

A study on the personal data processing and the UCPD focused on Italy, Germany and the UK

Maastricht Journal of European and
Comparative Law
2021, Vol. 28(1) 7–29
© The Author(s) 2020
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/1023263X20961493
maastrichtjournal.sagepub.com



Maja Nišević* 

Abstract

Manipulation with Big Data Analytics allows commercial exploitation of individuals based on unfair commercial practices. Consequently, the concepts of consumer protection are essential in the data-driven economy and a central issue for effective safety for individuals in the Big Data Age. Although the fields of consumer protection and data protection in the European Union (EU) have developed separately, there is an unambiguous relationship between them. While the GDPR plays a crucial role in an individual's data protection in a case of personal data processing, Directive 2005/29/EC (UCPD) plays an essential role in regulating an individual's protection from the unfair commercial practice when it comes to personal data processing. A vital aspect of the UCPD is the enforcement of issues related to consumer privacy. However, a much-debated question is whether the UCPD is fully effective or not when it comes to personal data processing. This paper examines case law examples on WhatsApp and Facebook in Italy, Germany and the United Kingdom. This paper also aims to come to a conclusion on the issue of the applicability of the rules on unfair commercial practice when it comes to data processing.

Keywords

The UCPD, data processing, unfair commercial practice, data protection, consumer protection

I. Introduction

Individuals are providing a lot of personal data through their active participation in social networks, posts on blogs and email communication. Consequently, personal data plays an essential role in the information society.

*University of Verona Department of Law

Corresponding author:

Maja Nišević, University of Verona Department of Law, Via S. Francesco, 22 Verona, 37129 Italy.

E-mail: maja.nisevic@univr.it

Development of Big Data Analytics offered substantial economic and commercial benefits to the private and public domain. Collecting and processing data through Big Data Analytics is often called the gold oil of the 21st century. Big Data Analytics, as an emerging technology, changed how data is collected, analysed and applied. Besides, data manipulation through Big Data Analytics has become essential for running today's businesses. However, Big Data Analytics includes novel, complex and sometimes unexpected non-transparent uses of personal data. The open question is whether Big Data Analytics could be considered personal even in a case of anonymization of personal data. There are two fundamental reasons for this question. Firstly, Big Data Analytics interferes with the privacy of individuals. Secondly, Big Data Analytics often leads to an imbalance between the data subject and data controllers.

Since the primary concern of personal data processing is either data collection or data manipulation intending to produce new information about individuals, it is not surprising that personal data processing is mainly used for commercial purposes. Besides, the use of Big Data Analytics has become a successful tool to create individual profiles that can be used for commercial and other purposes. Considering all the advantages of the collection and processing of personal data through Big Data Analytics, traders can very quickly obtain information about an individual's preferences or expected behaviour. Information about individuals can be communicated openly to the user (for example, recommendations for a specific music show or restaurant) or merely assumed by the user (for example, an advertisement that is not related to a past search) or can be hidden entirely (for example, data being assembled and sold by data brokers, such as Acxiom, or by other third parties, as was the case in the Cambridge Analytica scandal).¹ It is necessary to clarify that the consumer data are often processed to a third party, whose business is adding value with Big Data Analytics. In that regard, difficulties for consumer protection arise when an attempt is made to implement commercial exploitation of the consumer based on unfair commercial practices.

Without any doubt, the data-driven economy opens specific issues that have come up concerning transparency, payment with data and the moving meaning of the consumer benchmark. Although the development of the data economy does not raise the different legal doctrinal structures at a fundamental level, it does raise questions as to how existing doctrines can respond to the emergence of data-driven technologies. Current regulation may provide adequate answers to the question of which rights consumers can enforce against traders. However, modern consumer protection law requires a cornerstone. The GDPR,² as the main legislation on data protection in the European Union (EU) concerning the EU Charter of Fundamental Rights,³ sets out the rules regarding data processing.⁴ Looking at the EU Court of Justice (CJEU) case law, data processing includes the collecting, retrieving, recording, organization, storage and disclosing or making available of the data to third parties.⁵

1. See M. Büchi et al., 'The Chilling Effects of Algorithmic Profiling: Mapping the Issues', 36 *Computer Law & Security Review* (2019).

2. 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) [2016] OJ L 119.

3. Article 8 of EU Charter of Fundamental Rights.

4. Article 4(1)(2) GDPR.

5. See European Commission, What constitutes data processing? https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en.

Generally said, data processing contains six stages: data collection, data preparation, data input, data processing, data output and data storage.⁶

Since Big Data Analytics is often used for running a business, it imposed a causal relationship between consumer protection law and data protection law in the EU. In that regard, while the GDPR plays a crucial role in an individual's data protection, Directive 2005/29/EC (the UCPD)⁷ plays a vital role in regulating an individual's protection from unfair commercial practice when it comes to personal data processing. From one side, the GDPR may have contributed to the increase in impacts on unfair commercial practices, concerning unfair means of communicating with consumers. On the other side, the UCPD offers protection when it comes to unfair commercial practices in business-to-consumer (B2C) transactions. Besides, traders who engage in unfairly influencing consumers by aggressive or misleading practices may distort consumers' economic choice-making. Responding to these practices, the UCPD aims to strengthen the consumer's choice and the fair operation of B2C markets. That is why the UCPD may have been an essential factor in the enforcement of consumer privacy issues considering the consumer's final decision.

In recent years there has been an interest from various national enforcement bodies in remedying commercial behaviour exploiting the increasing information and power between consumers and analytics companies. For this paper the examples of the Italian authority, the German authorities and the UK authority are researched. This paper then aims to analyse how national bodies are applied to different rules when it comes to personal data processing. For the research presented in this paper, the main focus is on WhatsApp and Facebook. This paper is divided into several sections. Section 2 is about the legal enforcement of the UCPD, including the interpretation of the online platform and consumer. Considering WhatsApp and Facebook cases in Italy, Germany and the UK, section 3, with its subsection, provides a broad overview of the rulings. Finally, section 4 provides a conclusion.

2. Legal enforcement of the UCPD in EU

The main aim of the UCPD lies in the prohibition of unfair commercial practices that are contrary to the requirements of professional diligence.⁸ Besides, the UCPD consists of specific prohibitions of misleading action and omission and aggressive practices.⁹ Finally, the UCPD consists of the last level of the prohibition set out in its Annex 1 (blacklist), which contains a list of unfair practices in any circumstance.¹⁰

However, the UCPD only sets the detailed framework for how the Member States may regulate commercial practice. Considering the UCPD's Article 11, Member States 'shall ensure adequate and effective means exist to combat unfair commercial practices' and that persons or organizations should be able to contest such practices by taking legal action and bringing the case before

6. See Case C-131/12 *Google Spain and Google*, EU:C:2014:317, para. 50.

7. Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (Text with EEA relevance)[2005] OJ L 149/22 .

8. Article 5 UCPD.

9. Article 6-7 and 8-9 UCPD.

10. Annex 1 of the UCPD.

administrative authorities. Consequently, the Member States had the power to decide which sanction is applicable in the case of violation. Article 13 stated that the Member States are obligated to lay down penalties for infringement of national provisions adopted in application of the UCPD and that these penalties shall be ‘effective, proportionate and dissuasive’. In addition, Article 16 UCPD set out the deadline for the UCPD adoption by the Member State.

Although there must be identical conditions within the system of enforcement among national legislation to achieve the UCPD’s objectives, several types of effect resulted after the UCPD was transposed into the national systems. Firstly, there are different examples of the UCPD implementation inside of the EU. Secondly, there are differences in how the Member States assess key concepts used in determining whether a commercial practice is unfair. Thirdly, there are differences in the interpretation of the image of consumers protected by national laws. Since the interpretation of the image of consumers varies among national systems inside of the EU, it is essential to clarify that there are Member States with strong consumer protection elements and Member States with strong controls on competition by competitors. Fourthly, there are differences in referring to the duties of the trader in commercial practices and especially in misleading advertising. All in all, the objective of maximum harmonization seems very difficult to reach when the general clause in Article 3 UCPD is constituted so that notions are open to national interpretation. Consequently, the enforcement of unfair commercial practices seems mostly unharmonized within the EU.

A possible explanation for all this might be that the Member States have introduced a different strategy for enforcing the rules, choosing between public and private enforcement. Concerning the history and the culture of the law governing unfair commercial practices, the UCPD implementation within the Member States has been carried out with different technical choices. Besides, some of the Member States already had legislation on unfair practices and others did not.

A. The UCPD and online platform

The UCPD does not define an online platform. However, Guidance on the UCPD¹¹ recognizes the online platform as a business model emerging in the digital economy.

The business model often referred to as an online platform may be a social media platform, online app store, search engine, e-commerce platform, user comparison review tools, collaborative economy platform, collective buying platform, etc.

One of the emerging services in the digital economy is internet-based communication services (OTT services – for example, voice over IP provided by WhatsApp).¹² The services mentioned are not still adequately regulated under the EU. Consequently, users face a very high risk of operator misconduct, and it creates a new challenge for the consumer protection agenda inside the EU.

The OECD report described the online platform as a range of services available on the Internet, including marketplaces, search engines, social media, creative content outlets, app stores, communications services, payment systems, services comprising the so-called ‘collaborative’ or ‘gig’ economy, and much more.¹³ Generally speaking, an online platform is a digital service that merely makes interactions between two or more Internet users.

11. Guidance on the application of the Unfair Commercial Practices Directive, https://ec.europa.eu/info/law/law-topic/consumers/unfair-commercial-practices-law/unfair-commercial-practices-directive_en.

12. Ibid.

13. See OECD, ‘What is an “Online Platform”?’ in OECD, *An Introduction to Online Platforms and Their Role in the Digital Transformation* (OECD Publishing, 2019), p. 19–26.

Since consumers play an essential role on the Internet, online platforms have become key market players, which are covering any service or application delivered over the Internet to consumers. Further, the EU digital market and digital platforms are essential factors for the EU's minimal digital borders. For this reason, digital platforms typically offer their services seamlessly across the entire EU. Without a doubt, digital platforms are bringing different benefits. Firstly, they are making consumers' lives more comfortable. Secondly, digital platforms are providing possibilities for consumers to enjoy the digital revolution.

However, the growth of digital platforms leads to different legal challenges. Data-driven technologies can learn about consumer preferences and tailor production and advertising to these preferences. Besides, very little of what happens with the data is clear and transparent to consumers. Lack of transparency and adequate information for consumers prevent consumers from assessing the real value of the service they are getting, as well as the underlying contractual relationship and economic trade-off that is taking place.¹⁴

B. Type of transactions covered by the UCPD

The UCPD has a comprehensive scope of application, and it is technology-neutral.¹⁵ It covers all B2C transactions. The UCPD contains a three-tier division. Firstly, it prohibits generally unfair practices. Secondly, it prevents explicitly misleading (action and omission) and aggressive practices. Thirdly, the UCPD includes blacklisted practices in its Annex 1.

For a practice to be covered by the UCPD it must be commercial by nature (that is, it must originate from a trader). It must be directly connected with the promotion, sale or supply of trader's products to consumers. Further, the UCPD's rules that are applicable B2C transaction means practices performed before, during and after a commercial transaction. For this reason, as it is defined in Article 2(1)(d) UCPD, commercial practice must be 'any act, omission, course, of conduct or representation, commercial communication including advertising and marketing, by a trader, directly connected with the promotion, sale or supply of product to consumers'. Consequently, UCPD is suitable for either offline or online B2C transactions.

The first step in evaluating the UCPD applicability to online B2C transactions contains the evaluation of whether the online provider is qualified as a trader under Article 2(1)(b) UCPD. Considering Article 2(1)(b) UCPD, a trader is any natural or legal person who is acting for purposes relating to his trade, business, craft or profession and anyone acting in the name of or on behalf of the trader. Here it is clear that Article 2(1)(b) UCPD covers not only traders who act on their account but also persons, including consumers, acting in the name of or on behalf of another trader. There is a strong possibility a that commercial transaction is assumed to be a B2C transaction, even though it exists between consumers. What follows from this type of transaction is the hidden B2C transaction. A hidden B2C transaction considers consumers who either act as a trader or act on behalf of traders, and are selling a product to other consumers. Considering the case law in the EU, the decision as to whether a seller qualifies as a trader or consumer varies from case to case. Still, the main criteria should be the presence of profit through commercial activities directed

14. See: BEUC, Ensuring Consumer Protection in the Platform Economy, Position paper, p. 7–12.

15. Article 3 of the UCPD.

towards consumers. Moreover, the national provision transposing the UCPD will determine who could be considered a trader.¹⁶

The second step in evaluating the UCPD applicability to online B2C transactions is the evaluation of whether the online provider is involved in B2C practices as stated in Article 2(1)(d) UCPD.

Concerning these evaluation steps, an online platform qualified as a trader must act following Articles 6 and 7 UCPD.¹⁷ Consequently, traders must avoid any misleading actions and omissions whenever engaging in the promotion, sale or supply of a product to consumers. In line with Article 6, a misleading action exists if it contains either false information and is untruthful or is likely to mislead the average consumer aiming to take a transactional decision that he would not have taken otherwise. In line with Article 7 UCPD, a commercial practice is misleading if it omits material information, and the average consumer needs to make an informed transactional decision. In the end, a commercial practice will always be unfair if it materially distorts or is likely to materially distort the average consumer's economic behaviour or the average member of the group.¹⁸

3. The UCPD and consumers

The protection system in the UCPD offers a consumer the right to information.¹⁹ This strong emphasis on the provision of information and transparency as being a good thing and an effective means of the consumer protecting himself came throughout the development of EU unfair commercial practices law. The key counterbalance to these transparency and information obligations was to create a strong consumer image, based on which picture consumers could be judged. In that regard, the UCPD Articles 5, 6 and 7 offer protection to the average consumer. The average consumer is not just the main objective for protection but also the main benchmark on which the assessment of the fairness of a trader's commercial practice is based. The case law of the CJEU firstly developed this notion of the average consumer.²⁰ Concerning the definition of the average

16. For instance, in a decision of 19 December 2014, the Italian Consumer and Competition Authority decided that an online travel intermediary was a 'trader' in relation to certain claims it had provided on its Italian website. The company's role was not limited to storing information on its platform, but it involved the activity of classification and systematization of information related to hotel facilities, restaurants and tourist attractions. In particular, the company provided a comparison service of tourist facilities. See: Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices, SWD(2016) 163 final, para. 5.5.2., p. 119.

17. Article 6 of the UCPD, 'Misleading action' and Article 7 of the UCPD, 'Misleading omission'.

18. Article 5(2)(b) of the UCPD.

19. Article 7 of the UCPD.

20. The genesis of the CJEU rules based on the average consumer can be identified in the judgment of the Court of 16 July 1998. Case C-210/96 *Gut Springenheide GmbH and Rudolf Tusky v. Oberkreisdirektor des Kreises Steinfurt – Amt für Lebensmittelüberwachung*, EU:C:1998:369. Gut Springenheide sold packed eggs with the indication '6-grain-10 fresh eggs' due to the fact that the food that was used for the animals was composed of 60% of a variety of different cereals. The court stated that for determining if a statement can be considered as misleading, the national courts should evaluate on the basis of the average consumer who is 'reasonably well informed and reasonably observant and circumspect'. This means that the consumer that is less averagely informed, observant and circumspect is not protected from the distortion of their economic behaviour. This practice of the court was repeated in Case C-220/98 *Estée Lauder Cosmetics GmbH v. Lancaster Group GmbH*, EU:C:2000:8, para. 30: 'Although, at first sight, the average consumer – reasonably well informed and reasonably observant and circumspect – ought not to expect a cream whose name incorporates the term "lifting" to produce enduring effects, it nevertheless remains for the national court to determine, in the light of all the relevant factors, whether that is the position in this case.'

consumer, there is always the presumption that the average consumer is expected to behave as a critical player in the market.

In sum, the UCPD defines the meaning of the consumer²¹ by introducing the consumer's type covered with the protection (that is, an average consumer) and defining the consumer as a means of assessment of the commercial practice fairness (that is, the consumer as a benchmark). The UCPD also introduced the meaning of the vulnerable consumer. Looking at Article 5(3) UCPD, 'vulnerable consumer' is used as a benchmark for assessing the fairness of a commercial practice when it hinders the economic interests of particularly vulnerable consumers.

A. The UCPD is suitable for an online platform

Considering that personal data is often sold to third parties and de facto has economic value, it is reasonable to assume that data-driven businesses engaging in B2C transactions should always fall under the scope of the UCPD. Besides, whenever an online platform can be considered a trader as regards the UCPD, it is required to act with a degree of professional diligence and not mislead consumers through action or omission. Further, looking at the online platform's data processing, the protection offered against the unauthorized use of consumer's data is provided by the transparency requirements set out in the UCPD.²² An example might be a trader who fails to disclose in a clear, intelligible and timely manner that personal data provided by the consumer are processed and used for commercial activities of the trader; this would be an unfair omission, defined in the UCPD.

It is more than clear that transparency requirements defined in the UCPD have a strong overlap with conditions stipulated in the GDPR (by Articles 13 and 14). Besides, the GDPR requires for lawfully personal data processing, the existence of the consumer consent or the performance of the contract, or the legitimate interests. However, data processing for commercial purposes is unlikely to itself constitute legitimate interest, and the existence of the consent is always doubtful.²³

From a practical point of view, consumer consent would mostly be obtained through the consumer's acceptance of general terms and conditions, in which data processing is included. For example, in popular social media platforms, such as Facebook, terms of services clearly state that personal data will be processed to evaluate some of the user's preferences.²⁴ Difficulties arise if a social media platform does not inform users that their data may be processed for commercial purposes. Further, some evidence suggests that social media as an online platform is often used by third-party traders to engage directly in unfair commercial practices towards users. For this reason,

21. Article 2(1)(a) of the UCPD.

22. At the first point, Article 6 and Article 7. In addition, it is necessary to mention here Directive 93/13/EEC of 5 April 1993 on unfair contract terms in consumer contracts [1993] OJ L 95/29, which protects consumers against unfair standard contract terms imposed by traders. It applies to all kinds of contracts on the purchase of goods and services, for instance online or offline purchases of consumer goods, gym subscriptions, or contracts on financial services, such as loans. For more information, see: EU Commission, Unfair contract terms directive, https://ec.europa.eu/info/law/law-topic/consumers/consumer-contract-law/unfair-contract-terms-directive_en

23. See V. Mak, 'Contract and Consumer Law', in V. Mak and E. Tjong Tjin Tai, *Research Handbook in Data Science and Law* (Edward Elgar Publishing, 2018), p. 17–38.

24. Point 2 'How are our services funded: We collect and use your personal data in order to provide the services described above for you. You can learn about how we collect and use your data in our Data Policy. You have controls over the types of ads and advertisers you see, and the types of information we use to determine which ads we show you.' Available at: www.facebook.com/terms.php

social media platforms, as well as other online platforms, which are considered as the traders under the UCPD, should take appropriate measures that enable relevant third-party traders to comply with transparency requirements under the UCPD.

Although online platforms should always provide detailed and accurate information for users concerning the UCPD, it is not always the case. The EU Commission investigation against merger activities between Facebook and WhatsApp showed that valuable Big Data caused anti-competitive market power because the same party controlled either the input or Big Data processing and collection.²⁵ All in all, Facebook engaged directly in unfair commercial practices towards consumers.

The importance of this investigation is not just that a fine was imposed on Facebook for the first time by the EU Commission, but also that it resulted in an investigation that has been carried out by national authorities of Member States.

4. Practical examples of Italy, Germany and the UK

Since the UCPD represents maximum horizontal harmonization in the EU, the UCPD only sets the specific framework for how the Member States may regulate commercial practice. The strict application of the UCPD caused Member States to substantially adapt their national legal systems to comply with the rules of the UCPD. On that ground, there are different examples of the UCPD implementation inside of the EU. For example, the single statute having common provisions for competitors, consumers and other market participants against unfair acts could be found in Germany. Unlike Germany, the existing Italian Consumers Code implemented the UCPD rules by Legislative Decree in the Italian Consumer Code. As far as unfair competition is concerned, Italian Competition Law plays an important role. By contrast, in the UK, the UCPD was implemented by the adoption of a new Regulation on Consumer Protection from Unfair Trading (CPR).

A. Example of Italy

Italy was among the first Member States that implemented the UCPD before the deadline.²⁶ The Italian legislator tried to balance the EU's ambition to harmonize legislation against unfair commercial practices through the national legal system. Consequently, Italy enacted different decrees,

25. EU Commission competition case No. COMP/M.7217 – Facebook/WhatsApp, para. 47: ‘the vast majority of social networking services are provided free of monetary charges. They can however be monetized through other means, such as advertising or charges for premium services’, and para. 167–190, inter alia para. 167, which states: ‘However, the Commission has examined whether the transaction could nevertheless have the effect of strengthening Facebook’s position in the online advertising market, thereby raising serious doubts as to its compatibility with the market. For this purpose, the Commission has analysed two main possible theories of harm, according to which Facebook could strengthen its position in online advertising by: (i) introducing advertising on WhatsApp, and/or (ii) using WhatsApp as a potential source of user data for the purpose of improving the targeting of Facebook’s advertising activities outside WhatsApp. Each of these two possible theories of harm is examined below’, and para. 168: ‘According to this possible theory of harm, post-Transaction, the merged entity could introduce targeted advertising on WhatsApp by analysing user data collected from WhatsApp’s users (and/or from Facebook users who are also WhatsApp users). This would have the effect of reinforcing Facebook’s position in the online advertising market or sub-segments thereof’, and para. 180: ‘The merged entity could start collecting data from WhatsApp users with a view to improving the accuracy of the targeted ads served on Facebook’s social networking platform to WhatsApp users that are also Facebook users.’

26. See M.A. Ruggiero, *Unfair Commercial Practices, Consumer and Internal Market Protection: A Comparative Study*, MA Thesis, 2017, p. 37.

such as Legislative Decree No. 145/2007 (LD 145/07) on misleading and comparative advertisements (business-to-business practice)²⁷ and Legislative Decree No. 146/2007 (LD 146/07) on unfair business to consumer practices (business-to-consumer practice).²⁸ Harmonization of the unfair B2C practices in Italy led to the implementation of LD 146/07 in the Italian Consumer Code (ICC).²⁹ The second chapter of the ICC set out the rules on unfair commercial practices, aiming to ensure adequate protection for consumers.³⁰ What follows from the UCPD implementation in Italy is consumer protection from unfair commercial practices, which is an essential part of the ICC.

Besides the fact that Italy used two different pieces of legislation to clarify consumer protection from unfair practice and unfair competition, the enforcement of both is the responsibility of *Autorità Garante Della Concorrenza e Del Mercato* (AGCM).³¹ Since the AGCM is an independent administrative authority, it has powers to investigate the repression of unfair commercial practices, misleading and unlawful comparative advertising, and the application of conflict of interest's laws to government office holders.³²

The AGCM took different investigations, but different scholars' debates were caused by the Big Data sector investigation from May 2017. The most prominent finding to emerge from this investigation was defining a regulatory framework able to protect privacy and consumers, to foster competition in the markets of the digital economy, and to promote pluralism within the digital economy. However, the most exciting result was that the AGCM took two decisions considering ICC rules on unfair commercial practices and imposed fines on WhatsApp and Facebook.

In addition, *Garante per la Protezione Dei Dati Personali*³³ as an independent administrative authority followed the AGCM, and it imposed a fine for Facebook based on violations of national data protection law attached to the Cambridge Analytica Data Scandal. The fine was set based on the former Italian Privacy Code as the investigation was initiated before the GDPR application. The decision followed the first decision, which prohibited further processing the data related to Italian users by Facebook.³⁴ All in all, Italian case law provides examples that settled either ICC rules on unfair commercial practices or rules on data protection.

The importance of the Italian example of investigations against a dominant market player such as Facebook is a big step for several reasons. Firstly, it presents privacy violations in Italy based on the ICC. Secondly, it is the support for digital activists to strengthen the case against privacy violations in the other EU Member States.

27. For more, see the text of the LD, see AGCM, Legislative Decree no. 145 of 2 August 2007, <https://en.agcm.it/en/about-us/legislation-agcm/detail?id=4eed4de2-6465-40a0-9524-c9dccc7135f7&parent=Consumer%20protection&parentUrl=/en/about-us/legislation-agcm/consumer-protection>.

28. For more, see the text of the LD, *ibid*.

29. Legislative Decree No 146 of 2 August 2007, <https://e-justice.europa.eu/fileDownload.do?id=9eab82ae-7398-4cb0-aa18-a9577845ae57>.

30. It is worth mentioning that the implementation of the UCPD has been completed by Legislative Decree 221/07, which tried to harmonize the text of the ICC with a list of rights guaranteed to the consumers. In particular, the right to have commercial practices with respect to 'good faith, fairness and loyalty' has been introduced at the letter c-bis. Besides, Law No. 27, from March 24th, 2012, extended the protection against unfair practices.

31. Italian Competition and Market Authority.

32. See AGCM, What the authority is, <https://en.agcm.it/en/about-us/>.

33. The Italian Data Protection Authority.

34. More about decision available at *Garante per la Protezione dei Dai Personali*, *Ordinanza ingiunzione nei confronti di Facebook Ireland Ltd e Facebook Italy s.r.l. - 14 giugno 2019* [9121486], www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9121486.

1. The WhatsApp Case

A California-based company, WhatsApp Inc., which is providing services *via* the smart mobile app (for example, WhatsApp Messenger), became part of the Facebook Group. The merger activities between Facebook and WhatsApp caused an investigation by the Italian national authority.

In 2016, the AGCM opened two separate proceedings concerning alleged infringements of the ICC.³⁵ The first enforcement addressed imbalances between users and providers, based on the application of some contractual clauses included in WhatsApp Messenger's Terms of Service (Terms). The AGCM stated that these clauses were unfair. The other enforcement referred to personal data processing. The AGCM's investigation addressed WhatsApp's aggressive conduct in forcing users to accept new Terms. In addition, the acceptance of new Terms meant the automatic transfer of consumers' data to Facebook. In sum, WhatsApp convinced users to believe that without granting consent for personal data sharing, they would no longer be able to use the service. Here it is essential to clarify that the modified Terms were mostly forced on users who already used WhatsApp Messenger. Since users could decide not to give their consent to share with Facebook the information of their WhatsApp accounts and still be able to use WhatsApp, they were unable to accept only part of the WhatsApp's new Terms.

The most interesting aspect was the implementation practice of the new Terms, by which they were implemented while insufficient information was available for consumers. Firstly, an in-app procedure for obtaining the new Term's acceptance was characterized by an excessive emphasis placed on the need to accept the new conditions within the following 30 days or lose the opportunity to use the service at all. Secondly, inadequate information followed the new Terms. Based on that, consumers were without the possibility to deny consent for sharing personal data with Facebook. Finally, acceptance of new Terms led to difficulty in activation of the opt-out option. In line with the AGCM opinion, the nature of the services itself and the importance of WhatsApp as an operator led to inadequate attention to the consequences.

Concerning Articles 20, 24 and 25 ICC, the AGCM found that WhatsApp's conduct constituted an unfair and aggressive commercial practice. The investigation of the AGCM placed several crucial points.

Firstly, the AGCM clarified that the practice at issue did not affect any of the Italian Data Protection Authority competences, which means that the AGCM objected to subject matter jurisdiction.³⁶

Secondly, the AGCM considered Article 27.6 of the ICC, which sets out the requirement for the AGCM to obtain a preliminary opinion from the communications authority (AGCOM).³⁷ Since the WhatsApp's practice referred to electronic communications, the AGCOM issued the statement, in which it argued that Facebook Messenger and WhatsApp hold two of the top three positions in the

35. The first proceeding was about WhatsApp's Terms of Service, and it had started on October 20th, 2016. (Case No. CV154: WhatsApp - Unfair Terms). The second proceeding was about sharing personal data between Facebook and WhatsApp, and it had started on October 27th, 2016. (Case No. PS10601: WhatsApp - Sharing personal data with Facebook).

36. As the AGCM concludes it, the AGCM would suspend its proceedings under Article 27.1bis of the ICC. The cited Article establishes that the AGCM exercises its jurisdiction on unfair commercial practices in regulated sectors upon receiving the competent authority's advisory opinion. However, the same Article did not materialize in this case.

37. Autorità per le Garanzie nelle Comunicazioni.

market for instant messaging. The AGCOM concluded that the use of both smartphones and the Internet facilitate and significantly expand the effects of the commercial practice, strengthening the undue influence on consumers.

Thirdly, an important issue during the investigation was whether the WhatsApp aggressive conduct falls within the ICC scope. WhatsApp's defensive argument was that its main function is to transmit messages between users rather than advertising. Consequently, WhatsApp argued that the transfer of data to Facebook would not constitute a commercial practice in the future. Following this defence argument, the AGCM rejected it by pointing out that the use of data as counter-performance in social media is recognized in the context of both antitrust and consumer protection law. The AGCM also concluded that WhatsApp shared personal data *inter alia* to improve advertising, causing financial growth for Facebook.

Fourthly, WhatsApp argued that there was no harassment, coercion or undue influence, which are elements required under Article 25 of the ICC for an aggressive practice. Following Article 24 of the ICC, WhatsApp argued that new Terms offered users proper notice through an unavoidable full screen informing them about the Terms update. WhatsApp also claimed that two additional informative pages included even a summary of the main changes. On the contrary, the AGCM concluded that the initial screen and the pre-ticked checkbox failed to explain the possibility of refusing the data sharing with Facebook and rendered the concrete exercise of this option impossible. Also, the AGCM concluded that it was possible only to modify user selection through a more complex procedure and that instructions to do it were only available on the second screen. Since WhatsApp offered to consumers only an excessive emphasis placed on the need to accept the new conditions within the following 30 days or lose the opportunity to use the service at all, the AGCM concluded that it caused uncertainty about the continuation of the service.

Finally, considering Article 20 ICC, WhatsApp argued that new Terms exceeded the amount of information provided by other widely used mobile applications, which consumers can reasonably expect from a professional. However, the AGCM considered that WhatsApp, with its 30–50 million users, represents an important player in the relevant national market. In its conclusion, the AGCM stated that WhatsApp's conduct significantly affected the freedom of choice or behaviour of the average consumers, which led to a commercial decision that would not otherwise take place.

For all the reasons mentioned above, the AGCM found that WhatsApp's practice violated Articles 20 (unfair commercial practice), 24 (aggressive commercial practice) and 25 (resort to harassment, coercion or undue influence) of the ICC.

The AGCM qualified the fine concerning Article 27.13 ICC, which stated several factors have to be taken into account to quantify the fine. The first factor was the weight of the infringement, which was serious, given the conclusion of the AGCM (for example, the insidious nature of the extraction of consent to the use of data for profiling and advertising). The second factor was the professional nature of the company, which was that it had the status of a leader in a market. The third factor was the duration of the infringement, which the AGCM found was problematic. As a result, the AGCM imposed the fine in the full amount of €3 million on WhatsApp.

2. The Facebook Case

Cambridge Analytica Ltd (CA), with its seat in London, was a British political consulting firm that combined misappropriation of digital assets, data mining, data brokerage and data analysis with

strategic communication during electoral processes.³⁸ In 2015 it was uncovered that CA collected the personal data of up to 87 million Facebook users³⁹ via the 270,000 Facebook users who used a Facebook app called 'This Is Your Digital Life'. Despite the fact that the majority of users did not explicitly permit CA to access their data, the Facebook app 'This Is Your Digital Life' allowed free access of information on the user's friend's network as well. The most obvious fact here was the breaching Facebook's of terms of service by giving the data to CA. Since the CA collected the personal data of millions of users' Facebook profiles without their consent and used it for political advertising purposes, it was a major political scandal in early 2018. Moreover, the CA scandal has already been described as a crucial moment in the public understanding of personal data and led to calls for more robust regulation for tech companies that are using personal data.

The AGCM opened the investigation in April 2018 and closed it in November 2018.⁴⁰ The investigation followed the supposed violation of the ICC by Facebook Ireland Ltd and its parent company Facebook Inc, which was attached to the CA scandal. At the end of the investigation, the AGCM found that Facebook violated articles 21 and 22 of the ICC. Facebook's misleading conduct led users to register on the Facebook platform, while not adequately and immediately informing them during the creation of the account that the data they provided was for commercial purposes. Besides the fact that Facebook offered the services for free, it did not correctly inform them of the commercial objectives (for example, profitable ends). Consequently, Facebook encouraged users to make a transactional decision that they would not have taken otherwise (namely, to register in the social network and to continue using it). Considering the AGCM opinion, Facebook provided general and incomplete information and did not adequately make a distinction between the use of data to personalize the service and the use of data to carry out advertising campaigns aimed at specific targets.

Further, the AGCM found that Facebook violated Articles 24 and 25 ICC by forcing an aggressive practice. Facebook used the pre-selection of the 'Active Platform' as a function for pre-setting its user's ability to access websites and external apps using their accounts. This Facebook service enabled the transfer of a user's data to single websites and online apps, without any user's consent manifestation. All in all, Facebook used the opt-out pre-selection mechanism concerning data sharing whenever users accessed third-party websites and apps, including games, by using their Facebook accounts. Users could only deselect the pre-setting operated by Facebook without being able to make a free and informed choice.

38. See C. Cadwalladr and E. Graham-Harrison, Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach, *The Guardian* (2018), www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

39. The Guardian's journalist, Harry Davies, was reported in December 2015 for the first time about the CA scandal. He reported that CA was working for the United States Senator Ted Cruz using data harvested from millions of people's Facebook accounts without their consent. However, the scandal finally erupted in March 2018. An ex-CA employee Christopher Wylie had been an anonymous source for an article in 2017 in *The Observer*, headlined 'The Great British Brexit Robbery'. He told the *Observer*: 'We exploited Facebook to harvest millions of people's profiles. And built models to exploit what we knew about them and target their inner demons. That was the basis the entire company was built on.'

40. Press release: AGCM, 'Facebook Fined 10 Million Euros by the ICA for Unfair Commercial Practices for Using its Subscribers' Data for Commercial Purposes', <https://en.agcm.it/en/media/press-releases/2018/12/Facebook-fined-10-million-Euros-by-the-ICA-for-unfair-commercial-practices-for-using-its-subscribers%E2%80%9999-data-for-commercial-purposes>.

Consequently, the users faced a significant restriction on the use of Facebook when they decided to limit their consent. Since Facebook transferred users' data to third parties only for commercial purposes, it caused undue influence on its users. Consequently, Facebook has been fined a full amount of €10 million by the AGCM for misleading users over its data practices.

The most prominent finding to emerge from the Italian example on the WhatsApp and Facebook cases is the enforcement of valid user's consent through the consumer protection agenda. Moreover, Italian case laws are an excellent example of the practical application of the rules on unfair commercial practice.

B. Example of Germany

In Germany, consumer protection is regulated within two systems: statutory rules and self-regulatory codes. One of the self-regulatory codes is the Act Against Unfair Competition (UWG),⁴¹ which is a single statute with common provisions for competitors, consumers and other market participants against unfair acts.⁴² The UWG, which dates back to 1909,⁴³ takes the leading role whenever unfair commercial practice is concerned. The UWG prohibits certain trade practices, which are considered unfair. Through time, the UWG was changing, aiming to modernize German law against unfair competition. Moreover, Germany was notable for successive cases associated with the unfair competition that referred to the CJEU.⁴⁴

German legislators tried to balance the EU ambition to harmonize legislation against unfair commercial practices through the national legal system considering developments in CJEU case law, and the new UWG passed in 2004. The basis of German unfair commercial practice law framed with Article 1 UWG, offers protection for competitors, consumers and public interests in case of the undistorted competition. Article 1 UWG⁴⁵ is the mirror of the UCPD. However, consumer protection is also provided by the general clause stated in Article 3 UWG. Article 3 UWG prohibits 'unfair acts of competition which are liable to have more than an insubstantial impact on competition to the detriment of competitors, consumers or other market participants'. Further, it stipulates threefold criteria: acts of competition, unfairness and more than an insubstantial impact on competition. Since the fair-trading law is covered by both civil and criminal law, the UWG offers some criminal sanctions besides administrative sanctions.

41. Gesetz gegen den unlauteren Wettbewerb.

42. It is worth mentioning that consumer law in Germany is not codified in one comprehensive legislative act, but rather spread over several statutes.

43. UWG was originally mainly concerned with the interests of honest businesses. However, the case law developed by the courts based on Article 1 UWG 1909 took into account the interests of the consumer and the public. Furthermore, Germany introduced the right to sue for consumers' associations in 1965, which meant that UWG directly also protects the (collective) interests of consumers. See R. Podszun, C. Busch and F. Henning-Bodewig, 'Consumer Law in Germany: A Shift to Public Enforcement?', 8 *Journal of European Consumer and Market Law* (2019), p. 75–82.

44. For instance decisions in Case C-315/1992 *Verband Sozialer Wettbewerb e.V. v. Clinique Laboratoires SNC et Estée Lauder Cosmetics GmbH*, EU:C:1994:34; Case C-220/98 *Estée Lauder Cosmetics GmbH & Co OHG v. Lancaster Group GmbH*, EU:C:2000:8; Case C-210/96 *Gut Springenheide GmbH and Rudolf Tusky v. Oberkreisdirektor des Kreises Steinfurt– Amt für Lebensmittelüberwachung*, EU:C:1998:369.

45. See Article 1 of the UWG.

Germany is an example of a state where complaints may be submitted by competitors as well as by consumers.⁴⁶ Considering individual consumer claims regarding unfair terms and conditions and other violations of consumer law, the German Civil Code is the primary basis.⁴⁷ Although Germany has introduced many rules on fair trading, the emphasis is on cases brought by competitors, which is reflected in the case law. Consequently, many of the rules in UWG can be viewed not so much as protecting consumers but rather as controlling competition from competitors. In that regard, literature reviews concluded that the case law in Germany was often to the benefit of a competitor rather than the injured consumer.

Compared to Italy, the enforcement of the UWG is complicated. Firstly, Article 8 UWG defined the role of the Centre for Protection against Unfair Competition,⁴⁸ which aimed to advance trade, industry and commerce in the Federal Republic of Germany. It was the most important institution, which had a formal (that is, judicially authorized) right to initiate legal action against those who infringe laws relating to the UWG. Secondly, Article 13 UWG established the exclusive competence of the District Courts for hearing claims based on the UWG. The jurisdiction lies with the Court in the district where the defendant has his business establishment or place of residence,⁴⁹ or with the Court in the district where the act was carried out.⁵⁰ Thirdly, just as in the provisions of the former UWG, Article 15 UWG defined mediation boards. Finally, the 9th Amendment⁵¹ to the Act against Restraints of Competition (GWB)⁵² in 2017 has empowered the Federal Cartel Office (FCO)⁵³ to carry out sector inquiries for violations of the UWG. The FCO has established a division for consumer protection with the aim of intervention in court proceedings relating to breaches of consumer protection law.

1. The WhatsApp case

Unlike Italy, the merger activities between Facebook and WhatsApp in Germany were first the subject of an order issued by the Hamburg Commissioner for Data Protection and Freedom of Information (HmbBFDI),⁵⁴ followed by the ruling of the district administrative courts. Moreover, the activities of the Federation of Consumer Protection Organizations marked the WhatsApp case in Germany. However, neither the HmbBFDI investigation nor the Federation of Consumer

46. For instance, the German Centre for Protection against Unfair Competition received around 14,000 requests and complaints per year, mostly from competitors or trade associations.

47. If, for example, a no negotiated fee clause is considered unfair and invalid under Article 307 to 309 of Bürgerliches Gesetzbuch (BGB), the consumer has a claim against the business under the rules on unjust enrichment (Article 812 para. 1 BGB). The same is true if an extra fee has been 'agreed' upon via a pre-ticked box in violation of Article 312 a para. 3 sent. 2 BGB. See R. Podszun, C. Busch and F. Henning-Bodewig, 8 *Journal of European Consumer and Market Law* (2019), p. 75–82.

48. See Wettbewerbszentrale, Unser Arbeit, www.wettbewerbszentrale.de/de/institution/profil/auftrag/.

49. Article 14(1) of the UWG.

50. Article 14(2) of the UWG.

51. Under the 9th Amendment to the GWB, which entered into force on 9 June 2017, the FCO has been conferred the competence to launch sector inquiries for consumer protection. Therefore, consumer protection has been given a new impetus in the framework of competition law. Furthermore, the FCO is now entitled to intervene in court proceedings relating to infringements of consumer protection laws.

52. Gesetz gegen Wettbewerbsbeschränkungen.

53. Bundeskartellamt. For more information, see Bundeskartellamt, The Bundeskartellamt, www.bundeskartellamt.de/EN/AboutUs/aboutus_node.html.

54. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit has the mandate to control the administration and the economy in Hamburg with unrestricted access to all data processing companies or authorities or institutions.

Protection Organizations investigation followed the UWG rules. Although the Federation of Consumer Protection Organizations has played an active role in WhatsApp case, the German example on WhatsApp raised just the significance of the national data protection law.⁵⁵ Besides, while the HmbBFDI directed investigation against Facebook, the Federation of Consumer Protection Organizations investigated WhatsApp. Consequently, the German example on the WhatsApp and Facebook merger activates, led to the conclusion that the same company for the same activities has been investigated by different authorities from another corner, whereas appropriate consumer protection is debatable.

Considering the investigation of the HmbBFDI, the conclusion was that Facebook and WhatsApp as independent companies processed users' data based on their Terms. Besides, the HmbBFDI considered that WhatsApp informed users in August 2016 that their data would also be transferred to Facebook without obtaining users' valid consent. Interestingly, the HmbBFDI, just like the Italian AGCM, concluded that new Terms did not give a choice to the users. However, the HmbBFDI considered this practice to be unlawful under national data protection law.

Since the HmbBFDI issued a decision using an administrative order, it ordered the immediate enforcement. In line with the order, Facebook was prohibited from collecting the personal data of WhatsApp users and storing them. However, Facebook has appealed against the order. The legal proceedings were in the jurisdiction of the Administrative Court and the Higher Administrative Court in Hamburg. In the first instance, Facebook appealed intending to repeal the immediate enforcement of HmbBFDI's administrative order. However, the Court rejected a Facebook request based on the fact that there was no legal basis for the planned data transfer. The court of the first instance concluded that the complete data transfer was necessary neither for network security and business analysis nor for advertising optimization. Besides, the court accepted the HmbBFDI conclusion that there was no valid consent from WhatsApp users for data transfer with Facebook. Finally, the court of the first instance considered that the interest of German WhatsApp users was above the economic benefit of Facebook.

One of the questions that were partly open during the first instance of court proceedings was the applicability of national law. However, the Court stated that EU data protection provisions had to be followed, besides Facebook's argument about Irish Law applicability. Consequently, Facebook was under obligation to introduce a lawful consent procedure under previous German data protection law.⁵⁶

The court of the second instance issued its decision based on the carefully analysed process of disclosures made by WhatsApp. Just like the Italian AGCM, the court stated that users accepted new Terms, which included consents to the processing of user information, to continue using the

55. Previous German Federal Data Protection Act (DSGVO) permitted the collection, processing and use of personal data only if a data controller meets certain requirements (the details of which are not relevant here) or if the data subject has consented. Under the BDSG, 'effective consent' must be based on a data subject's 'free decision'. Moreover, the data processors had to inform data subjects of the purpose of collection, processing or use and, insofar as the circumstances of the individual case dictate or upon request, of the consequences of withholding consent. The DSGVO stipulated that 'if consent is to be given together with other written declarations, it shall be made distinguishable in its appearance'. Considering that the GDPR entered into force after the decision in Germany, it should be noted that it contains similar requirements. Controllers may process data only based on at least one of the conditions defined in Article 6(1), one of which is obtaining user consent. Besides, consent is defined in Article 4(11) as any 'freely given, specific, informed, and unambiguous indication of the data subject's wishes'.

56. Article 4 (11) of DSGVO.

service. However, the court found that WhatsApp did not provide its users with the opportunity to give valid consent to the data processing as required under national data protection law. Just like the Italian AGCM, the court explained that WhatsApp users were not adequately informed about the circumstances under which they consented to the processing of their data and the consequences of their decisions.

The HmbBFDI filed the complaint to the CJEU, considering Article 77 GDPR in May 2018.⁵⁷ Regarding the complaint, WhatsApp ‘used a privacy policy and terms of service, which the data subject had to agree. If this privacy policy must be read on the screen of a mobile phone, it takes 89 screen pages to read the whole text’, which means that new privacy policy was ‘an aggressive and absurd attempt to deprive data subjects of their rights guaranteed by the GDPR’. The merger activities between Facebook and WhatsApp happened before the GDPR was officially applicable in the CJEU. Consequently, the HmbBFDI requested retroactive application of the GDPR. The basis for retroactive application of the GDPR according to the HmbBFDI was Recital 71. It clarified that the controller might establish processing operations on the consent obtained before 25 May 2018, with proof that such consent followed the GDPR requirements. Finally, the HmbBFDI requested issuing the fine under Article 83(5)(a), which would be about €1.3 billion (4% of the worldwide revenue). However, the CJEU has not still settled the case.

Although the decisions issued in Germany had a similar conclusion to the AGCM in Italy, they did not follow the rules on unfair commercial practice from the UWG. All in all, the decisions made under German data protection law provided helpful guidance on valid consent, but only under the data protection law.

In addition, the WhatsApp case was looked at by the Federation of German Consumer Organizations,⁵⁸ which has initiated two different investigations referring to WhatsApp.

The first investigation related to the WhatsApp Terms, which were in English.⁵⁹ The Court of Appeal Berlin issued a judgment against WhatsApp, prohibiting WhatsApp’s use of English Terms on its website for contracts with users in Germany unless the Terms are available in the German language. In line with the court’s opinion, a complex set of contractual Terms available only in the English language led to the conclusion that the whole set of contractual Terms should be deemed void because of a German Civil Code breach.⁶⁰ The court considered that consumers could not expect the Terms in the English language since the whole website was offered in the German language. Finally, the court concluded that all clauses of WhatsApp’s Terms should be invalid and unenforceable because they were in English.

The second investigation related to merger activities between Facebook and WhatsApp. The Federation of German Consumer Organizations shown activities in the very early beginning after new WhatsApp Terms entered into force. Firstly, it was issued the order, which aimed a range of issues, including the transfer of data to Facebook. Although the Federation of German Consumer Organizations considered collecting and sharing data to be illegal based on national data protection law, WhatsApp did not follow the order. Consequently, the Federation of German Consumers Organizations filed a complaint against WhatsApp before the court of the first instance in Berlin.

57. For more information about the complaint, see Noyb, <https://noyb.eu/en/>.

58. For more information, see www.vzbv.de/.

59. Press release: VZBV, 17 May 2016, ‘WhatsApp muss AGB auf Deutsch bereitstellen’, www.vzbv.de/pressemitteilung/whatsapp-muss-agb-auf-deutsch-bereitstellen.

60. Article 307(1) BGB.

Just as with the AGCM and the HmbBFDI, the Federation of German Consumer Organizations believed that the changes to the Terms meant acting against the law. Moreover, the Federation of German Consumers Organizations argued that collected user data should not be shared with Facebook, even though the users concerned have a Facebook account. Finally, the main request of the complaint was that data shared with Facebook should be deleted, along with a further ban on transfers of such data. Although the case has still not been settled by the Berlin court of the first instance, it is not reasonable to expect other consequences similar to those in the case launched by HmbBFDI. Perhaps the Federation of German Consumer Organizations' activities would be more appropriate if the complaints were legally based on rules on unfair commercial practice.

2. The Facebook Case

In March 2016, the FCO considering German competition law formally initiated proceedings against Facebook based on the suspicion that the social network was abusing its market power by violating data protection rules. Further, the FCO in 2017 published a detailed preliminary assessment and background information to the proceedings. Following an investigation of Facebook into the abuse of a dominant position, the FCO issued the final decision in 2019.⁶¹ The ruling of the FCO was prohibiting Facebook Inc., Menlo Park, USA, Facebook Ireland Ltd., Dublin, Ireland and Facebook Germany GmbH, Hamburg, Germany (Facebook) from processing user data from different sources without the user's consent.⁶² Interestingly, the FCO based the prohibition on Article 19(1) of the GWB, although the decision accepted the enforcement of data protection based on the UWG. A possible explanation might be that the FCO considered data protection regulations, which do not suspend abuse control. In line with the FCO opinion, the GDPR does not explicitly state that its provisions are final, so it could not be assumed that the GDPR leaves no further scope for examination by other authorities and under different aspects. Consequently, the FCO has found the place for applicability of Article 19 (1) GWB in the Facebook case.

Comparing to the Facebook case in Italy, it might be concluded that the FCO investigation was a bit different. The FCO investigation considered the way of sharing personal data made by platforms associated with the Facebook Business Tools (for example, Facebook's subsidiaries – WhatsApp and Instagram). The investigation covered several issues.

Firstly, the FCO examined whether the Facebook data policy was appropriate based on the data protection offered by the GDPR. In that regard, the FCO concluded that Facebook's processing of personal data from other corporate services and Facebook Business Tools enabled profiling and device fingerprinting. Based on such processing of personal data, Facebook violated the requirements defined in the GDPR. Facebook did not provide valid consent concerning Article 6(1)(a)⁶³ of the GDPR, affecting users' consent under data protection requirements. In the opinion of the FCO, data processing to the third party is not justified without the user's voluntary consent. Moreover, the FCO found that voluntary consent for the processing of the user information could not be assumed if a user's consent was a prerequisite for using Facebook's service in the first place.

61. FCO, Case B6-22/16, a decision from 7 February 2019.

62. The decision is available at Bundeskartellamt, Decision of Facebook-proceeding, (2019), www.bundeskartellamt.de/SharedDocs/Meldung/EN/AktuelleMeldungen/2019/11_07_2019_decisionFacebook.html.

63. As stated in Article 6(1)(a), processing shall be lawful if the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

Secondly, the FCO examined Facebook's market power. As stated in the FCO opinion, the violation of data protection requirements was a manifestation of Facebook's market power. The basis for such opinion the FCO found in case law, which showed that the conduct (that is, the violation) was only possible in the first place because of market dominance and that other market participants did not have a chance to behave similarly. In the opinion of the FCO, Facebook, with its dominant position, prevented users from protecting their data from being processed from a large number of sources (that is, they did not have the possibility to decide autonomously on the disclosure of their data). Further, an essential element of the market power was the strong direct network effects of Facebook's business model and the difficulties associated with switching to another social network.

Thirdly, the FCO found that Facebook data policy was abusive concerning the Article 19 (1) GWB since it allowed Facebook to collect user- and device-related data from outside Facebook and merge it with data collected on Facebook.

Finally, the FCO considered that Facebook is the dominant company in the German market for users as regards Article 18(1)(3) and (3a) GWB, as Facebook has a scope of action in the German national market. Consequently, it is not sufficiently controlled by competition law.

Considering all investigated issues, the FCO has prohibited the data processing policy Facebook imposes on its users and its corresponding implementation concerning Article 19(1) GWB and ordered the termination of this conduct. In addition, the FCO decision contained the prohibition relating to Terms of personal data processing.⁶⁴ Considering the end of the violations, the FCO required in its decision that Facebook implement the necessary changes and adapt its data and cookie policies within 12 months. Facebook was given an additional deadline of four months to present an implementation road map for the adjustments.

Facebook appealed against this decision to the Düsseldorf Higher Regional Court with the aim of delaying the application of the order. The Düsseldorf Higher Regional Court settled the case very fast by issuing a decision in August 2019.⁶⁵ Interestingly, the court made a different decision to the FCO with respect to crucial legal issues. Firstly, the court did not accept the FCO's opinion about a possible violation of privacy rules which automatically violated competition rules. Secondly, the Court decided that users autonomously decide whether they agree with Facebook's Terms when signing up for the service. In addition, the court did not agree that Facebook's data collection exploits users since they could continue to make the same data available to other companies. In that respect, the court did not find that Facebook is using a dominant position when it comes to data processing. Considering the ruling of the court, Facebook does not have to implement the decision of the FCO. Of course, the FCO appealed against Düsseldorf Higher Regional Court decision to the Federal Court of Justice. However, the case before Federal Court Justice has still not been settled.

The FCO's ruling provides an impressive legal novelty based on a combination of the data protection law rules and competition law rules. However, it represents a stretch to some extent. All

64. The Facebook Terms expressly stated that they involve the collection of user- and device-related data from other corporate services and Facebook Business Tools without the user's consent and their combination with Facebook data for purposes related to the social network. The FCO also prohibited the implementation of these terms and conditions in actual data processing procedures, which Facebook performs based on its data and cookie policies.

65. The decision is available at CPI, Germany: Facebook Succeeds in Blocking German Ban on Data Collection, (2019) www.competitionpolicyinternational.com/germany-cartel-office-to-take-facebook-case-to-high-court/.

in all, the Federal Court of Justice, with its decision, will answer whether the FCO ruling could prove to be very helpful for private users or not.

Besides the FCO investigation, in 2018, HmbBFDI announced that the investigation against Facebook is open concerning data abuse on the Facebook platform. In line with the Hamburg Data Protection Officer's opinion, Facebook could face a fine of up to €300,000, but only in a case where German users' data are breached.⁶⁶ Despite the announcement, this investigation still has no further step.

The Federation of Consumer Protection Organizations filed the complaint against Facebook for violation of the GDPR's request on informed consent with its privacy settings and some of its Terms. The ruling of the first and second court's instances were following the case.⁶⁷

Although the Federation of the Consumer Protection Organization argued that the advertising quote, such as 'Facebook is and remains free', was misleading, the court of the second instance did not conclude the same. In the opinion of the court, the advertising quote only referred to the fact that the services could be used without cash payments or other loss of assets. Interestingly, one of Facebook's arguments during the court proceedings was that the rules on unfair commercial practice were applicable. However, this was rejected by the courts of the second instance with the explanations that it was without importance, considering that the users were affected by missed effective consent for the use of personal data. The court of the second instance also prohibited several points in Facebook's Terms: firstly, the user's agreement to the use of the user's name and profile picture for commercial, sponsored, or related content; and secondly, the clause about the user's agreement in advance to all future changes to the Facebook data privacy policy. Following the court's opinion, such pre-formulated declarations did not meet the requirements for valid consent to the use of personal data defined in the GDPR. Finally, a clause that required users to provide their real name, among other things, was already legally prohibited in Germany.

The most prominent finding to emerge from this ruling is the importance of the German consumer protection in the enforcement of effective consumer consent through the data protection law. The decision of the Berlin court has enthroned the authority for German consumer protection authorities to take legal action in the event of the GDPR's violations. Consequently, the mentioned decision is not an example of effectively applied rules on unfair commercial practice when it comes to data processing. All in all, the Facebook example in Germany suggests that the Federation of Consumer Protection Organizations was more successful than the FCO.

C. Example of the UK

The United Kingdom is often seen as the Member State with the strongest self-regulation tradition in this area. Similar to Germany's legislators, the UK's legislators regulated consumer protection against unfair commercial practices through a self-regulatory code.

The CPR, as a single statute, came into force on May 26th, 2008. Since the CPR was a new unique corpus of legislation, it fully implemented the UCPD into UK law. A possible explanation for new single statutes on unfair commercial practice might be that before the UCPD, the UK legislative framework did not have any unique corpus of legislation for fighting against unfair

66. See DW, Facebook Could Face Fine if German Users Affected by Cambridge Analytica Data Breach, (2018), www.dw.com/en/facebook-could-face-fine-if-german-users-affected-by-cambridge-analytica-data-breach/a-43476184/.

67. Press release, available at Verbraucherzentrale Bundesverband, Facebook verstößt gegen Datenschutzrecht, (2020), www.vzbv.de/pressemitteilung/facebook-verstoest-gegen-datenschutzrecht.

practices. Considering that the UK legal background is different from the majority of the EU countries, different pieces of legislation were regulated based on precedent case law, but without specific sanctions aimed at better enforcement of consumers' rights. Although the CPR is the mirror of the UCPD, it also extended the scope to situations where a consumer sells goods to trade. However, the prohibitions defended within the CPR are the same as the UCPD's rules, and the CPR offers a three-tier division. Consequently, it consists of three prohibitions: a general ban on unfair commercial practices; prohibitions on misleading and aggressive practices; and 31 practices prohibited in all circumstances. The CPR is divided into three parts. The first part of the CPR contains the definition of essential notions, such as the average consumer, commercial practice, goods and invitation to purchase. The second part of the CPR is dedicated to the prohibition of unfair practices, with a scheme and wording that follow the European implementation. Finally, the last part of the CPR comprises 31 prohibited commercial practices, which are unfair in all circumstances. In addition, in the UK, another essential piece of law for defending consumers against unfair practices was adopted in 2014.⁶⁸

Just as in Germany, the UK is an example of a state where civil or criminal enforcement complaints are allowed. The UK's enforcers promote compliance by the most appropriate means, in line with their enforcement policies and priorities, consistent with available resources. In line with scholars' opinions, the UK is an example of a country which offers public enforcement of the UCPD's rules based on the implementation of consumer protection by criminal law. By contrast, Germany is an example of a country which employs private enforcement because, in practice, the private party's complaints result. However, in the UK, complaints can be submitted by consumers.

CPR sets out the obligation for enforcement for Local Authority Trading Standards Services (TSS), the Department of Enterprise, Trade and Investment in Northern Ireland and the Office for Fair Trading (OFT). However, as part of the UK Government's reforms to the arrangements for competition, consumer protection and consumer credit regulation, the OFT was closed on 31 March 2014. Its work and responsibilities passed to several different bodies. Consequently, the Competition and Markets Authority (CMA) has taken on the competition and certain consumer functions of the OFT. In addition, the CMA mostly promotes competition, within and outside the UK, for the benefit of consumers. Also, the Department of Enterprise, Trade and Investment (Northern Ireland) has been replaced by the Department for the Economy (Northern Ireland).

There are some activities which are aimed at consumer protection on online platforms, which is considered part of the role of the CMA. In 2019, the CMA published an update on online platforms and a digital advertising market study, including concerns and potential interventions.⁶⁹ The study refers to a summary of research on consumers' attitudes and behaviour on online platforms. The study brought together the most relevant academic literature and consumer survey material. The study's Appendix G aims to identify where there might be gaps in the evidence base and where further research would be useful when it comes to consumer data processing. Based on the central issues (for example, consumers' awareness of the value of data to platforms, consumers' feelings of data control and consumers' attitudes towards data processing), Appendix G debates the issue of whether consumers' awareness is an essential element for better consumer protection on online

68. CPAR (the Consumer Protection (Amendment) Regulations 2014), www.legislation.gov.uk/uksi/2014/870/regulation/3/made, which introduced the right for consumers to redress.

69. For more information, see Gov.uk, Online Platforms and Digital Advertising Market Study, (2019), www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study.

platforms. In line with Appendix G, consumer information should be regarded more as a process rather than a one-off act. The focus should be more on emphasizing the specific harmful effects that may emerge from the collection and analysis of personal data. Consequently, such a focus could help to raise awareness among consumers and could increase motivation to engage with the terms and conditions of online platforms.⁷⁰ Besides, Appendix G has stated that, considering some evidence, better protection of consumers requires more regulations for online platforms.⁷¹

In the end, it is recognised that there is a very active role in upholding information rights in the public interest for the UK Information Commissioner's Office (ICO).

1. WhatsApp case

WhatsApp was the subject matter of an investigation in the UK. The UK ICO conducted the investigation.⁷² The investigation on WhatsApp began in August 2016, and during the investigation, the ICO found several essential facts. Firstly, WhatsApp has not identified a lawful basis of processing for any such sharing of personal data. Secondly, WhatsApp has failed to provide users with adequate, fair processing information concerning any such sharing of personal data. Finally, concerning existing users, such sharing would involve the processing of personal data for a purpose that is incompatible with the primary purpose of collecting such data.

The ICO settled the case in March 2018. The investigation finished with a formal decision by the ICO, obliging WhatsApp not to share personal data with Facebook until data protection concerns were addressed. Interestingly, the ICO's decision was the reason for the signed public commitment by WhatsApp. However, the ICO found that there were no criteria for issuing a monetary fine since WhatsApp convinced the ICO that no UK user data was shared with Facebook. Considering that the WhatsApp case in the UK followed the rules of the UK Data Protection Act, WhatsApp was obligated, from the date of the decision, not to share personal data with Facebook, until it could satisfy the requirements of the GDPR.

Unlike in Italy and Germany, where the investigation against WhatsApp is based on unlawful data processing, the direction of the UK's investigation depended on whether WhatsApp legally shared users' data with Facebook. In the end, the ICO concluded that the UK Data Protection Act did not prevent a company from sharing personal data since it only had to follow the legal requirements. In that respect, the ICO's investigation did not concern WhatsApp's sharing of personal data with Facebook when Facebook was only providing a support service to WhatsApp. In line with the FCO decision, WhatsApp used Facebook as a data processor.

Interestingly, the ICO concluded that in the UK there was no need for consumers to take any further actions against WhatsApp. Consequently, it did not initiate any further investigation of the WhatsApp case in 2018. However, a new investigation in 2019 into WhatsApp has been opened based on serious security vulnerability on the WhatsApp platform.⁷³ The ICO announced that two agencies dealing with the incident: the National Cyber Security Centre (NCSC) on behalf of the

70. Point 289 of Appendix G.

71. Point 295 of Appendix G.

72. For more information, with enclosed ICO letter and decision, see Wiredgov, A Win for the Data Protection of UK Consumers – WhatsApp Signs Public Commitment not to Share Personal Data with Facebook Until Data Protection Concerns are Addressed, (2018), www.wired-gov.net/wg/news.nsf/articles/A+win+for+the+data+protection+of+UK+consumers+%E2%80%93+WhatsApp+signs+public+commitment+not+to+share+personal+data+with+Facebook+until+data+protection+concerns+are+addressed+15032018112000?open.

73. For more information, see ICO, Your Data Matters Blog, <https://ico.org.uk/your-data-matters/your-data-matters-blog/>.

UK consumers and the Irish Data Protection Commission (IDPC) as the lead authority for WhatsApp under the GDPR. Although the new investigation relates to the GDPR, the most obvious conclusion to emerge from a recent investigation into WhatsApp is a combination of the consumer and data protection law in the UK. Since the investigation is not over, there is no conclusion as to whether there are breaches of consumer protection law.

2. Facebook case

Just as in WhatsApp case, the ICO was the authority in the UK that opened the investigation against Facebook.⁷⁴ The ICO has placed Facebook's behaviour as an indirect influence on political choice and found it to be priority in the protection of democracy through data protection law instead of consumer protection. The activities of the ICO might be understood as a logical consequence, considering that the ICO launched the investigation about the use of personal data analytics solely for political purposes. Consequently, the investigation examined the transparent processing of users' data and the micro-targeting of political adverts during the referendum for Brexit and the 2016 American Presidential election process. Although the ICO investigation considered criminal issues, the ICO concluded that Facebook failed to comply with the national data protection law properly.⁷⁵

In addition, this investigation in the UK became the most extensive investigation, since it included not only Facebook but data brokers, analytics firms, academic institutions, political parties and campaign groups. The cornerstone for the ICO investigation was the link between Cambridge Analytica, its parent company SCL Elections Limited and Aggregate IQ, and it involved accusations regarding the collection of data from Facebook. The ICO's final findings resulted in a fine for Facebook of £500,000 for lack of transparency and security issues relating to the collection of data. Following the ICO's investigation, the fine it issued to Facebook was the maximum allowable under the national data protection law, which was applicable when the Cambridge Analytica scandal happened.

Summarizing the ICO's investigation, it concluded that between 2007 and 2014 Facebook processed the personal data of users unfairly by allowing developers access to their data through the Facebook Business Tool App without sufficiently clear and informed consent. In addition, Facebook allowed access to personal data, although some users did not download the Facebook Business Tool App but were simply 'friends' with people who downloaded it. Besides, Facebook also failed to keep personal information secure because it was unable to make appropriate checks on the Facebook Business Tool App while developers were using the Facebook platform. Further, the ICO found that Facebook Business Tool App collected up to 87 million pieces of data from the users, and at least one million were data of the UK users. According to the ICO's findings, Facebook Business Tool App was developed by Dr Aleksandr Kogan and his company GSR. The reason for the scandal was the fact that the collected data were shared with other organizations, including SCL Group, the parent company of Cambridge Analytica. The collected data involved the political campaigning in the US. However, another problem was the fact that Facebook users worldwide were not aware of the collection of their data from Facebook for political purposes. Based on all findings during the investigation, the ICO decided on fines against Facebook.

74. For more information, see ICO, Investigation into Data Analytics for Political Purposes, <https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/>.

75. Article 4(1) and (7) of the Data Protection Act 1998.


On 21 November 2018, Facebook filed an appeal against the ICO decision. The court of the first instance issued a decision on 14 June 2019. The court conclusion referred to procedural fairness and allegations of bias on the part of the ICO, and said that the ICO should be required to disclose materials relating to its decision regarding the fine. Following this court's decision, the ICO appealed on 2 September 2019. However, an agreement was reached between the ICO and Facebook. Consequently, Facebook and the ICO agreed to withdraw their appeals. Moreover, Facebook decided to pay the £500,000 fine, and each party should bear its legal costs of the proceedings. In the end, the agreement enables Facebook to retain documents disclosed by the ICO during the appeal for other purposes.

5. Concluding remarks

The purpose of this study was to determine how national bodies in Italy, Germany and the UK solved cases on WhatsApp and Facebook relating to personal data processing. The research showed that Italy could be an example of the Member State which effectively applied the rules on unfair commercial practice regarding personal data processing. While the example of Italy showed that the UCPD's rules are applicable, the case law in Germany showed that data protection law and competition law have a priority over the rules on unfair commercial practice. Also, examples in the UK showed that data protection law is the leader when it comes to personal data processing. The result of the Italian investigation into some of the most popular online platforms highlighted the need and the challenge of enforcing key pieces of legislation better. The supporting argument for the Italian experience is also a growing body of literature. Considering literature, the application of the UCPD's rules can potentially mitigate the effects of personalization and can support the ex-post protections provided in the GDPR by focusing on the effects on the decision-making capacity of the average consumer.

In the end, the debate regarding the economic value of personal data is wide-ranging. On one side, the European Data Protection Supervisor (EDPS) refused to accept the qualification of personal data as a mere economic asset or as a counter-performance to a contract. On the other side, the EU Commission in WhatsApp and Facebook merger activities accepted that data have relevant economic value. The view of the EU Commission provided light for Italian authority. Consequently, the Italian authority took data as tangible goods, and as a result it applied rules on unfair commercial practice. All in all, personal data are often sold to third parties, and de facto has economic value. Therefore, it is reasonable to assume that data-driven businesses engaging in B2C transactions should always fall under the scope of the UCPD rules.

ORCID iD

Maja Nišević  <https://orcid.org/0000-0002-5254-4267>

Author biography

Maja Nišević is employed as Researcher at the University of Verona, and she is doing her PhD studies at the University of Verona.