an online clothing retailer, embedded on its website the 'Like' social plugin from the social network Facebook ('the Facebook "Like" button'). When a visitor consulted the website of Fashion ID, his/her personal data were transmitted to Facebook Ireland as a result of that website including that button. It seems that the transmission occurred without the visitor being aware of it regardless of whether or not he or she was a member of the Facebook social network or had clicked on the Facebook 'Like' button.

Verbraucherzentrale NRW, a public-service association tasked with safeguarding the interests of consumers, criticised Fashion ID for transmitting to Facebook Ireland personal data belonging to visitors to its website, first, without their consent and, second, in breach of the duties to inform set out in the provisions relating to the protection of personal data. *Verbraucherzentrale NRW* brought before the *Landgericht Düsseldorf* (Regional Court, Düsseldorf, Germany) legal proceedings for an injunction against Fashion ID to force it to stop that practice.

By decision of 9 March 2016, the *Landgericht Düsseldorf* (Regional Court, Düsseldorf) upheld in part the requests made by *Verbraucherzentrale NRW*, after having found that it had standing to bring proceedings under Paragraph 8(3)(3) of the UWG.

Fashion ID brought an appeal against that decision before the referring court, the *Oberlandesgericht Düsseldorf* (Higher Regional Court, Düsseldorf, Germany). The referring court put the following question to the CJEU because it had doubts as to whether Directive 95/46 gave public-service associations the right to bring or defend legal proceedings in order to defend the interests of persons who have suffered harm.

Preliminary questions referred to the CJEU

> (1) Do the rules in Articles 22, 23 and 24 of Directive [95/46] preclude national legislation which, in addition to the powers of intervention conferred on the data-protection authorities and the remedies available to the data subject, grant public-service associations the power to take action against the infringer in the event of an infringement in order to safeguard the interests of consumers?

With its first question the referring court asked, in essence, whether Articles 22 to 24 of Directive 95/46 must be interpreted as precluding national legislation which allows consumer-protection associations to bring or defend legal proceedings against a person allegedly responsible for an infringement of the laws protecting personal data.

Reasoning of the CJEU

As a preliminary point, the Court noted that, under Article 22 of Directive 95/46, Member States are required to provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him/her by the national law applicable to the processing in question.

Article 28(3) of Directive 95/46 provides that the supervisory authority responsible for monitoring the application of the transposing measures within each Member State has the power to engage in legal proceedings when the national provisions adopted pursuant to that Directive have been violated or to bring those violations to the attention of the judicial authorities.

However, no provision of that Directive obliges Member States to provide, or expressly empowers them to provide, in their national law that an association can represent a data subject in legal proceedings or commence legal proceedings on its own initiative against the person allegedly responsible for an infringement of the laws protecting personal data.

Nevertheless, nothing in Directive 95/46 precludes national legislation allowing consumer-protection associations to bring or defend legal proceedings against the person allegedly responsible for such an infringement.

The Court then recalled that Member States are required, when transposing a directive, to ensure that it is fully effective in accordance with the objective which it seeks to attain, but they retain broad discretion as to the choice of ways and means of ensuring that it is implemented. In this regard, one of the underlying objectives of Directive 95/46 is to ensure effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data.

The fact that a Member State provides in its national legislation that it is possible for a consumer protection association to commence legal proceedings against a person who is allegedly responsible for an infringement of the laws protecting personal data in no way undermines the objectives of that protection and, in fact, contributes to the realisation of those objectives.

Since Directive 95/46 lays down rules that are relatively general and have a degree of flexibility, Member States have a margin of discretion in implementing that Directive. Although Article 22 of that Directive requires Member States to provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him/her by the national law applicable to the personal data processing in question, that Directive does not, however, contain any provisions specifically governing the conditions under which that remedy may be exercised. In addition, Article 24 of the Directive provides that Member States are to adopt 'suitable measures' to ensure the full implementation of its provisions, without defining such measures.

The Court then explained that a provision making it possible for a consumer-protection association to commence legal proceedings against a person who is allegedly responsible for an infringement of the laws protecting personal data may constitute a suitable measure, within the meaning of that provision, that contributes to the realisation of the objectives of that Directive.

Finally, the fact that Regulation 2016/679 (the General Data Protection Regulation, hereinafter the ***GDPR***), which repealed and replaced Directive 95/46 and has been applicable since 25 May 2018, expressly authorises, in Article 80(2) thereof, Member States to allow consumer-protection associations to bring or defend legal proceedings against a person who is allegedly responsible for an infringement of the laws protecting personal data, does not mean that Member States could not grant them that right under Directive 95/46, but confirms, rather, that the interpretation of that Directive in the present judgement reflects the will of the EU legislature.

Conclusion of the CJEU

> Articles 22 to 24 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 must be interpreted as not precluding national legislation which allows consumer-protection associations to bring or defend legal proceedings against a person allegedly responsible for an infringement of the protection of personal data.

Impact on the follow-up case

The referring court (*Oberlandesgericht Düsseldorf*) still has to deliver its decision.

Elements of judicial dialogue

The *Schrems* case[47] is also relevant to answering the question of whether a consumer protection association can seek an action in case of violations of data protection law.

In that case, the plaintiff (Mr Schrems) had founded an association which sought to uphold the fundamental right to data protection. However, he brought the action against Facebook on the basis of his own rights and similar rights of seven other contractual partners of the defendant, who were also consumers in Austria, Germany and India. Austrian law indeed allows for one applicant to bring different claims against the same defendant and for these claims be heard jointly in the same proceedings. The plaintiff claimed that the defendant had committed numerous infringements of data protection provisions. After his actions were dismissed by the lower courts, Mr Schrems brought an appeal before the *Oberster Gerichtshof* (Supreme Court, Austria), which referred a question to the CJEU.

In its question, the referring court asked, in essence, whether Article 16(1) of Regulation No 44/2001 (related to jurisdiction over consumer contracts) must be interpreted as meaning that it does not apply to the proceedings brought by a consumer for the purpose of asserting, in the courts of the country in which s/he is domiciled, not only his/her own claims, but also claims assigned by other consumers domiciled in the same Member State, in other Member States, or in non-member countries. In other words, as AG Bobek put it in his opinion of the case, can Article 16(1) of Regulation no. 44/2001 establish an additional special jurisdiction in the country of the assignee's domicile, thus effectively opening up the possibility of collecting consumer claims from around the world?

The Court did not depart from its settled case law and held that 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 other than those expressly referred to by Regulation no. 44/2001 cannot be established through the concentration of several claims in the person of a single applicant.[48]

By holding that the special rules of jurisdiction over consumer contracts do not allow consumers to seek redress jointly for their own claims and for claims assigned to them by consumers domiciled in the same Member State, in other Member States or in non-member countries, the CJEU interpreted Article 16(1) of Regulation 44/2001 strictly. Although the claim in these proceedings related to violations of data protection laws, the Court's conclusion applies to any claims related to consumer contracts.

While in *Schrems* the CJEU denied collective redress through the assignment of rights by consumers, it held in *Fashion ID* that Member States could allow consumer-protection associations to seek redress for violation of data protection laws. Consequently, if Austria had allowed such claims by consumer-protection associations, and if Mr Schrems had filed suit with his association, it is likely that he would have had standing to bring those third-party claims as

[47] Judgement of the Court (Third Chamber) of 25 January 2018, *Maximilian Schrems v Facebook Ireland Limited*, Case C-498/16.

[48] On 28 February 2018, the Austrian Supreme Court upheld the Higher Regional Court's decision dismissing the appeal. Given the CJEU's preliminary ruling, the Austrian Supreme Court explained that the plaintiff could only rely on his personal claim and not on the other claims assigned to him. The Austrian Court did not depart from the CJEU's ruling and dealt with the issue rapidly.

well. In any event, it is worth noting that the CJEU does not generally exclude the possibility of collective redress for violations of data protection provisions. However, the issue in *Schrems* was rather specific, because it concerned the assignment of rights by consumers to a single plaintiff (a possibility under Austrian law). Therefore, the CJEU did not hold that consumers victims of violations of data protection law cannot obtain collective redress, but rather that multiple plaintiffs cannot circumvent the European rules on international jurisdiction by concentrating their claims in the person of a single applicant.

In the meantime, the GDPR entered into force and now provides in its Article 80 that data subjects have the right to mandate a not-for-profit body, organisation or association to lodge complaints and to exercise the right to receive compensation, where provided for by Member State law (see below). As explained below, the major drawback of Article 80 is that Member States are free to implement it or not, which leaves consumer-protection associations upholding the fundamental right to data protection with unharmonized collective redress mechanisms in the EU.

9.1.2. Question 2 - Representation of data subjects under Article 80 of Regulation 2016/679 (General Data Protection Regulation)[49]

What is the impact of Article 80 GDPR on the role of associations in data protection collective redress? How should Article 80 GDPR be interpreted in light of Article 47 of the Charter of Fundamental Rights and of the principles of proportionality, effectiveness and dissuasiveness? Does the new legal framework leave any space for consumer protection associations in the field of data protection?

Article 80 GDPR

In the field of data protection, the GDPR repealed Directive 95/46/EC (the Data Protection Directive) and introduced a new collective redress mechanism. Its Article 80, titled 'Representation of data subjects', reads as follows:

> *"1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.*
>
> *2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a*

[49] 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 L 119/1, 4.5.2016.

complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing."

This regulation introduced two new innovations for collective redress in the field of data protection.

First, it introduced the possibility for representative bodies to *claim compensation on behalf of data subjects*. In this case, the data subject's rights of compensation are transferred to the representative body. This possibility is akin to an opt-in collective redress, in which data subjects voluntarily express their wish to claim compensation through the representative. The regulation only requires that the representative be a not-for-profit body, organisation or association, that its statutory objectives be in the public interest, and that it be active in the field of the protection of data subjects' rights and freedoms. This requirement notably excludes law firms and other for-profit litigators.

Second, this article introduced the possibility for representative bodies, *independently of a data subject's mandate*, to lodge complaints with supervisory authorities, but also to exercise the data subject's rights to an effective judicial remedy against supervisory authorities, controllers, and data processors. In this case, representative bodies cannot claim compensation.

The Meta case, C-319/2020, of 2 December 2021

With regard to the application of Article 80 GDPR for protecting (also) economic interests, the CJEU decision on case C-319/20, *Facebook Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände* is of particular interest.

In its **preliminary reference**, the **German Federal Court of Justice** asked the CJEU whether the rules in Chapter VIII of the GDPR, in particular in its Article 80 concerning collective redress, and Article 84 concerning sanctions preclude national rules which – alongside the powers of intervention of the supervisory authorities responsible for monitoring and enforcing the Regulation and the options for legal redress for data subjects – empower, on the one hand, competitors and, on the other, associations, entities and chambers entitled under national law, to bring proceedings for breaches of Regulation (EU) 2016/679, independently of the infringement of specific rights of individual data subjects and without being mandated to do so by a data subject, against the infringer before the civil courts on the basis of the prohibition of unfair commercial practices or breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions.

The CJEU, **in its Decision of 28 April 2022 (*Meta*, C-319/20)**, stated that Article 80(2) GDPR does not preclude national legislation which allows consumer protection associations to bring legal proceedings against the person alleged to be responsible for an infringement of the protection of personal data, on the basis of the prohibition of unfair commercial practices, the infringement of a law relating to consumer protection or the prohibition of the use of invalid general terms and conditions, provided that the objective of the representative action in question is to ensure observance of the rights which the persons affected by the contested processing

derive directly from that Regulation. The CJEU recalled the principle of **dissuasiveness,** affirming that its interpretation of Article 80 was coherent with the deterrent nature and dissuasive purpose of actions for injunctions.

The implementation of Article 80 GDPR in Member States

The major weakness of Article 80 is that it does not oblige Member States to act. Member States are free to choose whether to implement such collective redress mechanisms in their national legislation. The Commission's initial proposal included an obligation for Member States to provide for such a mechanism, but the Council amended the text to remove that obligation, despite the fact that the Parliament had approved it. The fact that Member States seem reluctant to implement collective redress mechanisms in general is reflected in their national legislations, since, as explained below, only six of them have adopted a functioning and efficient collective redress system (Belgium, France, Italy, Portugal, Spain and Sweden).[50]

Consumers soon took advantage of this new possibility at national level. In **France,** the UFC-Que Choisir consumer group brought a collective claim on 26 June 2019 before the *Tribunal de grande instance de Paris* (Tribunal of First Instance of Paris) to obtain an injunction against and claim compensation from Google for violation of the GDPR. The association wanted to obtain an injunction against Google to stop the illegal use by its Android system of the users' personal data and to mandate obtaining their express consent before collecting and treating their data. The association claimed a compensation of €1000 for any user of Google's Android system who had a Google account. Consumers who believe their rights have been violated will be able to join the case once the first-instance judge has decided on Google's liability.

In conclusion, the solution adopted by the Court in the *Fashion ID* case is important also in view of interpreting Article 80 GDPR, which introduced new possibilities for associations to claim effective judicial remedies and compensation on behalf of consumers whose personal data have been mishandled. However, the implementation of Article 80 depends on each Member State, and jurisdictional issues could still prevent consumer-protection associations from successfully representing data subjects in collective actions, as illustrated by *Schrems*.

9.1.3. The role of consumer associations in the field of data protection in light of the new Directive EU, 2020/1828, on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, adopted on 25 November 2020

On 11 April 2018, the European Commission published a legislative proposal for the adoption of a new Directive on representative actions for the protection of the collective interests of

[50] BEUC, *Why we need collective redress at EU level: a compelling collection of cases*, October 2019, accessible at: https://www.beuc.eu/publications/beuc-x-2019-062_why_we_need_collective_redress_at_eu_level.pdf.

consumers.[51] The new Directive EU 2020/1828, on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC was adopted on 25 November 2020.
With regard to the role of consumer-protection associations in the field of data protection, Article 2 of the Directive stated that:
"This Directive applies to representative actions brought against infringements by traders of the provisions of Union law referred to in Annex I, including such provisions as transposed into national law, that harm or may harm the collective interests of consumers".

The Regulation UE 2016/679 and some articles of Directive 2002/58 were included in Annex I. According to its recital 14, the Directive should cover infringements of the provisions of Union law referred to in Annex I *to the extent that those provisions protect the interests of consumers*, regardless of whether those consumers are referred to as consumers, travellers, users, customers, retail investors, retail clients, **data subjects**, or otherwise. "**However, this Directive should only protect the interests of natural persons who have been harmed or may be harmed by those infringements if those persons are consumers under this Directive. Infringements that harm natural persons qualifying as traders under this Directive should not be covered by it**" (see also recital 16).
Furthermore, according to recital 15, the Directive should be without prejudice to the legal acts listed in Annex I. Hence it should not change or extend the definitions laid down in those legal acts or replace any enforcement mechanism that those legal acts might contain. Furthermore, recital 15 of the Directive expressly states that "the enforcement mechanisms provided for in or based on Regulation (EU) 2016/679 (…) could, where applicable, still be used for the protection of the collective interests of consumers".
To a certain extent, the Directive encourages the role of consumer-protection associations in data-protection cases. The coordination between collective redress in consumer and data protection cases has been an important issue for Member States in the implementation of the new Directive, also in light of Article 47, Article 8 CFR and of the principle of effectiveness. In this respect, the following question arises:

If the data subject is also a consumer, can Article 47 CFR lead to a concurrence of remedies that combines data protection and consumer law remedies?

Furthermore, comparison between the legislation on collective actions in consumer law and in data protection law shows that, within the latter, the collective redress system is less developed. To be noted in this regard is that the relationships between, on the one hand, the data subject and the data controller, and on the other hand, the consumer and the professional, are both characterized by an imbalance of power, although – at least partially – they are different in nature.

[51] Proposal for a Directive of the European Parliament and of the Council on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC, COM/2018/0184 final - 2018/089 (COD). The Commission's proposal was published on 11 April 2018.

The weaker position of the consumer vis-à-vis the seller or supplier concerns the consumer's level of knowledge and his/her bargaining power (e.g. *Costea,* 3 September 2015, C-110/14; *Siba,* C-537/13, 15 January 2015; *Pouvin*, C-590/17, 21 March 2019; *Vapenik,* C-508/12, 5 December 2013). The data subject's weaker position is due at least to the knowledge concerning the data subject that the data controller acquires in processing data, and to the fact that the ways and timing of that processing are put in place by the controller, with the consequence of an information asymmetry concerning the processing operations.

9.2. Lack of conformity of digital content or services and GDPR compliance

In light of the principles of effectiveness and dissuasiveness, and of Article 47 of the Charter of Fundamental Rights, could the consumer remedies against a lack of conformity of a digital content/service provided by Directive 2019/770 be used against a violation of data protection law?

New Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services

Directive 2019/770 (the ***Digital Content Directive***) was published in May 2019.[52] As part of the EU's Digital Single Market strategy, this Directive fully harmonised certain key contractual rules for the supply of digital content or services. Member States had until 1 July 2021 to adopt and publish the measures necessary to comply with this Directive. They should have applied those measures from 1 January 2022 onwards.

Among the measures that Member States had to transpose were remedies for lack of conformity of the digital content or service offered by a trader. In that case, Article 14 of the Directive provided three options for the consumer: (i) have the digital content or service brought into conformity; (ii) receive a proportionate reduction in price; or (iii) terminate the contract, in accordance with the conditions established by the Directive.[53] In regard to compensation, Article 3(10) of the Directive provided that Member States are free to regulate the right to damages in the case of violations of their national legislation transposing the Directive. However, it is beyond the scope of this note to detail these remedies extensively. Instead, the question at hand is whether these remedies for lack of conformity of a digital content or service can be used for violations of data protection law.

The scope of the Directive is rather broad, because it applies to any contract where the trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer pays or undertakes to pay a price.[54] Furthermore, Article 3(1) of the Directive provides that it applies *"where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader"*.

[52] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, *O.J.E.U.*, 22.5.2019, L 136/1.
[53] Article 14 of Directive (EU) 2019/770.
[54] Article 3(1) of Directive (EU) 2019/770.

The Directive also provides that Union law on the protection of personal data, especially the General Data Protection Regulation (the ***GDPR***), shall apply to any personal data processed in connection with such contracts.[55] In the case of conflict between Directive 2019/770 and data protection law, the latter prevails.[56] In the same vein, Recital 48 of the Directive explicitly mentions that the lack of compliance with the GDPR may constitute a lack of conformity in the sense of the Digital Content Directive:

> *"Facts leading to a lack of compliance with requirements provided for by Regulation (EU) 2016/679, including core principles such as the requirements for data minimisation, data protection by design and data protection by default, may, depending on the circumstances of the case, also be considered to constitute a lack of conformity of the digital content or digital service with subjective or objective requirements for conformity provided for in this Directive. One example could be where a trader explicitly assumes an obligation in the contract, or the contract can be interpreted in that way, which is also linked to the trader's obligations under Regulation (EU) 2016/679. In that case, such a contractual commitment can become part of the subjective requirements for conformity. A second example could be where non-compliance with the obligations under Regulation (EU) 2016/679 could, at the same time render the digital content or digital service unfit for its intended purpose and, therefore, constitute a lack of conformity with the objective requirement for conformity which requires the digital content or digital service to be fit for the purposes for which digital content or digital services of the same type would be normally used".*

Therefore, consumers whose personal data have been mishandled by a trader in the context of such a contract would be able to seek remedies available under the Digital Content Directive if that mishandling of personal data also constitutes a lack of conformity and all conditions laid down in the Directive are fulfilled. Recital 48 of the directive confirms this finding:

> *"Where the facts leading to non-compliance with requirements under Regulation (EU) 2016/679 also constitute a lack of conformity of the digital content or digital service with subjective or objective requirements for conformity as provided for in this Directive, the consumer should be entitled to the remedies for the lack of conformity provided for by this Directive, unless the contract is already void or voidable under national law".*

In this respect, the **principle of effectiveness, Article 47 and Article 8 CFR**, should be taken into account by Member States in the implementation of Directive 2019/770 and by courts in its interpretation. In particular, it raises the question of whether compliance with data protection law by the service and digital content is to be qualified as an objective requirement for conformity, regulated by Article 8 of that directive.

Another **issue is the relationship between the information provided to the data subject in accordance with Regulation 2016/679 and Article 7 of Directive 2019/770, which regulates the subjective requirements for the conformity of digital content or service.**

[55] Article 3(8) of Directive (EU) 2019/770.

[56] Article 3(8) of Directive (EU) 2019/770.

Moreover, this possibility is not reserved only for consumers who paid a price for the supply of a digital content or service. In fact, one of the main innovations of this Directive is that it acknowledges that consumers are often offered digital content and services for free, which is made possible by the processing of personal data concerning the data subject-consumer by the trader. In this regard, Recital 24 of the Directive states the following:

> "*Such business models are used in different forms in a considerable part of the market. While fully recognising that the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity, this Directive should ensure that consumers are, in the context of such business models, entitled to contractual remedies. This Directive should, therefore, apply to contracts where the trader supplies, or undertakes to supply, digital content or a digital service to the consumer, and the consumer provides, or undertakes to provide, personal data. The personal data could be provided to the trader either at the time when the contract is concluded or at a later time, such as when the consumer gives consent for the trader to use any personal data that the consumer might upload or create with the use of the digital content or digital service. Union law on the protection of personal data provides for an exhaustive list of legal grounds for the lawful processing of personal data. This Directive should apply to any contract where the consumer provides or undertakes to provide personal data to the trader. For example, this Directive should apply where the consumer opens a social media account and provides a name and email address that are used for purposes other than solely supplying the digital content or digital service, or other than complying with legal requirements. It should equally apply where the consumer gives consent for any material that constitutes personal data, such as photographs or posts that the consumer uploads, to be processed by the trader for marketing purposes. Member States should however remain free to determine whether the requirements for the formation, existence and validity of a contract under national law are fulfilled".*

The recognition of the ubiquity of this type of business model (where consumers basically pay for digital content and services with their personal data) materialised in Article 3(1) of the Directive. In this case, consumers are entitled to have the digital content or digital service brought into conformity or to terminate the contract. Whereas consumers who pay a price for digital content or services are only entitled to terminate the contract when the lack of conformity is not minor, consumers who are supplied digital content or services and who provide their personal data are entitled to terminate the contract even if the lack of conformity is minor. Conversely, they obviously cannot claim a proportionate reduction of the price.

Consumers are not the only ones who can seek remedies for lack of conformity. In order to guarantee effective enforcement of the Directive's provisions, Member States should include in their legislation the possibility for either public bodies, consumer organisations, professional organisations or not-for-profit bodies active in the field of data protection to take action under national law before courts or administrative bodies.[57] Member States are free to choose which of these types of organisations (one or more) will be able to take action.

[57] Article 21(2) of Directive (EU) 2019/770.

9.3. Unfair commercial practices and information provided to the data subject

Main questions addressed

Question 1 **a.** Shall, in light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the Charter of Fundamental Rights, the Unfair Commercial Practices Directive (2005/29) be applied in the case of a **violation of the duty of information on data processing** provided by Articles 13 and 14 of the General Data Protection Regulation (2016/679)? Could, in light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the Charter of Fundamental Rights, the Unfair Commercial Practices Directive (2005/29) be **used to interpret extensively the duty of information provided in the General Data Protection Regulation** (2016/679)?

b. What authority **is competent**? How should authorities coordinate with each other in light of the principles of effectiveness, good administration and duty of cooperation?

Relevant national cases in the cluster:

- Italian Consumer Protection Authority (Autorità Garante per la Concorrenza e il Mercato – AGCM), decision no. 26597, 11 May 2017, *Whatsapp-Trasferimento dati a Facebook*
    - Italian Consumer Protection Authority (Autorità Garante per la Concorrenza e il Mercato – AGCM), decision no. 27432, 29 November 2018, *Facebook- condivisione dati con terzi*
- Administrative court (T.A.R.) of Rome, 10 January 2020, no. 260 (judicial review of Italian consumer protection Authority, decision no. 27432, 29 November 2018)
- Administrative court (T.A.R.) of Rome, 10 January 2020, no. 261 (judicial review of Italian consumer protection Authority, decision no. 27432, 29 November 2018)
- Council of State, decisions nos. 2631 and 2630 of 29 March 2021

9.3.1. Introduction: coordination and existence of parallel systems and authorities regulating the digital economy

Although unfair commercial practices linked to infringements of data protection laws are not limited to the digital economy, the best examples of such practices occur online. The most significant cases, in fact, involve online platforms, online traders and connected objects. Digital markets are characterized by a lack of informed consent by data subjects, leading to a lack of transparency in how their data are collected and processed. These characteristics give rise to situations where a single conduct can potentially constitute infringements of data protection, consumer and/or competition law.

Another issue is determining what regulator is competent to investigate and sanction infringements of data protection law that also constitute infringements of consumer law and

potentially restrict competition on the market. In February 2019, the German Competition Authority (*Bundeskartellamt*) issued a decision against Facebook for abusing its dominant position on the German market for social networks, based on the practice of collecting, using and merging data in user accounts. Similarly, the Italian Competition Authority (*Autorità Garante della Concorrenza e del Mercato*), also in charge of consumer protection, fined WhatsApp in May 2017 for violating consumer law because it shared its users' personal data with Facebook and forced its users to accept its new terms and conditions.

Both cases are discussed below because they involve practices prohibited by a mix of consumer, data protection and/or competition law. They illustrate the existence of parallel systems and authorities regulating the digital economy. Each system has its own legal bases, goals, procedures and remedies. But can those systems overlap, and if so, to what extent? This section will focus on the interplay between the General Data Protection Regulation (the ***GDPR***) and Directive 2005/49 (the ***Unfair Commercial Practices Directive***). In particular, it aims to answer the question of whether violations of information duties provided by the GDPR can also constitute unfair commercial practices under the Unfair Commercial Practices Directive, and whether this Directive could be used to interpret extensively the duty of information provided by the GDPR. This section also tries to determine which authorities are competent, and how they should be coordinated.

9.3.2. Question 1 a – Unfair commercial practices and information provided to the data subject

Shall, in light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the Charter of Fundamental Rights, the Unfair Commercial Practices Directive (2005/29) be applied in the case of a **violation of the duty of information on data processing** provided by Articles 13 and 14 of the General Data Protection Regulation (2016/679)?
Could, in light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the Charter of Fundamental Rights, the Unfair Commercial Practices Directive (2005/29) be **used to interpret extensively the duty of information provided in the General Data Protection Regulation** (2016/679)?

EU law perspective

The European Commission ***Guid*ance on the Implementation/Application of the Unfair Commercial Practices Directive**[58] provides that:

- A trader's violation of Data Protection rules will not, in itself, always mean that the practice is also in breach of Directive 2005/29, but such **data protection violations should be considered when assessing the overall unfairness of commercial practices**, particularly in the situation where the trader processes consumer data in violation of data protection requirements, (*i.e.* for direct marketing purposes or any other commercial purposes like profiling, personal pricing or big data applications).

[58] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016SC0163&from=IT

- Personal data, consumer preferences and other user generated content, have a "de facto" economic value and are being sold to third parties. Depending on the circumstances, this could also be considered a violation of the EU data protection requirements to provide the required information to the individual concerned as to the purposes of the processing of the personal data.

Furthermore, the European Commission affirmed in the Guidance that:

"According to its Article 51(1), the EU Charter of fundamental rights applies to the Member States when they implement Union law, thus also when they implement the provisions of the UCPD. The Charter contains provisions, among others, on the **protection of personal data (Article 8)**, the rights of the child (Article 24), consumer protection (Article 38) and the **right to an effective remedy and a fair trial (Article 47)**. The Court has stressed the significance of Article 47 of the Charter on access to justice in relation to remedies available to consumers in connection with consumer rights granted under EU directives. **The principle of effectiveness**, as referred to by the Court, means that national rules of procedure may not make it excessively difficult or impossible in practice for consumers to exercise rights conferred by EU law."

The statement on the economic value of certain uses of personal data, such as those for commercial purposes should be coordinated with the impossibility of their qualification as "mere commodities". In this respect, recital (24) of Directive 2019/770 states:

"Digital content or digital services are often supplied also where the consumer does not pay a price but provides personal data to the trader. (…) While fully recognising that the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity, this Directive should ensure that consumers are, in the context of such business models, entitled to contractual remedies".

According to the EDPB' s Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, personal data cannot be regarded as commodities. In this Opinion, the EDPB states:

"The EDPS warns against any new provision introducing the idea that people can pay with their data the same way as they do with money. Fundamental rights such as the right to the protection of personal data cannot be reduced to simple consumer interests, and personal data cannot be considered as a mere commodity".

National case law

Italy

In two decisions, the Italian Consumer Protection Authority (*Autorità Garante per la Concorrenza ed il Mercato,* hereinafter: ***AGCM***) has considered the conduct of professionals concerning information about the data subject in light of Directive 2005/29 on unfair commercial practices.

In both **decisions** (no. 27432, 29 November 2018, and no. 26597, 11 May 2017), the AGCM affirmed that **the unfair commercial practices discipline is to be applied** where **personal data** concerning Facebook's users acquire economic value because they are **used for commercial purposes**, also in the absence of a price paid for the commercial use of those data.

Furthermore, in the decision no. 27432, 29 November 2018 the AGCM considered:

a) as **a misleading commercial practice,** the professional's conduct consisting, during the first registration phase of the user on Facebook Platform, of the non-provision of clear, complete and immediate **information concerning the professional's activity of collecting and using, for commercial purposes, the data of its users**. The AGCM considered that the information provided by Facebook is generic and incomplete and that it does not adequately distinguish between, on the one hand, the use of data for the customization of the service with the aim of facilitating socialization with other users ("consumers"), and on the other hand, the use of data to carry out targeted advertising campaigns. **The misleading character of the practice is aggravated by the circumstance that, in the use of Facebook, the commercial purposes are mixed and presented as confused with the social and cultural purposes typical of the social network.**
b) as an **aggressive commercial practice**, the professional's conduct whereby it applies, in relation to its registered users, a mechanism that, through various steps, involves the **transmission of user data from the platform of the social network to third-party websites/apps and *vice versa*,** without the prior express consent of the person concerned, for the use of the data for profiling and commercial purposes. The option available to the user to authorise or not this method is pre-set on the consent to the technical integration between Facebook and third-party websites/apps (so-called "Platform activation"), which implies, by default, a generic predisposition to the reciprocal transmission (Facebook/third parties) of Facebook users' data, and users' right to opt out. Moreover, Facebook affirms that the deactivation of the above-mentioned integration produces penalizing consequences for the users, both in the use of Facebook, and in the accessibility and use of third-party websites and apps**. <u>The AGCM considered that this practice, by means of undue influence, is to be considered liable to considerably restrict the freedom of choice or conduct of the average consumer, thus inducing him/her to take a decision of a commercial nature that s/he would not otherwise have taken: in particular, the decision to integrate the functionalities of Facebook with those of third-party websites/apps, including games, and to transfer, consequently, his/her data from Facebook to third parties and vice versa</u>**. According to the AGCM decision, the professional exercises undue influence on registered

consumers, who, without express and prior consent, therefore unconsciously and automatically, suffer the transmission and use by Facebook/third parties, for commercial purposes, of the data concerning them (information deriving from the use of Facebook and from their own experience on third party websites and apps). Undue conditioning derives from the application of the pre-selection system of the widest consent to the transmission of one's own data from/to third parties, described above, together with the description of significant limitations in the usability of the social network and of the websites/apps of third parties due to the deselection of the transmission option.

With regard to **decision no. 26597, 11 May 2017**, the proceeding concerned WhatsApp's conduct towards its customers (consumer users) which had induced users to accept in full the changes made to the Terms of Use of the WhatsApp Messenger application, which provided the option, pre-selected, of sharing certain personal data from their WhatsApp with Facebook so that the company could use such data for commercial profiling and advertising purposes. In the event of non-acceptance of those changes, the information given to the user/consumer suggested that the service would be discontinued. It should also be noted that for those who were already users of the application at the time of the update, WhatsApp allowed them to accept its contents even "partially". The existence of this option was not stated on the main screen dedicated to the acceptance of the new Terms of Use. Only on the next screen, which was accessed by clicking on the link to the Terms and Privacy Policy, would the user have realized that s/he had an alternative choice – which was, however, pre-set – by checking the box provided, to consent to the sharing of data. If the user had wanted to continue to use the application, without sharing his/her data with Facebook, s/he would have to uncheck the checkbox.

The commercial practice is classified by the AGCM **as aggressive because, through undue influence, it is likely to significantly restrict the average consumer's freedom of choice or conduct, thereby causing him/her to take a transactional decision that s/he would not have taken otherwise**. This undue influence stemmed from the fact that WhatsApp Messenger users were effectively forced to accept the new contractual terms in full, in particular with regard to the sharing of data with Facebook, making them believe that it would otherwise have been impossible to continue using the application whilst those who were already users at the date of the amendment of the Terms instead had the opportunity to "partially" accept its contents.

In July 2019 the **Italian Consumer Protection Authority (AGCM), the Italian Data Protection Authority (GPDP) and the Media Authority (AGCOM) issued a joint statement entitled "Big Data. Joint Investigation, Guidelines and Policy Recommendations"**, in which they set out some shared guidelines and policies, which stated that it is necessary (point no. 10):

"To strengthen the powers of AGCM and AGCom to acquire information outside the investigation procedures and to increase the maximum level of sanctions in order to ensure an effective deterrent effect of the consumer protection rules".

In this respect, the Authorities affirmed that **consumer protection** can affect a variety of factors related to the relationship between operators and users in the acquisition and processing of data. According to the statement, the fact that the **legislation on the protection of personal data** is

applicable to the conduct of companies does not exempt them from complying with the rules **on unfair commercial practices**; **the two disciplines are seen as complementary and not alternative**. The authorities considered that consumer protection and privacy protection are undoubtedly important components of a fair competitive system.

As to the case law, the **Italian administrative court of Rome in its judgement no. 260, 10 January 2020**, which constituted the judicial review of the AGCM decision no. 27432/2018, stated that the economic value of the personal data of users requires the professional to inform the consumer that the information obtained from such data will be used for commercial purposes that go beyond its use in the "social network". The practice may be qualified as misleading in the case of a lack of adequate information, or in the case of misleading statements. The court confirmed the AGCM's decision, stating that the claim used by Facebook on the registration page in order to encourage users to subscribe ("Subscribe. It's free and it will be forever") suggested the absence of a counter-performance required from the consumer in exchange for the use of the service. Therefore, according to the court's judgement, the practice was to be sanctioned because of the incompleteness of the information provided, where the claim of the service's gratuitousness did not allow the consumer to understand that the professional would use his/her data for remunerative and commercial purposes.
Furthermore, the **Council of State, in its decisions nos. 2631 and 2630 of 29 March 2021**, stated that the rules on unfair commercial practices apply where the data subject provides personal data to the controller and a third party processes such data for commercial purposes, without the data subject being fully aware of such processing. However, the Council of State highlighted that the case should be interpreted, not as a case of commercialization of personal data by the data subject, but as a case where a data subject made information available to a third party, which used it for commercial purposes, without the data subject being fully aware of such purposes, also considering that s/he was misled by terms and conditions drafted by the professional.

Considering the Italian case law, and in light of the principle of effectiveness and dissuasiveness, the following questions can be raised:

In light of Article 47 of the Charter of Fundamental Rights, when there is a violation of data protection law and the conduct is qualified also as a commercial practice, taking into account Article 8 of the Charter of Fundamental Rights, what are the cases in which the practice is not to be considered unfair? Could a decision of the Data Protection Authority declaring a violation of data protection rules be relevant to the Consumer Authority's assessment concerning the existence of an unfair practice? If so, is it decisive in that assessment?

9.3.3. Question 1b – Competent administrative authorities and their coordination

b. What authority is competent? How should authorities coordinate themselves in light of the principles of effectiveness, good administration and duty of cooperation?

National cases

Italy

The Consumer Protection Authority examined the question of its **competence** in Decisions 27432, 29 November 2018 and no. 26597, 11 May 2017. The AGCM stated that the data protection and the commercial practicesdisciplines have different material scopes and pursue different interests. As a result, the Authority affirmed that there is no conflict between the two disciplines; rather, they are complementary. On this basis, the authority stated that the conducts analysed in the proceeding were considered in light of the rules on unfair commercial practices. Therefore, the Italian Consumer Protection Authority affirmed its competence.

It should be noted that in both proceedings (related to decision no. 27432, 29 November 2018 and decision no. 26597, 11 May 2017), the Italian Consumer Protection Authority requested an **opinion from the Italian Media Agency** (*Autorità per le Garanzie nelle Comunicazioni*, AGCOM), in accordance with **article 27(6) of the Consumer Code**, which states that when a commercial practice has been or is intended to be disseminated in the periodical or daily press, or by radio or television or any other telecommunications medium, before issuing a decision, the Consumer Protection Authority shall request the opinion of the Communications Regulatory Authority.

In July 2019 the **Italian Consumer Protection Authority (AGCM), the Italian Data Protection Authority (GPDP) and the Media Authority (AGCOM) issued a joint statement entitled "Big Data. Joint Investigation, Guidelines and Policy Recommendations"**, in which they elaborated some shared guidelines and policies, and according to which (point no. 11) **it is necessary to create a permanent coordination among the three Authorities.** In particular, the Authorities considered that:

> "The challenges posed by the development of the digital economy and Big Data require full use to be made of the synergies between ex ante and ex post instruments for protecting privacy, competition, consumers and pluralism.
> AGCM, AGCom and the GPDP, each within their own sphere of competence, can best guarantee their own institutional objectives, insofar as they will be able to take full advantage of the opportunities offered by fruitful cooperation.
> To this end, the three Authorities, in the exercise of the complementary competences assigned to them and which contribute to tackling the critical issues of the digital economy, are committed to close forms of collaboration in interventions that affect the digital markets, including through the signing of a memorandum of understanding."

The Authorities considered also that in order to allow a full understanding of the new phenomena in the digital economy, it seems appropriate to strengthen the powers of acquisition of information by AGCM and AGCOM outside the investigative procedures (investigations, pre-instructive activities), including the possibility to impose administrative sanctions in case of refusal or delay in providing the information.

In the judgement of the **Italian administrative court of Rome no. 260, 10 January 2020**, which constitutes the judicial review of the AGCM decision 27432/2018, the court addressed the

question of the consumer protection authority's competence, which was denied by the claimant. The court stated that the plaintiff's arguments presupposed that the protection of personal data only concerns fundamental rights. The national court considered that this approach did not take into account the economic value of personal data. The court stated that personal data are to be protected as an expression of an individual's right to privacy, and as such subject to specific and not renounceable forms of protection, such as the right to revoke consent, access, rectification, erasure.

In the court's view, a different kind of protection of personal data should be developed, because of the economic value of personal data. The court affirmed that the existence of an economic value of personal data, typical of the new economies of digital markets, requires operators to respect, in the relative commercial transactions, those obligations of clarity, completeness and non-deceptiveness of the information imposed by the legislation for protection of the consumer, who must be made aware of the exchange related to the adhesion to a contract for the fruition of a service, such as the use of a "social network". The court recalled the *Guidance on the Implementation/Application of Directive 2005/29/ec on Unfair Commercial Practices* released by the EU Commission on 25 Mary 2016, where the economic value of personal data and the possible relevance of Directive 2005/29 was affirmed.

Moreover, the Italian administrative court stated that the omission of information about the exploitation for commercial purposes of user data is not a matter entirely regulated and sanctioned within data protection law. The court recalled also *Wind Tre* (C-54 and C-55/17), concerning the coordination among multiple administrative bodies competent in relation to the same conduct.

Then, according to the court in the present case, there was no incompatibility or antinomy between the provisions of data protection and consumer law, since they are complementary, imposing, in relation to the respective purposes of protection, specific information obligations, in one case functional to the protection of personal data, understood as a fundamental right, and in the other to the correct information to be provided to the consumer in order to allow him/her to make an informed economic choice.

Furthermore, the court highlighted that there was not a risk of over-deterrence consisting in a double sanction for the same conduct, considering that the object of investigation by the competent authorities concerned different conducts by the operator, the correct processing of personal data and the clarity and completeness of the information about the exploitation of the data for commercial purposes.

Similar arguments and the same conclusion were adopted by the **administrative court of Rome in the judgement 10 January 2020, no. 261**.

The **Italian Council of State, in its decisions nos. 2631 and 2630 of 29 March 2021**, confirmed the decision of the Tribunal. In its reasoning, the Council of State considered that the special EU discipline of personal data protection has a very extensive scope also due to the broad notion of "processing" (Article 4 GDPR), but that the application of data protection rules does not exclude the application of other disciplines, such as consumer law. Therefore, according to the Council of State, there is not a principle of the speciality of data protection law that excludes

the application of other provisions. In this regard, the Council of State considered that, when the processing involves behaviours and situations regulated by other legal sources for the protection of other values and interests, the legal system – first at the EU level and then at the national level – cannot exclude the application of other sectoral disciplines, such as that of consumer protection, to reduce the protection guaranteed to natural persons. Accordingly, the Council of State affirmed the need to ensure "multi-level protections" that can enhance the protection of individuals' rights. As to the merits of the case, the Council of State affirmed that not at stake was the commercialization of personal data by the data subject, but instead the exploitation of personal data made available by the data subject in favour of a third party who will use it for commercial purposes, without the data subject being fully aware of the data uses.

Germany

On 6 February 2019, the German Competition Authority (*Bundeskartellamt*), which was also granted competences in the area of consumer protection, issued a decision against Facebook for abusing its dominant position on the German market for social networks, based on violations of data protection law. In its summary of the decision,[59] the Authority explained that the GDPR does not rule out the possibility for authorities other than the national data protection authorities (including competition and/or consumer protection authorities) to apply substantive data protection law.

The Authority also explained that the GDPR explicitly states that data protection law can also be enforced under civil law, i.e. that full consistency is not aspired to. More importantly, the Authority specified that:

> "This applies in particular to consumer protection organisations and competitors and their associations. These entities can enforce data protection based on stipulations of the Act Against Unfair Competition (UWG) or regulations on business terms linked to data protection and also based on Section 19 GWB. A large part of the ECJ's case law which data protection authorities and the data protection board have to consider has been obtained from civil law proceedings. Civil law proceedings promote rather than threaten the consistent implementation of data protection law, especially as the ECJ can be involved at an early stage as part of the preliminary ruling procedure".

The *Bundeskartellamt* explained that, in the course of its proceedings against Facebook, it had maintained regular contact with data protection authorities, none of which has considered that it had exclusive competence. This is consistent with the approach taken by the Italian competition, data protection and telecom authorities in their joint statement.

EU law perspective

The AGCM decision of May 2017 fining WhatsApp for data transfer to Facebook came three years after the European Commission approved the merger between the two companies.[60] In its

[59] https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=3

[60] European Commission, Case COMP/M.7217 Facebook/Whatsapp 3 October 2014.

merger decision, the Commission had concluded that the merged entity would be unable to establish reliable automated matching between Facebook users' accounts and WhatsApp users' accounts. However, in August 2016, WhatsApp announced updates to its terms of service and privacy policy, including the possibility of linking WhatsApp users' phone numbers with Facebook users' identities. This led the Commission to fine Facebook €110 million for providing misleading information during the merger process.[61]

Therefore, the Italian authority issued a decision against WhatsApp based on consumer law, but the problem originated in the Commission's decision not to oppose the merger. Since then the Commission has been criticised for not taking sufficient account of data-protection concerns in its review of the merger. In its decision, the Commission indeed stated that:

> "For the purposes of this decision, the Commission has analysed potential data concentration only to the extent that it is likely to strengthen Facebook's position in the online advertising market or in any sub-segments thereof. Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules".

Nothing in the Commission's decision suggests that it had coordinated its investigation with national data or consumer protection authorities. This illustrates the fact that there is a lack of coordination among the different national and European authorities in the field of consumer, data protection and competition enforcement.

In this respect, t**he Advocate General, in its opinion on case C-319/20 of 2 December 2021, has** recently stated that "in the modern economy, marked by the boom in the digital economy, personal data processing is liable to affect individuals not only in their capacity as natural persons enjoying the rights conferred by Regulation (EU) 2016/679, but also in their capacity as consumers".

The following questions therefore arise:

In light of the principles of effectiveness and good administration, is it necessary to provide a system of coordination between data protection and consumer authorities at national and European level? Could the documents and the investigations made by an authority be used in proceedings of another authority?

9.4. Information to be provided to the data subject and consumer protection

Main questions addressed

Question 1 Could, in light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the Charter of Fundamental Rights, the **Unfair Contractual Terms Directive** (93/13) and the **Consumer Rights Directive** (2011/83) be

[61] https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1369

applied in the case of missing or wrongful information to be provided to the data subject?

Question 2 In light of the principles of effectiveness, proportionality, equivalence, dissuasiveness and Article 47 of the Charter of Fundamental Rights, what is the **relationship between the information duties provided in Articles 5 and 6 of the Consumer Rights Directive** (2011/83) and in **Articles 13 and 14 of the General Data Protection Regulation** (2016/679)? Could the information duties provided in the Consumer Rights Directive be interpreted, in certain cases, as covering also those of the General Data Protection Regulation? What are the consequences on remedies available under the Consumer Rights Directive?

Question 3 In light of Articles 41 and 47 of the Charter of Fundamental Rights, what is the relationship between the administrative authorities and the judicial ones? Is there an impact of the principles of effectiveness, proportionality and dissuasiveness on organizing the coordination between data protection authorities ascertaining a data protection violation and judicial authorities in proceedings concerning the ascertainment of a consumer law violation?

Relevant national cases in the cluster:

- LG Berlin, 30/04/2013, (2013) *Neue Juristische* Wochenschrift 2605, 2606 – Apple
- LG Berlin, 19/11/2013, (2014) *MultiMedia und Recht 563, 565* – Google
- LG Frankfurt a.M., 10/06/2016, (2016) *Beck Rechtsprechung (BeckRS) 10907* – Samsung

9.4.1. Question 1 – Unfair contractual terms and information provided to the data subject

Could, in light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the Charter of Fundamental Rights, the **Unfair Contractual Terms Directive** (93/13) and the **Consumer Rights Directive** (2011/83) be applied in the case of missing or wrongful information provided to data subject?

With regard to this question, there are no European-level cases.

This sub-section will therefore focus on German national cases.

National case law

Germany

On **30 April 2013**, the **Landgericht Berlin** (District Court of Berlin) issued a decision against **Apple**.[62] The plaintiff, a consumer-protection association, requested an injunction against non-transparent clauses in the defendant's terms and conditions. The defendant sold computer hardware and communication devices. It also operated a telemedia service, which was available

[62] Registration no. 15 O 92/12.

in German at 'www.apple.com/de'. On this website, the defendant published its terms and conditions, as well as its 'Apple privacy policy'. The plaintiff claimed that clauses of the privacy policy and the terms and conditions were problematic under § 307 BGB and requested an injunction against their use.

The district court held that the clauses of a privacy policy also constitute terms and conditions. Under § 305 German Civil Code, terms and conditions are pre-formulated conditions for numerous contracts which one party stipulates with the other. On the basis of the presentation of the privacy policy as part of the order process (as a one click-wrapping option with the terms and conditions), the court adopted the least consumer-friendly interpretation of that clause. It held that consumers would assume the privacy policy to be part of the terms and conditions of the order. Consequently, the privacy policy formed part of the terms and conditions and was subject to the same control.

On **19 November 2013**, the **Landgericht Berlin** (District Court of Berlin) issued a decision against **Google**.[63] The defendant offered numerous services on its website, i.e. a well-known internet search engine, specialised search engines for images, maps, books, movies, e-mail and calendar services. Many of these services could be used without registration and free of charge, whereas some of them (i.e. the email service) required registration, and some were chargeable.

The plaintiff, a registered consumer-protection association, first successfully requested an injunction regarding the terms of use and its privacy policy against the defendant in 2008.[64] In the case considered, the plaintiff requested an injunction against the defendant's updated Terms of Use and privacy policy (as used on the website in July 2012).

One of the issues dealt with by the District Court of Berlin was the extent of the possibility to control privacy policies and terms of services, and whether certain clauses of the terms and conditions are void.

First, the court decided that the defendant's terms of use and privacy policy constituted terms and conditions and were, thus, subject to the same level of control. It was decisive that the defendant's conditions of contract were pre-formulated for a multitude of contracts and stipulated in a one-sided manner. Adopting the least consumer-friendly interpretation of the website, the privacy policy was included in the analysis because it was impossible to sign up for the defendant's services without consenting to that policy and the terms of use via a single click-wrapping link. Consequently, the terms of use and the privacy policy constituted terms and conditions. In addition, the defendant's services did not constitute 'gifts', but rather a reciprocal relationship because the defendant made use of information collected in exchange for the services offered.

Second, the court declared several clauses of the defendant's terms and conditions void on the grounds that the clauses were worded too broadly and that some of them were too one-sided. For example, it was unclear to the consumer how the defendant examined the uploaded content

[63] Registration no. 15 O 402/12.

[64] LG Hamburg, judgement of 19.05.2011 - 10 U 32/09.

and what constituted infringements, because the clauses were phrased too generally and did not contain restrictions regarding conduct entailing criminal responsibility. The defendant also assumed continuing obligations although it should have been possible to terminate the relationship in the case of misconduct by either party. The privacy policy was similarly declared void because the consumer could not understand from it how his/her data would be processed. Lastly, the clauses regarding the 'android market' were illegal insofar as the defendant was authorized to access the devices owned by the consumer, to unilaterally change the conditions of the contract, and to terminate the use of services. Therefore, the court stressed that it did not matter whether the clauses were currently in use. Due to the abstract danger of re-offending, an official court injunction was necessary.

On **10 June 2016**, the **Landgericht Frankfurt** (District Court of Frankfurt) issued a decision against **Samsung Electronics**.[65] The plaintiff was the consumer-protection association of North Rhine-Westphalia. It acquired a 'smart TV' produced by the defendant Samsung Electronics. These 'smart TVs' feature the 'Smart Hub' user surface, where consumers can access third-party applications, but also upload their own movies and receive recommendations regarding a TV programme. In the assembly instructions, there was reference neither to the terms and conditions, nor to the privacy policy. The terms and conditions related to the privacy policy could be accessed after the assembly of the television set. During the first use of the television, it uses the consumer's IP address to download and present the terms and conditions, as well as the appropriate privacy policy according to the region of the purchaser. The purchaser can then read the terms and conditions and the privacy policy displayed without sub-sections or headings, and then issue a blanket approval regarding them. The plaintiff complained that the HbbTV function was activated without the consent of the consumer, and that this function transferred data to the producer without previously informing or obtaining the consumer's consent.

Addressing the points raised by the plaintiff, the Frankfurt district court concluded that there was no obligation on the defendant to inform the consumer about the activated HbbTV function, and the possible transfer of information. While this function transmits IP-addresses, §13(1) TMG is aimed at service providers who use data collected during the provision of the service. The defendant was not in a position where it had active knowledge of the data or the authority to dispose of the collected data. Hence, §13(1) TMG was not applicable to the defendant.

While the Frankfurt district court addressed the points raised by the plaintiff, its focus was on controlling the terms and conditions, including the privacy policy without explicit discussion. The district court raised this issue on its own motion and decided that the privacy policy lacked transparency. Due to its length and unclear presentation (56 TV pages in running text without sections or headings), the district court found that the privacy policy was not a suitable basis for agreeing to the collection and use of data. Furthermore, the court deemed the phrasing of the privacy policy unsuitable. At the beginning of the use of the product, the provider had to inform the consumer about the form, extent and purpose of collecting and using the data in an understandable manner.

[65] Registration no. 2-03 O 364/15.

Therefore, it was necessary to inform the consumer about what kind of data would be collected. By using phrases including 'for example' and 'possibly' regarding the data used, the provider did not present an exhaustive list of what kinds of data were collected, and the consumer could not validly agree.

EU law perspective

Article 3(1) of the **Unfair Contractual Terms Directive** (the ***UCTD***) provides that terms that have not been negotiated individually should be considered as unfair if they cause "a significant imbalance in the parties' rights and obligations arising under the contract". This provision gives courts the possibility to consider if violations of information requirements under the GDPR cause a significant imbalance in the parties' rights and obligations.

Nevertheless, **in the case of conflict between the UCTD and the GDPR**, the latter should be considered the *lex specialis* because it regulates the specific sector of data protection. Indeed, it could be argued that Recital 42 of the GDPR provides indications on how to apply the UCTD in the area of data protection, (and therefore has *lex specialis* value) by providing that "in accordance with Council Directive 93/13/EEC a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment".

In July 2019, the Commission adopted a **Guidance Notice on the interpretation and application of the Unfair Contractual Terms Directive**.[66] The Guidance was remarkably silent about the interplay of transparency requirements under the Directive and similar information duties under data protection provisions. However, concerning the interplay of transparency requirements under the Directive and those in other EU instruments in general, the Guidance stated as follows:

- "Where other EU provisions apply in addition to the UCTD, one will, in general, favour an interpretation that preserves as much as possible the *effet utile* of the UCTD and of a potentially conflicting provision. For instance, rules of procedure should not jeopardise the effectiveness of the protection against unfair contract terms under the UCTD" (p. 16).
- "Various EU acts regulate in a detailed fashion the pre-contractual information that traders have to provide to consumers in general or with regard to specific kinds of contracts. […] The UCTD is without prejudice to such provisions and the consequences of the failure to comply with them as set out in such specific instruments" (p.28).
- "Insofar as specific pre-contractual and contractual information requirements apply, they will also have to be taken into account for the transparency requirements under the

[66] Commission notice — Guidance on the interpretation and application of Council Directive 93/13/EEC on unfair terms in consumer contracts, OJ C 323, 27.9.2019, pp. 4–92.

UCTD, on a case-by-case basis, and in light of the purpose and scope of those instruments" (p. 28).

- "The fact of whether a seller or supplier has complied with sector-specific requirements is an important element when assessing compliance with the transparency requirements under the UCTD. However, given the parallel applicability of the UCTD with sectorial legislation, compliance with such instruments does not automatically indicate compliance with all transparency requirements under the UCTD" (p. 29).

Since this guidance was published after the entry into force of the GDPR, it is reasonable to assume that the Commission foresaw the interaction of the transparency requirements provided for in the UCTD and the GDPR when drafting these guidelines.

Regarding the relationship between information duties under the Consumer Rights Directive and the GDPR, see Section 9.4.2 below.

9.4.2. Question 2 – Relationship between information duties under the Consumer Rights Directive and the GDPR

In light of the principles of effectiveness, proportionality, equivalence, dissuasiveness and Article 47 of the Charter of Fundamental Rights, what is the **relationship between the information duties provided in Articles 5 and 6 of the Consumer Rights Directive** (2011/83) and in **Articles 13 and 14 of the General Data Protection Regulation** (2016/679)? Could the information duties provided in the Consumer Rights Directive be interpreted, in certain cases, as covering also those of the General Data Protection Regulation? What are the consequences for remedies available under the Consumer Rights Directive?

EU law perspective

In this area, the maxim *lex specialis derogat legi generali* is confirmed by Article 3(2) of the **Consumer Rights Directive**, which provides that in the case of conflict with another Union act governing specific sectors, the provision of that other Union act shall prevail and shall apply to those specific sectors.

In June 2014, the Commission adopted a **Guidance document concerning the Consumer Rights Directive.** This Guidance stated that, in the case of conflicts about information requirements provided for in Directive 95/46/EC (the Data Protection Directive) or Directive 2002/58/EC (the ePrivacy Directive), these sector-specific requirements prevail. In online sales, this is especially relevant to issues such as information about data processing and data subjects' consent to the tracking and use of personal data supplied. By extension, this may also hold true for the General Data Protection Regulation. Therefore, information duties stated in both the Consumer Rights Directive and the GDPR apply in parallel, but the ones from the latter prevail in the case of conflict. This is consistent with the fact that the GDPR contains more detailed transparency requirements than the Consumer Rights Directive does.

However, the fact that the European legislator has adopted sector-specific requirements and specifies that they prevail in the case of conflict means that the **information duties provided in the Consumer Rights Directive cannot automatically cover those of the GDPR**.

It is true that both consumer protection and data protection pursue **common purposes**, such as the free movements of goods and services in the internal market, transparency, and fair treatment. However, a teleological interpretation of both instruments arguing that information duties from the Consumer Rights Directive also cover those of the GDPR would be difficult to reconcile with the textual interpretation set forth above.

Hence, the **remedies** available under the Consumer Rights Directive cannot be used against violations of information duties provided in the GDPR alone. Violations of information duties under the GDPR can only be remedied with the Consumer Rights Directive if they also constitute violations of information requirements under that Directive.

9.4.3. Question 3 – Relationship between the administrative and judicial authorities

In light of Articles 41 and 47 of the Charter of Fundamental Rights, what is the **relationship between the administrative authorities and judicial ones**? Is there an impact of the principles of effectiveness, proportionality and dissuasiveness on organizing the coordination between data protection authorities ascertaining a data protection violation and judicial authorities in proceedings concerning the ascertainment of a consumer law violation?

This question concerns the possible impact of an administrative decision issued by a data protection authority which ascertains a data protection violation on a judicial proceeding concerning ascertainment of a consumer law violation. In this respect, the new Directive 2020/1828, on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC was adopted on 25 November 2020, and the new **Directive 2019/2161 on the better enforcement and modernisation of Union consumer protection rules** should be considered.

As explained above, Directive EU 2020/1828, on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC was adopted on 25 November 2020. With this new Directive, the EU legislator set out rules to ensure that representative actions aimed at the protection of the collective interests of consumers are available in all Member States.

It should first be noted that the Directive allows Member States to decide whether the representative action can be brought in judicial or administrative proceedings. Recital 19 of Directive 2020/1828 provides:

> "Since both judicial proceedings and administrative proceedings could effectively and efficiently serve to protect the collective interests of consumers, it is left to the discretion of the Member States whether a representative action can be brought in judicial proceedings, administrative proceedings, or both, depending on the relevant area of law or

the relevant economic sector**. This should be without prejudice to the right to an effective remedy under Article 47 of the Charter, whereby Member States are to ensure that consumers and traders have the right to an effective remedy before a court or tribunal, against any administrative decision taken pursuant to national measures transposing this Directive. This should include the possibility for a party in an action to obtain a decision ordering the suspension of the enforcement of the disputed decision, in accordance with national law**".

The Directive further deals with the coordination between administrative and judicial authorities. In particular, Article 15 of Directive 2020/1828 states:

> "Member States shall ensure that the final decision of a court or administrative authority of any Member State concerning the existence of an infringement harming collective interests of consumers can be used by all parties as evidence in the context of any other action before their national courts or administrative authorities to seek redress measures against the same trader for the same practice, in accordance with national law on evaluation of evidence.".

On 27 November 2019, the European Parliament and the Council also adopted the new **Directive on the better enforcement and modernisation of Union consumer protection rules**, 2161/2019. The amending Directive modernized Directive 2005/29/EC (unfair commercial practices), Directive 93/13/EEC (unfair contract terms), Directive 2011/83/EU (consumer rights), and Directives 98/6/EC (indication of prices).

The new Directive states that consumers have the right to bring individual actions if they are harmed by unfair commercial practices, such as aggressive marketing. Member States shall provide contractual and non-contractual remedies. At minimum, contractual remedies should include the right to obtain a price reduction or to terminate the contract. Non-contractual remedies should, as a minimum, include the right to compensation for damages. To that effect, the new Directive inserts a new Article 11a entitled 'Redress' to Directive 2005/29/EC, which states:

> 1. "Consumers harmed by unfair commercial practices, shall have access to proportionate and effective remedies, including compensation for damage suffered by the consumer and, where relevant, a price reduction or the termination of the contract. Member States may determine the conditions for the application and effects of those remedies. Member States may take into account, where appropriate, the gravity and nature of the unfair commercial practice, the damage suffered by the consumer and other relevant circumstances.
> 2. Those remedies shall be without prejudice to the application of other remedies available to consumers under Union or national law".

This right to individual remedies was introduced in Directive 2005/29/EC because the Commission considered that consumers harmed by unfair commercial practices did not have

access to effective remedies. Indeed, while Directive 2005/29/EC did ban aggressive and misleading commercial practices, it did not harmonise the rules on remedies.
Taken together, both Directives would allow consumers, who in some cases may also be data subjects, harmed by unfair commercial practices to initiate representative actions and seek the new remedies available for infringements of unfair commercial practices. While individual consumers should not be able to interfere with the procedural decisions taken by the qualified entities allowed to initiate the action, the consumers concerned by a representative action should be entitled to benefit from that representative action. In representative actions for redress measures, the benefits should take the form of remedies, such as compensation, repair, replacement, price reduction, contract termination or reimbursement of the price paid. In representative actions for injunctive measures, the benefit for the consumers concerned would be the cessation or prohibition of a practice that constitutes an infringement (recitals 36 and 37).

9.5. Guidelines emerging from the analysis

The general issue addressed in this chapter concerns the intersections between consumer and data protection.

Collective redress between collective and data protection

With regard to collective redress, national legislation could allow consumer-protection associations to bring or defend legal proceedings against a person allegedly responsible for an infringement of the protection of personal data (*Fashion ID,* C-40/17).
Furthermore, when a violation of the GDPR violate the interests of consumers, and the person harmed is a consumer, Directive 2020/1828 on representative actions for the protection of the collective interests of consumers, which repealed Directive 2009/22 is to be applied. In any case, the relationship between collective redress in consumer and data protection should be carefully assessed; the existence of collective redress in consumer law, applicable to consumers who seek action for a data protection claim, may not be sufficient for ensuring effective data protection, especially within the digital context (e.g. where the parties are a small business and an online platform).
On the extension of collective redress, Article 80 GDPR does not preclude national legislation which allows a consumer-protection association to bring legal proceedings, in the absence of a mandate conferred on it for that purpose and independently of the infringement of specific rights of the data subjects. The legal proceedings can be brought against the person allegedly responsible for an infringement of the laws protecting personal data because of the infringement of the prohibition of unfair commercial practices, a breach of a consumer protection law, or the prohibition of the use of invalid general terms and conditions, where the data processing concerned is liable to affect the rights that identified or identifiable natural persons derive from that regulation.

Unfair commercial practices and information provided to the data subject

According to the EU Commission's *Guidance on the implementation/application of the Unfair Commercial Practices Directive,* although a trader's violation of Data Protection rules will not, in itself, always mean that there is an unfair commercial practice, data protection violations should be considered when assessing the overall unfairness of commercial practices, particularly in the situation where the trader processes consumer data in violation of data protection requirements. The Italian decisions of the Consumer Protection Authority and the related case law are examples of the interplay between data protection rules and Directive 2005/29.

Information to be provided to the data subject and consumers' rights (Directive 2011/83)

The amendments of Directive 2011/83 provided in Directive 2019/2161 show the importance of the relationship between data and consumer law. In fact, the Directive applies when the trader supplies or undertakes to supply digital content which is not supplied on a tangible medium or a digital service to the consumer and the consumer provides or undertakes **to provide personal data** to the trader, except in some specific cases (Article 3 Directive 2011/83). Moreover, before the consumer is bound by a distance or off-premises contract the trader shall provide the consumer with the information concerning the fact that the price was personalized on the basis of automated decision-making.
However, the **remedies** available under the Consumer Rights Directive cannot be used against violations of information duties provided in the GDPR alone. Violations of information duties under the GDPR can only be remedied with the Consumer Rights Directive if they also constitute violations of information requirements under that Directive.

Information to be provided to the data subject and unfair contractual terms

National case law (especially French and German) shows the importance of the interplay, with regard to information duties, between the GDPR and the UCTD Directive. There are not EU case law or documents in that regard. Nevertheless, the principle of effectiveness and Article 47 and 8 CFR may give important guidance in interpreting the relationship between the notion of unfairness under Directive 1993/13 and breaches of data protection law.

Competent administrative authorities and their coordination

As explained in a joint statement of July 2019 by the Italian consumer, telecom, and data protection authorities, **data protection and consumer protection are complementary, and not mutually exclusive**.
The same conduct can constitute an infringement of consumer, data protection and competition law. At least at the European level, there is a **lack of coordination between the national and European authorities** in charge of consumer, data protection and competition enforcement, which may have negative consequences on the principles of effectiveness, good administration and the duty of cooperation.

Lack of conformity of digital content or services and the GDPR compliance

In light of Article 47 8 CFR, and of recital 48 of Directive 2019/770 on digital contents and services, the remedy which consists in the bringing-into-conformity of a service with regard to data protection compliance could be a means to gran consumers the right to data protection.