Paying with Personal Data

Delforge, Antoine

Published in:
Deep diving into data protection

Publication date:
2021

Document Version
Publisher's PDF, also known as Version of record

Paying with Personal Data: Between Consumer and Data Protection Law

Antoine DELFORGE[1]

Introduction

Since the advent of the information society, many companies (such as Facebook, Google, etc.) offer services that are presented as "free of charge".[2]

This notion of "free services" must be well understood. Indeed, these companies have developed a business model based on the commercial exploitation of their users' personal data. The processing of their personal data thus enables them to finance their services by reusing these data, most often to offer targeted advertising. From an economic point of view, in return for the service they want to access, users accept that their personal data be used to finance the service (targeted advertising, monitoring of consumption habits, etc.).[3]

---

[1] University of Namur, Faculty of Law, CRIDS. This contribution is inspired by a study carried out for the Digital Clearing House in June 2019, cowritten with A. DE STREEL and I. GRAEF. We thank them for their inputs in our reflections.

[2] 'It's free and it always will be', a slogan that has long been present on the Facebook homepage. However, this slogan was considered misleading and did not reflect the commercial nature of Facebook's collection of personal data (e.g. see Autorita Garante della Concorrenza e del Mercato, Decision of 29 November 2018 against Facebook, 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'-data-for-commercial-purposes). Following a discussion with the European Commission about its General Terms, it has now been replaced in Europe by 'it's easy and quick' (http://europa.eu/rapid/press-release_IP-19-2048_en.htm).

[3] J. NEWMAN, 'The Myth of free', *George Washington Law Review*, 2017, vol. 86, available at https://ssrn.com/abstract=2827277; A. ESTEVE, 'The business of personal data: Google, Facebook, and privacy issues in the EU and the USA', *International Data Privacy Law*, 2017, vol. 7, pp. 36-47, available at https://doi.org/10.1093/idpl/ipw026. For an explanation of M. ZUCKERBERG on the Facebook model, see 'Understanding Facebook's Business Model', 2018, available at https://newsroom.fb.com/news/2019/01/understanding-facebooks-business-model.

It is now even possible, in the United States, to buy a coffee in exchange for providing some personal data (surname, first name, email address, centres of interest…).[4]

Facebook and Google are not the only ones to finance their "free service" in this way. Some press websites do the same. This model is so common that some people fear the disappearance of many "free" online media should the legislation on the use of "cookies" be tightened as a consequence of the revision of the ePrivacy Directive.[5]

In this contribution, we will analyse if it is legal in EU data protection and consumer laws to provide personal data in exchange of the access to service. If the applicability of data protection law to this kind of service is quite obvious, it is less so for the applicability of consumer law. We will therefore review the applicability of the main consumer law Directives, before analysing the transparency obligation of the service provider about the commercial reuse of personal data provided by its customers. We will then discuss the possibility to ground this processing of personal data on the different legal bases of the General Data Protection Regulation[6] and examine the right of the consumer to terminate the contract. Finally, we will study how data protection and consumer law approach the assessing of the fairness of the contractual relationships between the service provider and its client.

[4] K. Burgess, 'Café offers free latte at the price of your personal data', 2019, https://www.thetimes.co.uk/article/shiru-cafe-free-latte-comes-at-the-price-of-your-personal-data-xgp6mtwdh.

[5] Report of the General Council of French Economy on the 'Access to data, consent, impact e-privacy Regulation' (in French), available at https://www.economie.gouv.fr/files/files/directions_services/cge/Rapports/CGE_R2017-17_e-privacy.pdf, p. 42. On this topic of cookies and the ePrivacy Regulation, see EDPS, Recommendations on specific aspects of the proposed ePrivacy Regulation, 5 October 2017; EDPB, Statement 3/2019 on an ePrivacy regulation, 13 March 2019; F. Zuiderveen Borgesius, S. Kruikemeier, S. Boerman, and N. Helberger, 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation', *EDPLR*, vol. 3, 2017, pp. 353-369; A. Delforge, 'Le placement de "cookies" sur un site web : la Cour de Justice fait le point, l'APD commence à sanctionner', *R.D.T.I.*, 2020, pp. 101-112.

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

1. Applicability of EU Consumer Law

The applicability of consumer law to non-monetary business model[7] is a difficult issue because the counter-performance is not always clearly defined and understood. This is even more complicated as the EU consumer acquis is made of several Directives with different application criteria which, in addition, are often transposed with differences across the Member States. The EU Consumer acquis, which is particularly relevant for non-monetary price services, is based of the following Directives:

– Digital Content Directive[8], hereinafter DCD,
– Consumer Rights Directive[9], hereinafter CRD,
– Unfair Contract Terms Directive[10], hereinafter UCTD;
– Unfair Commercial Practices Directive[11], hereinafter UCPD.[12]

The DCD and CRD aim at harmonising the pre-contractual information requirements and the right of withdrawal. The UCTD and UCPD prohibit unfair terms or commercial practices in consumer contracts.

The applicability of some of these Directives to non-monetary price services has raised some issues as counter-performance is not a monetary price but something else, most of the time the consumers' consent to the collection and processing of their personal data. This issue is now settled

[7] We prefer to use the term of 'non-monetary price service' rather than 'free service'. The term 'non-monetary price service' will be used in this contribution to define a service which is not provided in exchange for a monetary price, but in exchange for the user's consent to provide personal data that could be reused to fund the service.

[8] Directive 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, OJ 2019, L 136, pp. 1-27.

[9] Directive 2011/83 of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ 2011, L 304, pp. 64-84.

[10] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ 95, L 95, pp. 29-34.

[11] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, OJ 2005, L 149, pp. 22-39.

[12] In addition, there is Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers, OJ 98, L 80, pp. 27-31. However, this Directive only applies to products; and non-monetary price services almost always concern online services, therefore falling outside of the scope of this Directive.

with the recent adoption of the DCD, which specifies that it applies to contracts where the trader supplies digital services and the consumer pays a price or provides personal data.[13] For example, the DCD applies to social media requiring that consumers consent to provide their personal data for purposes other than solely supplying the service.[14]

However, the possibility to pay with personal data and considering personal data as a mere currency may conflict with data protection rules that link personal data to fundamental rights protection. Indeed, the European Data Protection Supervisor (EDPS) warned that the fundamental rights nature of the protection of personal data goes against the idea of personal data as a "simple consumer interest" or a "mere commodity".[15] This is why the term "data as counter-performance" proposed by the Commission has been removed from the agreed text and the Directive clarifies that personal data should be collected and processed in accordance with EU data protection rules and, in case of conflict between those rules and the DCD, the former should prevail.[16]

The scope of the CRD has also recently been amended with the "Better enforcement and modernisation of EU consumer protection rules" Directive to be aligned with the scope of the DCD.[17] Thus, the CRD now also applies to contracts under which the trader supplies a digital service to consumers and consumers provide their personal data.[18]

However, the DCD and CRD do not apply to online services where there is no contract under national law between the trader and the user. That may be the case when a consumer only scrolls a webpage and their personal data (browsing history for example) are collected or they are exposed to advertising.[19] The recital containing this exception is not clear

[13] Art. 3(1) DCD.

[14] Recital 24 DCD.

[15] EDPS, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, p. 3.

[16] Recital 37 and art. 3(8) DCD.

[17] Recitals 32, 33, 34 of the Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, OJ L 328, hereafter "'Better enforcement and modernisation of EU consumer protection rules' Directive".

[18] Art. 1(a) CRD as amended by the 'Better enforcement and modernisation of EU consumer protection rules' Directive.

[19] Recitals 25 DCD. Recital 35 'Better enforcement and modernisation of EU consumer protection rules' Directive: CRD 'should also not apply to situations where the trader only collects metadata, such as information concerning the consumer's device or the browsing history, except where this situation is considered a contract under national law. It should also not apply to situations where the consumer, without having concluded a contract with the

on whether the collection of personal data for the purpose of providing targeted advertising to the user is covered by the DCD and CRD. Moreover, the draft ePrivacy Regulation[20] requires the consent of the webpage user to place cookies on their computer if these cookies are used to profile the user or expose them to target advertising.[21] This consent could be considered as a *contract* given that the purpose of the collection of this personal data should be explained to the user before they consent.

Finally, the DCD and the CRD do not apply to services provided in exchange for non-personal data.[22]

The applicability of the UCTD and the UCPD to non-monetary price services is now clearly recognised by national jurisdictions and enforcement authorities.[23] Indeed, these two Directives apply to the relationship between consumers and professionals who act for purposes relating to their trade.[24] For example, the *Tribunal de première instance* of Paris justi-

trader, is exposed to advertisements exclusively in order to gain access to digital content or a digital service. However, Member States should remain free to extend the application of the rules of Directive 2011/83/EU to such situations or to otherwise regulate such situations which are excluded from the scope of that Directive'.

[20] The ePrivacy Directive is currently under revision (no provisional agreement). So, we based our study on the last version (10 february 2021) of the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (hereinafter 'Draft ePrivacy Regulation').

[21] Articles 6 and following, and Recitals 18 and 21aa Draft ePrivacy Regulation.

[22] In the Commission proposal, DCD also applies to service for which the consumer 'provides counter-performance other than money in the form of personal data or any other data' (art. 3.1). It has been removed.

[23] Recent case law: TGI Paris, 9 April 2019, available at https://www.quechoisir.org/action-ufc-que-choisir-donnees-personnelles-l-ufc-que-choisir-obtient-la-condamnation-de-facebook-n65523/?dl=44179; TGI Paris, 12 February 2019, available at https://www.quechoisir.org/action-ufc-que-choisir-donnees-personnelles-l-ufc-que-choisir-obtient-la-condamnation-de-google-n63567/; Decision of the Autorita Garante della Concorrenza e del Mercato against Facebook, 29 November 2018, press release available at 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'-data-for-commercial-purposes; Berlin Landgericht, 12 February 2018, VzBv/Facebook. See VzBv's press release available at https://www.vzbv.de/sites/default/files/downloads/2018/02/14/18-02-12_vzbv_pm_facebook-urteil_en.pdf. See also the decisions listed and explained by N. Helberger et al., 'The Perfect Match? A Closer Look at the Relationship between EU Consumer law and Data protection Law', *Common Market Law Review 2017*, vol. 54, n° 5, available at https://ssrn.com/abstract=3048844, pp. 17-18, and N. Zingales, 'Between a Rock and Two Hard Places: WhatsApp at the Crossroad of Competition, Data protection and Consumer law', *Computer Law and Security Review 2017*, available at https://ssrn.com/abstract=2990939.

[24] Art. 2 (1) UCTD. Same idea for UCPD. It applies to '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 a product to consumers' (art. 2(1)(d)).

fies the application of the UCTD to the Facebook business model for the reason that the monetisation (via target advertising…) of the collected personal data from Facebook users must be considered as an "advantage" within the meaning of the French Civil Code. The contract is therefore a commercial contract between a consumer and a supplier acting for professional purposes.[25] The Italian Competition Authority (AGCM) also stated that the collection of Facebook users' personal data for target marketing (a commercial use) has an economic value and that it is therefore enough to consider the relation between Facebook and its users as a commercial relationship between a "professional" and a "consumer" even in the absence of any formal monetary consideration.[26] In this respect, the AGCM relied in particular on the Commission Guidance on the application of the UCPD which considers a platform drawing revenues from targeted advertising as a "trader".[27]

2. Transparency Obligation About the Commercial Reuse of Personal Data

Both consumer law and data protection aim at achieving a high level of consumer/data subject protection by regulating the relationship between a trader (also a data controller) and its customer (also the data subject) in order to compensate the information and power asymmetry between both parties.[28] Regarding non-monetary price services, the main transparency issue is about the commercial reuse of the data provided by the customer in exchange for the access to this service. This commercial reuse of the personal data could be seen as the "price" paid by the user of these services.

[25] TGI Paris, 9 April 2019, available at https://www.quechoisir.org/action-ufc-que-choisir-donnees-personnelles-l-ufc-que-choisir-obtient-la-condamnation-de-facebook-n65523/?dl=44179, pp. 11-13.

[26] Free translation of the Decision of the Autorita Garante della Concorrenza e del Mercato against Facebook, 29 November 2018, available at https://www.agcm.it/dotcmsdoc/allegati-news/PS11112_scorr_sanz.pdf.

[27] Commission staff working document, Guidance on the implementation/application of directive 2005/29/EC on unfair commercial practices, 2016, p. 122.

[28] N. Helberger, 'Form matters: Informing consumers effectively', *Amsterdam Law School Research Paper* (2013) no. 2013-71, available at https://ssrn.com/abstract=2354988; EDPS, *calls for closer alignment between consumer and Data protection rules in the EU*, 8 October 2018, available at https://edps.europa.eu/press-publications/press-news/press-releases/2018/edps-calls-closer-alignment-between-consumer-and_en.

Consumer protection rules (CRD mainly) require the seller to inform the consumer of the total price of the service.[29] However, the concept of price is not always defined, which is why uncertainties can be raised in its application to non-monetary price services. The DCD defines price as "money or a digital representation of value that is due in exchange for the supply of digital content or a digital service"[30] with the digital representation of value referring to e-currency or e-voucher, but not to personal data.[31] Thus the DCD does not consider providing personal data as payment of a price.[32] The "Better enforcement and modernisation of EU consumer protection rules" Directive did not amend the CRD on the information requirements about the price and the concepts used appear to refer to monetary price.[33] Therefore, it could be argued that the obligation of information about the price in the CRD is not applicable to these non-monetary price services.

While the notion of "price" does not cover the collection of personal data, the UCPD considers the description of a service as "free" when this is not the case as an unfair misleading practice.[34] A commercial practice is *misleading* when it contains false information that could cause consumers to make a transactional decision that they would not have made otherwise.[35] An omission could also be *misleading* if it concerns important information that consumers need when making an informed transactional decision, and if the consumers would not have made the same decision had they been informed of this.[36] For example, presenting a social media to consumers as "free" when it requires personal data in exchange for access is an unfair practice.[37] Consumers would maybe

[29] Art. 5(1)(c) or 6(1)(e) CRD. The UCTD and UCPD also regulate what the trader can do when they indicate the price of their service (see below).

[30] Art. 2(7) DCD.

[31] Recital 23 DCD.

[32] In that sense as well, N. Helberger et al., 'The Perfect Match?', *op. cit.*, p. 14.

[33] Art. 5 (1)(c) CRD: 'the total price of the goods or services inclusive of taxes, or where the nature of the goods or services is such that the price cannot reasonably be calculated in advance, the manner in which the price is to be calculated, as well as, where applicable, all additional freight, delivery or postal charges or, where those charges cannot reasonably be calculated in advance, the fact that such additional charges may be payable'.

[34] N° 20 of the Annex to the UCPD containing a list of practices that are *per se* considered unfair.

[35] Art. 6 UCPD.

[36] Art. 7 UCPD.

[37] See Facebook's commitments following discussions with the European Commission and EU consumer authorities, available at http://europa.eu/rapid/press-release_IP-19-2048_en.htm; Commission Staff Guidance on the implementation/application of directive 2005/29/EC on unfair commercial practices, 2016, pp. 95 and 143. *Contra* see Berlin Landgericht, 12 February 2018, VzBv/Facebook. See VzBv's press release available at https://

not have created an account on this social network had they known that their personal data would have been reused for commercial purposes. In a recent decision, the Italian Competition Authority (AGCM) decided that the Facebook users were not adequately informed about the commercial use of their personal data. According to the Italian authority, the information provided by Facebook did not clearly make the distinction between the use of data to personalise the service (in order to connect users with each other) and the use of data to carry out advertising campaigns.[38] There was no indication about the importance of the commercial use of the user's personal data on the Facebook login page. The only information provided referred to the social purpose of the processing ("Facebook helps you to connect and stay in touch with the people in your life"). In the same decision, the AGCM considered as an aggressive practice the Facebook standard settings for the use of the personal data collected. These standard settings allowed Facebook to share these data to third parties by default and without explicit and prior consent of the user (only an opt-out possibility). The AGCM stated that these preselected settings prevented users from making an informed and conscious choice. Indeed, they were not informed of the economic implications of the sharing of their personal data and did not make an explicit choice.[39] Interestingly, this practice also violates the privacy by default obligation of the GDPR, which requires an opt-in procedure and the strictest possible privacy settings application by default.[40]

In data protection law, to ensure that any data collection and processing are transparent for the data subject[41], it is required for the data controller to inform the data subject on the main characteristics of the processing, namely what kind of personal data is collected, what the specific purpose of the collection is, to whom the data could be sent, and whether the processing could lead to a profiling of the data subject.[42] For example, the data controller has to explain to data subjects whether their

www.vzbv.de/sites/default/files/downloads/2018/02/14/18-02-12_vzbv_pm_facebook-urteil_en.pdf. This jurisdiction decided that intangible consideration (personal data) could not be regarded as a cost.

[38] AGCM Press Release, 29 November 2018, against Facebook, available at 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'-data-for-commercial-purposes.

[39] Free translation of the AGCM Decision, 29 November 2018, available at https://www.agcm.it/dotcmsdoc/allegati-news/PS11112_scorr_sanz.pdf.

[40] Art. 25(2) GDPR.

[41] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260, revised on 11 April 2018, endorsed by the EDPB.

[42] Art. 13-14 GDPR.

personal data are collected for profiling, therefore exposing them to target advertising, or whether the personal data are sold to other companies.

However, the GDPR does not explicitly force the data controller to explain that data collection serves as a counter-performance to fund the "free service", nor to explain the economic value of the data. Nevertheless, in accordance with the core principle of transparency and loyalty (broader informational obligation for the data controller)[43], the data controller should go further than providing the mere information required by articles 13 and 14 of the GDPR, and be more transparent on this economic aspect of the relationship they have with the data subject. The data controller should indicate that these processing operations are necessary to fund the service and constitute a required "counter-performance" to access this service.

For the information disclosure to be effective, it still needs to be done in a comprehensive way, taking into account the numerous biases and heuristics of consumers.[44] This is the reason why consumer law and the GDPR impose that the information be imparted in a plain and intelligible language, adapted by the service provider to the targeted public and presented in a concise manner (as 'user-friendly' as possible) so as not to overwhelm the data subject/consumer. If the terms used are too vague, a Court may invalidate these terms because they can be used by the trader to do things the consumer cannot clearly anticipate by reading the terms of the policy.[45]

In addition, the GDPR encourages information disclosure with standardised icons.[46] As consumers may not realise that 'free' services are financed by the exploitation of their personal data, the use of some icons to better understand those new business models should be promoted.

---

[43] Art. 5(1)(a) GDPR.

[44] OECD report, Quality considerations in the zero-price economy, 28 November 2018, p. 27, available at https://one.oecd.org/document/DAF/COMP (2018)14/en/pdf; A. DE STREEL and A.L. SIBONY, *Towards Smarter Consumer Protection Rules for the Digital Society*, CERRE Policy Report, October 2017.

[45] Art. 6 and 7 CRD, art. 5 UCTD, and art. 12 and Recitals 42 and 60 GDPR. On this topic, D. CLIFFORD, I. GRAEF and P. VALCKE, 'Pre-Formulated Declarations of Data Subject Consent – Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections', *CITIP Working Paper* 33/2017, p. 13, available at. https://ssrn.com/abstract=3126706. See also case law mentioned above (footnote 23) for recent applications of this principle to Facebook, Google and other giant's privacy policies and Facebook's commitments following discussions with the European Commission and EU consumer authorities, available at http://europa.eu/rapid/press-release_IP-19-2048_en.htm.

[46] Recital 60 GDPR.

Moreover, it is not disputable that most of the consumers do not read and/or understand the commercial or privacy conditions of the service when they subscribe to it. So, it is more important than ever to be extra vigilant about how the information is disclosed to data subjects.[47]

3. Analysis of the GDPR Legal Bases

To be lawful, the processing of personal data must rely on one of the six legal bases enshrined in article 6 of the GDPR. Three legal bases could be relevant for data processing used to fund a non-monetary price service: *the consent*, *the necessity for the performance of the contract* and *the legitimate interest of the data controller*.[48]

Before digging into these legal bases, it could be useful to clearly identify the analysed form(s) of processing(s).

In data protection law, a service (like social media for example) is often composed of several data processing operations. Some processing activities are useful or necessary for the performance of the service (to customise the user's experience for example), others can be useful for the data controller (to improve the service, to prevent fraud…), or to fund the service.

Even if all these different kinds of processing can be considered as a "bundle", given that all these processing operations are closely linked[49], each processing must rely on one of the GDPR legal bases.

[47] On this topic in consumer and data protection law, see R. DUCATO and A. STROWEL, 'Information duties between consumer and data protection in the "Internet of Platforms": promoting awareness by design', *DCCR* 2019, pp. 123-149.

[48] Art. 6 GDPR. The two other possible legal bases for the private sector are 'necessary for compliance with a legal obligation' or 'necessary in order to protect the vital interests of the data subject or of another natural person'. These two legal bases are clearly not relevant for this topic. We limit our study to article 6 and we do not analyse the case in which 'sensitive' data would be processed (article 9 GDPR). In its recent Guidelines of 2 September 2020 on the targeting of social media users, the EDPB did not even mention the possibility for a data processing to be based on the 'necessity for the performance of the contract'.

[49] In that sense, see EUCJ Case C-131/12, *Google Spain v. AEPD and Costeja Gonzales*, 13 May 2014, point 46. The EUCJ stated that 'the promotion and sale of [target] advertising space, […], constitute the bulk of the Google group's commercial activity and may be regarded as closely linked to Google Search'. This case concerned the location of the establishment of Google, but the same line of argument can be implemented here.

The choice of the legal basis is not a purely theoretical element. The data subject's rights might vary according to the chosen legal basis.[50]

a. Necessity for the performance of the contract to which the data subject is party

To perform a contract concluded with someone (a consumer for example), the data controller may have to process personal data of the other contracting party (e.g. to check credit card information for the payment or the address to deliver the product).[51] In this case, the data controller may process these data without a specific consent from the data subject. This is only possible when the data processing is necessary (and not merely useful), which means there is no other way to perform the contract without the processing of these personal data.

Arguing that a data processing is *necessary* for providing "free services" (i.e. to fund the business model of these kinds of services) is highly controversial and generally not accepted in the literature.[52] Indeed, the data processing is often not strictly necessary for the performance of the contract, but only to fund it. For example, in the case of target advertising, there are two different types of processing, one which is strictly necessary (to propose the personalised content…) and the other one which is not strictly necessary to propose such content (namely, reusing these personal data to finance the service and to provide target advertising).[53] For this reason, the EDPB does not accept this legal basis for target advertising by the social media.[54]

However, from a purely contract law perspective, it could be argued that the data processing is considered as the counter-performance of the service, hence that it is included in the commercial contract between the consumer/data subject and the trader/data controller. Indeed, the main issue is to identify the content of the contract. This perspective is maybe more in accordance with the new business models, where personal data

[50] See below for more practical consequences of this (Termination of the contract and withdrawal of consent).

[51] It can also cover the pre-contractual step.

[52] EDPS, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, p. 14. EDPB, Guidelines 2/2019 on the processing of personal data under Article 6 (1) (b) GDPR in the context of the provision of online services to data subjects, pp. 12-14.

[53] EDPB, Guidelines 2/2019 on the processing of personal data under Article 6 (1) (b) GDPR in the context of the provision of online services to data subjects, pp. 12-14.

[54] Idem; EDPB, Guidelines 8/2020 on the targeting of social media users, 2 September 2020, p. 16.

become a *de facto* price (trader perspective) or a *de facto* currency (consumer perspective), although it is not actually accepted in the data protection law literature. In this case, the validity conditions of the consent are the conditions of national contract/consumer law and no longer those of data protection law.

b. Legitimate Interests of the Data Controller

A data processing can also be grounded on the legitimate interests of the data controller or of a third party, if these interests are not overridden by the interests or fundamental rights and freedoms of the data subject. First, the interests of the data controller (or of a third party) have to be legitimate.[55] Secondly, there should be a balance of interests in order to evaluate the impact of the processing on the data subjects and compare it with the benefit expected from the processing by the data controller.[56]

In its opinion on the DCD Proposal, the EDPS analyses the possibility to base the data processing financing the non-monetary price service on the legitimate interests pursued by the data controller. The EDPS does not exclude the possibility to link this kind of process on the legitimate interests of the data controller but indicates its preference for the consent, as this forms a more transparent option.[57] Personal data processing to provide behavioural advertising constitutes a legitimate interest for the data controller, but this legitimate interest must still be balanced with the rights and interests of the data subject, and this balance should be performed on a case-by-case basis.[58] The EDPS however recalls the *Google Spain* case[59], in which the Court of Justice decided that "the data subject's fundamental rights override, as a rule, the economic interests of an operator". For example, the ICO states that RTB (Real-Time-Binding)[60] systems cannot rely their processing operations on the legitimate interests of their members. The "balancing test" seems unacceptable and the privacy

[55] There is no pre-set list. For some example of legitimate interests, see Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46.

[56] Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46, p. 56.

[57] EDPS, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content opinion digital content, p. 17.

[58] On the legitimate interests of the data controller, see Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46 and Opinion 2/2010 on online behavioural advertising.

[59] EUCJ Case C-131/12, *Google Spain v. AEPD and Costeja* Gonzales, 13 May 2014.

[60] The RTB system is a marketplace where advertising inventory is sold and bought in real time.

impact on the data subjects could actually be too high.[61] The EDPB also recalls[62] that "the WP29 has previously considered that it would be difficult for controllers to justify using legitimate interests as a legal basis for intrusive profiling and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data-brokering".[63]

Another issue relating to the use of this legal basis by the service provider is that the data subject has the right to object where personal data are processed for direct marketing purposes (e.g. target advertising). The EDPB considers that this right should clearly be given to the data subject *before* the processing.[64]

c. Data Subject's Consent

As the possibility to rely on other legal bases is limited or controversial, the last option is to base the data collection and processing on the user's consent. To be valid in data protection law, consent needs to be *freely given*, *informed*, *specific* and *explicit*.[65] We will especially concentrate on the condition that consent should be given freely.[66]

The consent should reflect a true choice of the data subject to accept the processing of personal data for a specific purpose.[67] However, in some circumstances, data subjects do not have the possibility to refuse to consent, because it could be too harmful for them (e.g. if the extra cost is too high or if there is no realistic alternative to this service).[68] For example,

---

[61] ICO updated report on RTB, 20 June 2019 available at https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.

[62] EDPB, Guidelines 8/2020 on the targeting of social media users, p. 16. We guess that it is its way to endorse this opinion.

[63] Article 29 Working Party, Opinion on profiling and automated decision-making, WP 251, rev. 01, p. 15, see also Article 29 WP, Opinion on legitimate interest, p. 32.

[64] EDPB, Guidelines 8/2020 on the targeting of social media users, p. 15.

[65] Art. 4(11) GDPR; EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, revised on 4 May 2020.

[66] The other points have mostly been addressed previously. For more details, see C. DE TERWANGNE, 'Les principes relatifs au traitement des données à caractère personnel et à sa licéité', *Le règlement général sur la protection des données (RGPD/GDPR) : Analyse approfondie 2018*, Cahier du CRIDS, Bruxelles, Larcier, pp. 120 et s.

[67] The trader cannot use these data for another incompatible purpose (principle of purpose limitation, art. 5(1)(b) GDPR).

[68] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, p. 8. For more details on this topic, see D. CLIFFORD, I. GRAEF and P. VALCKE, 'Pre-Formulated Declarations of Data Subject Consent–Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections', *CITIP Working Paper* 33/2017, pp. 35-40.

the consent would not be validated if it is required to access public transport.[69] Most of the "free" services block access to their services until the data subjects accept the privacy policy of the service. If data subjects want to access this service, they do not have a real choice and must give their consent to all the processing activities mentioned in the privacy policy ("take or leave it"-choice). In most of the cases, some processing operations are indeed necessary for the performance of the service, while others are not considered as strictly necessary (personalised advertising…).[70] Consumers should be able to choose the processing they accept or refuse.[71] In the case of mixed necessary and non-necessary processing operations, the given consent could be assumed not to have been freely given as the data processing is not strictly necessary for the performance of the service proposed.[72] The purpose of the GDPR, according to the EDPB, was to "ensure that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract".[73] This concern is probably now partially outdated since the adoption of the DCD, which specially legalises this kind of deal.[74] We regret that in its *Planet 49* case, the EUCJ does not give any answer regarding the lawfulness *per se* of the bundle, where one of the processing operations is only useful to fund the service.[75] However, the Advocate General Szpunar had clearly identified this issue in his Opinion.[76]

So now, the most important thing is not to discuss the lawfulness *per se* of this kind of bundle, but rather to check whether these bundles are "acceptable". To do that, the validity of the consent has to be analysed on a case-by-case basis taking into account all the circumstances of that specific situation and, in particular, look for a possibly clear imbalance

[69] In this sense, the French Data protection authority (CNIL) imposes on public transports to offer an anonymised way to take a transport ticket (instead of nominative cards). This ticket must also be at the same price. See Decision of the CNIL in 2004 available at https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017653201; Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP259, revised on 10 April 2018 (replaced now but this example has been cut out of the new EDPB guidelines).

[70] See above regarding this distinction.

[71] Recital 43 GDPR and EDPB, Guidelines 05/2020 on consent under Regulation 2016/679.

[72] Recital 43 and art. 7(4) GDPR.

[73] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, p. 10.

[74] The guidelines have been published after the DCD but it seems that the EDPB still refuses to accept this kind of business model.

[75] EUCJ Case C-673/17, *Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, 21 March 2019. On this case, see A. Delforge, 'Le placement de "cookies" sur un site web : la Cour de Justice fait le point, l'APD commence à sanctionner', *op. cit.*

[76] Point 99 of his Opinion.

between the two parties.[77] The GDPR does not say more about what should be included in this "imbalance". This "balance assessment" could maybe include the amount of data collected. A too voluminous collection of personal data could indeed be an indication of a forced consent (a data subject having a real choice would not have accepted to provide so much information).[78] One thing is clear: the imbalance of power must be assessed. If the data controller has too much power to impose its conditions (a public authority or an undertaking in dominant position), consent could be assumed not to be freely given. Indeed, there is no real choice when there is no alternative to the services offered. It is often the case in the online environment where network effects are massive and self-reinforcing.[79] For all these reasons, the EDPS and some literature suggest banning tracking walls in some circumstances.[80]

The best option to get a free consent, especially for dominant service providers, is to propose an alternative which would exclude the processing of personal data.[81] This alternative could be a fee-paying one, if the price remains reasonable, in the form of a subscription, for example. Given the existence of this affordable alternative, consumers/data subjects have a real choice to consent or not to the collection and the processing of their personal data. Such alternative offer also contributes to transparency as it renders the monetary value of personal data more explicit or, at least, sheds lights on the costs of providing the free service. This monetary alternative is not actually required. Nevertheless, in some circumstances of manifest imbalance of power given the dominant position of the undertaking on the market, it could *de facto* be the only indisputable way to obtain a real and freely given choice if the validity conditions were to be strictly interpreted.

The necessity to obtain the consent of the data subject can also be explained by the fact that the draft ePrivacy Regulation requires the consent of the data subject to set or read non-purely technical cookies on the

[77] D. Clifford, I. Graef and P. Valcke, 'Pre-Formulated …', *op. cit.*, pp. 35-38.

[78] On this aspect, see below "Assessing the fairness of the contractual relationships".

[79] Competition law principles could be very useful to evaluate this balance of power.

[80] 'Tracking walls mean that users who do not accept tracking across other sites will be denied access to the websites that they are seeking to access', see EDPS, Preliminary Opinion 5/2016 on the review of the ePrivacy Directive, p. 15; F. Z. Borgesius, S. Kruikemeier, S. Boerman et N. Helberger, 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation', *Eur. Data protection Law review 2017*, vol. 3, Issue 3, pp. 353 et s.

[81] EDPS, Preliminary Opinion 5/2016 on the review of the ePrivacy Directive, p. 15. Also in Recital 20aaaa of the Draft ePrivacy Regulation.

data subject's computer and does not actually provide other relevant legal bases for this kind of processing.[82]

4. Termination of the Contract and Withdrawal of the Consent

Consumer law provides consumers with a right to terminate a contract as well as a right to withdraw their consent. If the supplier does not provide a service or content to the consumer in conformity with the contract, the consumer can terminate the contract and be reimbursed for all the costs.[83] Upon contract termination, the supplier of the service should refrain from using any content other than personal data provided or created by the consumer during the use of the digital content or service, except where such content (A) has no utility outside the context of the digital content or digital service supplied by the trader; (B) only relates to the consumer's activity when using the digital content or digital service supplied by the trader; and (C.1) has been aggregated with other data by the trader and cannot be disaggregated or only with disproportionate efforts, or (C.2) has been generated jointly by the consumer and others, and other consumers are able to continue to make use of the content.[84] In addition, the consumer has the right to retrieve that content[85] free of charge, without hindrance, within a reasonable time and in a commonly used and machine-readable format.[86] Such a right of retrieval for non-monetary prices services can be regarded as equivalent to the right of a refund for monetary prices services. If it is possible to be reimbursed for all sums paid, the DCD does not provide for the possibility to require

[82] There is a discussion around the addition of other specific legal bases in the ePrivacy Regulation. Regarding the link between the 'GDPR consent' and the 'ePrivacy Consent', see A. DELFORGE, 'Le placement de "cookies" sur un site web : la Cour de Justice fait le point, l'APD commence à sanctionner', *op. cit.*

[83] Art. 13, 14, 15, 16 and 18 DCD.

[84] Art. 16(3) DCD and 13(5) CRD.

[85] This right does not apply in the same cases as we previously mentioned with respect to art. 16(3) DCD, see art. 16(4) DCD.

[86] Art. 16 DCD and 13(5) CRD. These articles specify that the GDPR is fully applicable and consequently, the consumer has, at any time and free of charge, the right of access to her personal data (art. 15 GDPR) and the right to data portability (art. 20 GDPR); EDPS, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, pp. 19-20.

a compensation for the personal data processing which has already been carried out.[87]

Even if the provided service is fully compliant, the consumer also has a right to withdraw during a specific period (14 days). There is an exception to this right with respect to digital content, which is not supplied on a tangible medium or for digital service, when the consumer "has to pay". In both cases, consumers have to be informed that they will lose their right before consenting.[88] Considering that the exception only applies to cases where a consumer is under an obligation to pay, one can argue that it is not applicable when personal data is used as a counter-performance.[89]

The trader should also be allowed to terminate the contract if the consumer does not provide personal data or provides wrong personal data. Indeed, it seems complicated to oblige the consumer to provide personal data (or correct/updated data). Damages could be claimed by the trader on the basis of the applicable contractual law.[90]

In addition to the DCD, the interaction with data protection law should also be considered. If consumers provide personal data instead of paying with money, they also have the right to withdraw their consent, at any time.[91] The DCD reminds that this right remains fully applicable.[92] Consumers have *de facto* a permanent right to terminate the contract, whenever they want. This withdrawal is without consequence to the past. If, in parallel with the termination of the contract, a user withdraws consent for the processing of personal data, the data controller has to stop such processing. The user may also use its right to object, due to its particular situation, to a data processing if this processing is based on the legitimate interests of the data controller.[93] The user also has the right

[87] Art. 16(1) DCD; A. METZGER, 'Data as Counter-Performance What Rights and Duties do Parties Have?', *JIPITEC 8 (1) 2017*, available at https://www.jipitec.eu/issues/jipitec-8-1-2017/4528, par. 22.

[88] Art. 16 (a) and m) CRD.

[89] The Commission proposal for DCD contained a provision on a right to terminate the contract for an indefinite period of time or exceeding 12 months (see art. 16 of the Proposal).

[90] In a German law context, A. METZGER, 'Data as Counter-Performance What Rights and Duties do Parties Have?', *JIPITEC 8 (1) 2017*, available at https://www.jipitec.eu/issues/jipitec-8-1-2017/4528, par. 19.

[91] See previously why consent actually appears as the only Data protection legal basis possible.

[92] Recitals 39 and 40. The consequences of this withdrawal for the consumer contract must be specified by national law.

[93] Art. 21 GDPR. This right is a way for the data subject to contest the balance of interests carried out by the data controller and to explain to the data controller that the data subject's

to object, without justification, to direct marketing purposes.[94] In this case, the data controller must stop the processing and the data may not be processed any more.

Data subjects may also request the erasure of personal data when they withdraw their consent or when the personal data is no longer necessary for the purpose for which they were collected or processed in the first place (for instance, if the contract is terminated and the processing was solely based on the performance of a contract as legal basis).[95]

5. Assessing the Fairness of the Contractual Relationships

In some cases, the volume of required data could be considered disproportionate to the type and quality of the services offered. For example, some torchlight apps for mobile phones require the activation of the mobile's location data.[96] Therefore, it seems interesting to examine how consumer and data protection laws can prevent this imbalance.

Under consumer protection law, the UCTD does not entail the control of such type of imbalance in the contract as it provides that "assessment of the unfair nature of the terms shall relate neither to the definition of the main subject matter of the contract nor to the adequacy of the price and remuneration".[97] As the UCTD is a minimum harmonisation Directive[98], Member States can go further and adopt national rules which are more protective for the consumer. Indeed, some Members States have entrusted their judicial Courts to control the balance between the price and the quality of the service or the product.[99] However, as already explained, the concept of price in consumer law does not, at least explicitly, cover the provision of personal data and the DCD makes a distinction between "pay with money" and "provide personal data". If this interpretation is chosen ("providing data" is not considered a "price" under consumer law), the fairness check on the quality/price ratio, *a priori* outside

rights and freedoms prevail, due to their specific situation, in regard to the legitimate interests of the data controller. The data controller should then justify why in this particular case its legitimate interests still prevail in order to be able to continue processing these data.

[94] Art. 21(2) GDPR.

[95] Art. 17 GDPR.

[96] N. HELBERGER et al., 'The Perfect Match?', *op. cit.*, p. 14.

[97] Art. 4.2. UCTD.

[98] As confirmed in EUCJ Case C-484/08, *Caja de Ahorros y Monte de Piedad de Madrid v. Asociación de Usuarios de Servicios Bancarios (Ausbanc)*, 3 June 2010.

[99] N. HELBERGER et al., 'The Perfect Match?', *op. cit.*, p. 18.

of the UCTD, could also "apply to the conditions under which consumers are required to provide data to access a service".[100] This means that the consumer fairness check could be relied upon to ensure that the terms of a privacy policy are not unbalanced to the detriment of consumers. It could be the case if the volume of data collected is too high in relation to the value of the service provided. Indeed, one can argue that the economic value of the data collected can be used as an equivalent to the monetary price. Given the revenues generated by some platforms, it can therefore be considered that they have to collect less data to rebalance the economic value of the respective performance of the user and the service provider. Actually, some jurisdictions invalidate the contractual terms of some of the giant Internet companies for being too vague, leaving these companies with too much power in respect of the data and data subjects with too little control over what is done with their data. These decisions did not go so far as to evaluate the economic value of personal data.[101]

Under data protection law, a severe imbalance between the required data and the provided service could violate the principles of proportionality and data minimisation.[102] An imbalance of the respective performance could also be useful element to assess the *freely given* aspect of the data subject's consent and the *clear imbalance* between the data subject and the data controller.[103]

Competition law is also another way to regulate some situations where the service provider holds a dominant position and can unilaterally impose its terms. In a recent decision, the German *Bundeskartellamt* decided that Facebook's terms and conditions violate data protection law and thereby also constitute exploitative business terms under the abuse of dominance prohibition under competition law. According to the *Bundeskartellamt*, it cannot be assumed that users effectively consent to Facebook's collection and use of data from third-party sources in view of its dominant position in the market for social networks.[104]

---

[100] *Ibidem.*

[101] See footnote n° 23 for a list of recent case law in which the jurisdictions analysed the fairness of data protection terms from a consumer law perspective.

[102] Explanatory report of the Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), § 44; N. HELBERGER et al., 'The Perfect Match?', *op. cit.*, p. 18. It is very complex to examine precisely how to evaluate the proportionality of a personal data processing.

[103] See above.

[104] German Bundeskartellamt Decision of 7 February 2019, Press release and FAQ in English at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

Conclusion

On the Internet, "free services" have become the norm and most people refuse to pay for accessing a service. The service providers understood that people consented more or less consciously to the provision of their personal data. They could thus easily reuse the data commercially to fund their service.

If, at the beginning, it could be seen as an opportunity to freely access new disruptive services, there is now usually no alternative to access these services if we refuse to provide our personal data.

The lawfulness of this business model has always been discussed in data protection law, and it remains so. Indeed, data protection law literature has trouble admitting that personal data could be seen as a "currency", which means it is "officially" unacceptable to provide personal data in exchange to the access to a service. As a consequence, this means that there are some difficulties to find a valid legal basis to ground the data processing. The necessity for the performance of the contract is not even considered by the EDPB as a possible legal basis, whereas it seems to be the more logical one if we go beyond the question of the lawfulness *per se* of this kind of service.

However, this refusal to admit the lawfulness of these services seems outdated since the adoption of the DCD, which settles the question of the applicability of consumer law to these "non-monetary services". By doing so, this Directive seems to "legalise" this new business model and the current challenge is now to determine how to regulate it.

Indeed, consumers are not always conscious of the amount of data collected nor of the commercial reuse of these data and they do not often have the choice to consent if they want to access the service. To avoid this, some argue to ban certain types of tracking walls or to impose on certain services to offer a monetary alternative, as implemented by some digital newspapers.

With this new business model, service providers can collect a huge amount of data, which is not adequate to the service provided.

Today, these issues are well known. Data protection and consumer laws can settle these issues efficiently. We take as an example the decision of the *Tribunal de première instance* of Paris[105] or, in competition law, the decision of the *Bundeskartellamt* against Facebook. These decisions

[105] TGI Paris, 9 April 2019, available at https://www.quechoisir.org/action-ufc-que-choisir-donnees-personnelles-l-ufc-que-choisir-obtient-la-condamnation-de-facebook-n65523/?dl=44179, pp. 11-13.

illustrate perfectly how different legal frameworks can interact with their rules and enforcement tools to regulate some complex situations.

These recent decisions do not mean that everything is settled. The overlaps between these different legal frameworks may cause several issues. The necessary joint application of these different legal frameworks should lead to the adoption of a more global and comprehensive vision on a "data consumer law"[106] as a mix of these two legal frameworks to address specific problems posed by these new services funded by a commercial use of consumer personal data.

[106] N. Helberger et al., 'The Perfect Match?', *op. cit.*, pp. 27-28.