Web 2.0 and the Concept of 'Data Controller': Recent Developments in EU Data Protection Law

Maria Berger & David Eisendle***

Abstract *In order to operationalise the fundamental right to privacy, as reaffirmed by the Supreme Court in the landmark K.S. Puttaswamy judgment, the Indian government has recently introduced a draft data protection legislation. The present draft is inspired — to a considerable extent — by the EU's GDPR and defines numerous key notions in largely identical terms. In view of these similarities, this paper seeks to examine the recent developments in the EU regarding the concept of 'data controller' and its application to what may be termed as a 'Web 2.0 setting'. The paper commences with a review of the obligations imposed on controllers under the GDPR. Next, it introduces the 'Web 2.0 setting' and traces the evolution of the 'data controller' concept with the emergence of the internet. The paper then turns to a substantive analysis of the understanding of data controllers in a Web 2.0 context by examining the case of Wirtschaftsakademie Schleswig-Holstein, which concerns the potential joint controllership of Facebook and the administrator of a Facebook fan page. The final section challenges the interpretations of the concept previously adopted by the ECJ and provides suggestions to better realise the objectives of data protection law.*

* Honorary Professor at the University of Vienna School of Law – Department of European, International and Comparative Law, Austria; former Judge at the Court of Justice of the European Union, Minister of Justice of the Republic of Austria and Member of the European Parliament.

** Legal Secretary (*référendaire*) in the Chambers of Judge Andreas Kumin at the Court of Justice of the European Union, prior to that in the Chambers of Judge Maria Berger and Advocate General Juliane Kokott; law and business studies in Vienna (Austria), Hong Kong and St. Gallen (Switzerland); LL.M, B.Sc., LL.B.

I. Introduction

From a European and judicial perspective, it is both valuable and enriching to keep an eye on key developments taking place in the case-law of top courts in other parts of the world. In that respect, the recent seminal judgment rendered by the Indian Supreme Court on 24 August 2017 in *K.S. Puttaswamy* v. *Union of India* deserves particular attention, for it ruled, in essence, that the right to privacy is protected as a fundamental right under the Constitution of India.[1] As the Supreme Court noted in memorable terms, privacy is the "*constitutional core of human dignity*" and subserves, at a normative level, "*those eternal values upon which the guarantees of life, liberty and freedom are founded*".[2] It went on to observe that while the negative content of privacy "*restrains the state from committing an intrusion upon the life and personal liberty of a citizen*", its positive content "*imposes an obligation on the state to take all necessary measures to protect the privacy of the individual.*"[3] Mindful of the challenges inherent to the network society and the information age that we live in, the Supreme Court rightly emphasised in this context that informational privacy is a facet of the right

---

1 *KS Puttaswamy v Union of India* (2017) 10 SCC 1 (*Puttaswamy*); *See*, for a presentation of the judgment, M Guruswamy, 'Justice K.S. Puttaswamy (Retd) and Anr v Union of India and Ors' (2017) 111 American Journal of International Law 994; further, on the evolution of the right to privacy in India, *see*, A Pillai and R Kohli, 'A Case for a Customary Right to Privacy of an Individual: A Comparative Study on Indian and other State Practice' (2017) Oxford University Comparative Law Forum 3 <https://ouclf.law.ox.ac.uk/a-case-for-a-customary-right-to-privacy-of-an-individual-a-comparative-study-on-indian-and-other-state-practice/> accessed 10 October 2019. It is interesting to note that the judgment was interpreted as having paved the way for another landmark decision of the Indian Supreme Court, of 6 September 2018, in *Navtej Singh Johar v Union of India* (2018) 10 SCC 1, concerning the decriminalisation of any consensual sexual relations among adults in private.

2 *Puttaswamy* (n 1) part T, para 3(E).

3 *Puttaswamy* (n 1) part T, para 3(I); *See also*, Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4(5) Harvard Law Review 193. This ground-breaking article on the subject famously captured the essence of this negative content of the right to privacy by referring to the right "*to be let alone*". As regards EU law, any limitation on the exercise of the right to privacy, laid down in Article 7 of the Charter of Fundamental Rights of the European Union, must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others; *See*, to that effect, European Court of Justice (ECJ) judgment of 8 April 2014, Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* 2015 QB 127: [2014] ECR 238 (38).

to privacy, and that dangers to privacy in an age of information can originate not only from the state but from non-state actors as well.[4]

In order to give effect to the right to privacy, the Indian government was thus directed to examine and put into place a robust regime for data protection. Subsequently, the committee established in response to the judgment and entrusted with the task of elaborating such a legal framework under the direction of retired Justice Srikrishna ('**Srikrishna Committee**') prepared a draft bill for a comprehensive Personal Data Protection Act.[5] In the Committee's explanatory report,[6] this bill – which is likely to be introduced in the Indian Parliament in June 2019 – is described as representing a fourth path, distinct from the approaches to data protection in the US, the EU and China.[7] However, as is apparent from both its structure and content, the bill is inspired to a considerable extent by the EU General Data Protection Regulation ('**GDPR**'),[8] which became applicable as of 25 May 2018. In particular, processing personal data requires a lawful basis – which is, first and foremost, consent – and the individuals whose data is being processed are conferred specific rights such as the right to confirmation of data and access to data, the right to data portability, the right to correction of data and the right to be forgotten, though these rights may differ in scope compared to the GDPR.[9] What is more, key notions of both the draft bill and the GDPR are defined in largely identical terms. This holds true not only for 'personal data' and 'processing', but also for 'data subjects' and 'data controllers', even though, in respect of the two latter notions, the terminology differs as the draft bill refers to 'data principals' and 'data fiduciaries'.[10]

---

4 *Puttaswamy* (n 1) part T, para 5.

5 The Draft Personal Data Protection Bill 2018 (*Draft Bill*). For an analysis of the bill, *see*, Lothar Determann and Chetan Gupta, 'Indian Personal Data Protection Act, 2018: Draft Bill and its History, compared to GDPR and California Privacy Law' (2018) UC Berkeley Public Law Research Paper <https://dx.doi.org/10.2139/ssrn.3244203> accessed 10 October 2019.

6 Committee of Experts under Justice BN Srikrishna, *A Free and Fair Digital Economy—Protecting Privacy, Empowering Indians* (2018) <https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf> accessed 10 October 2019.

7 ibid 14.

8 Regulation (EU) 2016/679 of 27 April 2016 of the European Parliament and of the Council 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(2016) OJ L119/1 (GDPR).

9 *See*, Draft Bill, chs III and VI.

10 As is pointed out at pages 7 and 8 of the Srikrishna Committee's report (n 6), in a regulatory framework where the rights of the individual with respect to her personal data are respected and the existing inequality in bargaining power between individuals and entities that process such personal data is mitigated, the individual must be the *data principal* since she is the focal actor in the digital economy. By contrast, entities collecting personal data

In view of these similarities, it appears to be of interest from a comparative legal perspective for this Journal's readers in India and beyond to shed light on recent developments in EU data protection law with regard to the concept of data controller. This concept plays a crucial roles since it determines responsibility for compliance with data protection rules. In this contribution, we first provide a brief overview on the definition of data controller under EU law and the case-law of the European Court of Justice ('**ECJ**') on this concept's application in the context of the Internet. We then examine how this concept is applied in what can be called a 'Web 2.0 setting'. For this purpose, we focus on the recent judgment rendered by the Grand Chamber of the ECJ in the case of *Wirtschaftsakademie Schleswig-Holstein*[11] concerning the question of data protection responsibility in relation to a fan page on the social network Facebook.

II. The Concept of 'Data Controller' in EU Data Protection Law

A. Principles

In EU data protection law, data controllers take on a central role. As it has previously been held in the ECJ's case-law, controllers must ensure, within the framework of their responsibilities, powers and capabilities, that the data processing in question meets the legal requirements in order that the guarantees laid down by law may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved.[12] Under the regime of the GDPR, this is reflected most fundamentally in Article 24(1), according to which the controller is tasked to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the regulation. The provisions in Chapter III of the GDPR, which concern the rights of the data subject, are essentially directed at the controller and define obligations incumbent on him. It is therefore the controller's responsibility to provide transparent information to the data subject concerning collected personal data relating to him, to grant access to the personal data, and to

have a duty of care to deal with such data fairly and responsibly for purposes reasonably expected by the principals, which makes such entities *data fiduciaries*.

[11] C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* (2019) 1 WLR 119 (ECJ, 5 June 2018) (*Schleswig-Holstein*).

[12] C-131/12 *Google Spain SL and Google v Agencia Española de Protección de Datos* (AEPD) 2014 QB 1022: (2014) 3 WLR 659 (ECJ, 13 May 2014) paras 38 and 83 (*Google Spain*).

ensure rectification of inaccurate personal data or its erasure. Furthermore, under Article 82(1) GDPR, any person who has suffered damage as a result of an infringement is entitled to receive compensation from the controller, and under Article 82(2), any controller involved in processing shall be liable for the damage caused by processing data in violation of the regulation.

According to Article 4(7) GDPR, 'controller' is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.[13] This definition corresponds to the one retained in Article 2(d) of the original EU Data Protection Directive[14] ('**DPD**'), which was adopted in 1995 and repealed by the GDPR. For analysing the notion of controller, valuable guidance has been provided by a detailed study[15] carried out by the Article 29 Data Protection Working Party, an independent advisory board set up by the DPD and comprising, in particular, representatives from the EU Member States' national data protection authorities.[16] As the Working Party pointed out, the concept of controller has, fundamentally speaking, a wide and dynamic meaning and scope, for it relates to activities reflecting the life cycle of information from the point of its collection to its destruction.[17] Furthermore, it is a functional concept intended to allocate responsibilities where the factual influence is, and is thus based on a factual rather than a formal analysis.[18]

The definition of controller includes three central elements. Besides the *personal* aspect ("*natural or legal person, public authority, agency or any other body*") and the possibility of *pluralistic control* ("*alone or jointly with others*"), it is the *substantive* element (determination of the "*purposes and means of the processing of personal data*") that deserves particular attention, as it is this part that allows one to distinguish the controller from other actors. According to the Working Party's findings, determining the purposes and the means amounts to determining respectively the *why* and the *how* of

---

[13] By way of comparison, cl 13(3) of the Draft Bill defines 'data fiduciary' as "*any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data*."

[14] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L281/31 (DPD).

[15] Article 29 Working Party (WP 29), *Opinion 1/2010 on the concepts of 'controller' and 'processor'* (2010) 00264/10/ENWP 169 (Opinion 1/2010).

[16] As of 25 May 2018, the WP 29 has been replaced by the European Data Protection Board; *See*, GDPR, arts 68-76.

[17] Opinion 1/2010 (n 15) 3.

[18] Opinion 1/2010 (n 15) 9. It is stated, in this connection, that one should look at the specific processing operations in question and understand who determines them, by replying in a first stage to the questions "*why is this processing taking place? Who initiated it?*".

certain processing activities. While determination of the purpose of the processing would in any case trigger the qualification as controller, determining the means implies, in their view, control merely over the essential elements of the processing. By contrast, as regards technical or organisational questions, the determination of the means of processing can be delegated by the controller.[19]

B. The Concept's Application in the Context of the Internet

It must be borne in mind that the foundations of EU data protection law, and the definition of data controller included in this legal framework, date back to a time at which the Internet – here understood in the sense of the World Wide Web – was still in its infancy.[20] This framework, originally established by the DPD and now carried forward to the GDPR, has been characterised as a *linear model*, fitting well for an environment of centralised data processing with independent relationships between data subjects and data controllers. In such a setting, the controller is the main architect of the information system, exercising full control and responsibility.[21] Given that both the DPD and the GDPR were drafted in a technology neutral manner, it presented no particular difficulties to clarify that, in principle, data protection rules fully apply to data processing taking place on the Internet as well. Thus, in its early landmark case *Lindqvist*, the ECJ ruled that the DPD applied to a situation where elements of personal data are published on a web page on the Internet.[22]

Subsequently, in *Google Spain and Google,* the ECJ was called upon to examine a situation where an Internet search engine provided search results

---

[19] Opinion 1/2010 (n 15) 13 and 15. The WP 29 identifies aspects such as "*which data shall be processed?*", "*for how long shall they be processed?*", or "*who shall have access to them?*" as essential elements.

[20] In effect, the EU Commission's original proposal for the EU Data Protection Directive (DPD) was presented in 1990, when the World Wide Web had not even existed yet and the epoch-making changes it would induce could barely be foreseen.

[21] *See*, Omer Tene, 'Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws' (2013) 74 Ohio State Law Journal 1219; Rene Mahieu, Joris van Hoboken and Hadi Asghari, 'Responsibility for Data Protection in a Networked World – on the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe' (2018) 10 Journal of Intellectual Property, Information Technology and E-Commerce Law 85 <https://dx.doi.org/10.2139/ssrn.3256743> accessed 10 October 2019.

[22] C-101/01 *Bodil Lindqvist v Aklagarkammareni Jönköping* 2004 QB 1014: (2004) 2 WLR 1385 (ECJ, 6 November 2003). The case concerned a church worker in Sweden who published, on her personal internet website, information about other parish members, such as their names, hobbies and phone numbers, without having obtained those individuals' prior consent.

which direct the engine's users to the source web page. The question was, inter alia, whether the operator of such a search engine had to be regarded as a data controller in respect of the processing of personal data that it carried out. It was argued that the operator did not meet the definition of data controller, given that it did not exercise control over the personal data published on the web pages of third parties.[23] The Court explicitly rejected this argument, pointing out that the concept of controller must be interpreted broadly, with a view to ensure effective and complete protection of data subjects, and that it was not necessary, in order to be regarded as a controller, to have complete control over all aspects of data processing.[24] The Court further considered that the processing of personal data carried out in the context of the activity of a search engine could be distinguished from, and was additional to, that carried out by publishers of websites, consisting in loading those data on an Internet page.[25] For it is the search engine operator which determines the purposes and means of its activity and thus of the processing of personal data that it itself carries out within the framework of that activity. Consequently, the search engine operator had to be regarded as the data controller in respect of that processing.[26]

One cannot but realise, however, that in comparison to the factual circumstances which the two cases outlined above were based on, contemporary technological reality is immensely more sophisticated. This reality is characterised by multi-tiered structures and complex, interactive relationships between individual actors. New features have emerged and continue to expand rapidly; including social networks, hosted services and web applications – developments that are commonly referred to as being part of and forming *Web 2.0*. A typical situation is that an information provider's interactive web presence is integrated in another provider's platform. Think, for instance, of blogs or of merchants offering goods on Amazon Market place or Ebay. Visitors to theses web pages are faced with at least two different information providers. From a data protection point of view, the question thus arises as to how one must apply data protection rules in these settings. In particular, in addition to establishing data protection responsibility, it

---

[23] *Google Spain* (n 12) para 22.
[24] *Google Spain* (n 12) para 34.
[25] *Google Spain* (n 12) para 35.
[26] *Google Spain* (n 12) para 33. By contrast, in his opinion rendered in this case, Advocate General Jääskinen argued that Internet search engine service providers merely supply an information location tool without exercising control over personal data included on third-party web pages. As they cannot in law or in fact fulfil obligations of a controller in relation to the personal data on source web pages, they should not generally be considered as having that position.

must be determined how responsibility is to be allocated between the individual information providers.[27]

III. Data Control in a Web 2.0 Setting – the *Wirtschaftsakademie Schleswig-Holstein* Case

A. Facts of the Case

The ECJ was recently called upon to address precisely this issue in a case concerning a fan page hosted on the social network Facebook. Such a fan page can be set up, by individuals or businesses registered with Facebook, who can then use the platform, for instance, to introduce themselves to their users and to communicate with them. Additionally, operating the fan page entails the possibility to obtain, by means of a function called *Facebook Insights*, 'anonymous' statistical information on visitors to the page. This feature, which can be categorised as a form of *online behavioural tracking*,[28] is made available by Facebook free of charge under non-negotiable conditions of use. Information is collected by means of evidence files (cookies), which each contain a unique user code and remain active for two years while they are stored by Facebook on the fan page visitor's computer hard disk or other media. The user code is collected and processed when the fan pages are opened. Consequently, Facebook receives, registers and processes the information stored in the cookies when a person visits its services.

The German-based company Wirtschaftsakademie Schleswig-Holstein ('**Wirtschaftsakademie**') operates a fan page hosted on Facebook, by means of which it offers educational services. In November 2011, Wirtschaftsakademie

---

[27] *See*, P Hacker, 'Mehrstufige Informationsanbieterverhältnisse zwischen Datenschutz und Störerhaftung' (2018) 21 Multimedia und Recht 779; Bernd Wagner, 'Disruption der Verantwortlichkeit: Private Nutzer als datenschutzrechtliche Verantwortliche im Internet of Things' (2018) Zeitschrift für Datenschutz 307, 308; S Schulz, 'Case Comment Wirtschaftsakademie Schleswig-Holstein' (2018) Zeitschrift für Datenschutz 357, 364.

[28] Such tracking consists in recording and collecting data linked to an individual visiting the internet over a period of time in order to gain information on this individual. *See*, G Skouma and L Léonard, 'On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection' in S Gutwirth et al (eds), *Reforming European Data Protection Law* (Springer 2015) 35; Mireille Hildebrandt, 'Profiling: From Data to Knowledge – The Challenges of a Crucial Technology' (2006) 30 Datenschutz und Datensicherheit 548, 549; *See also*, Claude Castelluccia, 'Behavioural Tracking on the Internet: A Technical Perspective' in S Gutwirth et al (eds), *European Data Protection: In Good Health?* (Springer 2012). Behavioural tracking used for advertisement purposes is referred to as *behavioural advertising*. In this context, characteristics of online behaviour are tracked to develop a specific profile of users in order to provide tailored advertisement; *See*, WP 29, *Opinion 2/2010 on online behavioural advertising* (2010) 00909/10/ENWP 171 4, 5.

was ordered by a German data protection authority to deactivate the fan page it had set up, on the ground that visitors to the fan page were not informed that Facebook, by means of cookies, collected and processed personal data concerning them. Wirtschaftsakademie brought a complaint against that decision, arguing, in essence, that it was not responsible under data protection law for the processing of the data by Facebook or the cookies which the latter installed. By contrast, the data protection authority took the view that, by setting up the fan page, Wirtschaftsakademie had made an active and deliberate contribution to the collection by Facebook of personal data relating to visitors to the fan page, from which it profited by means of the statistics provided to it by Facebook. Subsequently, Wirtschaftsakademie turned to the Administrative Court which annulled the data protection authority's decision and found that the administrator of a fan page on Facebook, such as Wirtschaftsakademie, cannot be considered as controller and therefore cannot be the addressee of a measure such as to deactivate its fan page.[29] The Higher Administrative Court confirmed this view, stating that Wirtschaftsakademie was not a responsible entity in relation to the data collected by Facebook. Facebook alone decided on the purpose and means of collecting and processing personal data used for the Facebook Insights function, whereas Wirtschaftsakademie only received anonymised statistical information.[30]

The data protection authority appealed to the German Federal Administrative Court which, in line with the courts of lower instance, also held that Wirtschaftsakademie could not itself be regarded as responsible for the data processing.[31] It considered that while Wirtschaftsakademie, as a result of setting up a fan page, objectively provided Facebook with the possibility of using cookies when the fan page is retrieved and collecting data via these cookies, this could not lead to the inference that Wirtschaftsakademie was able to influence, administer, design or otherwise control the nature and scope of the processing by Facebook of its users' data. The conditions of use for the fan page did not give Wirtschaftsakademie any rights to influence or control this aspect. The unilaterally imposed conditions of use of Facebook were not the result of a process of negotiation and did not give Wirtschaftsakademie the right to prohibit Facebook from collecting and processing data of users of its fan page. Thus, Wirtschaftsakademie had

---

[29] *Rechtsanwälte A v Das Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (2013) 8 A 14/12 (Verwaltungsgericht Schleswig).

[30] *Rechtsanwälte A v Das Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (2014) 4 LB 20/13 (Schleswig-Holsteinisches Oberverwaltungsgericht).

[31] BVerwG (Federal Administrative Court, Germany), decision of 25 February 2016 1 c 28.14 para 16.

no decision-making, design or control powers. Accordingly, without any legal or actual influence on the decision about how personal data is processed, it could not be regarded as a controller. Furthermore, the Federal Administrative Court noted that while there was a legal relationship between Wirtschaftsakademie and Facebook to provide a fan page, this user relationship did not mean that Wirtschaftsakademie had commissioned Facebook to collect and process the data of the users of its fan page on its behalf.

However, the Court wondered whether, under such circumstances, the monitoring and intervention powers available to the data protection authority may relate solely to the data controller (i.e., in the present case, Facebook) or whether there nonetheless remained scope for responsibility of an entity that does not control the data processing, like Wirtschaftsakademie, when choosing the operator for its information offering. It took the view that in information provider relationships in which providers use an infrastructure such as that offered by Facebook, where they do not themselves control the processing of personal data by the infrastructure provider, it is necessary to also include the information provider itself within the scope of responsibility. This is essential to ensure the effective protection of the users of the information. This data protection responsibility would then relate to the careful choice of the operator of the infrastructure used for the information provider's own offering. Therefore, having in mind the objective of effective protection of the right to privacy, the Federal Administrative Court decided to stay the proceedings. It referred to the ECJ the question of whether the notion of data controller in EU data protection law definitively and exhaustively defines liability and responsibility for data protection infringements, or whether scope remains, in multi-tiered information provider relationships such as in the setting at issue, for responsibility of an entity that does not control the data processing, when it chooses the operator of its information offering.[32]

B. The ECJ's Judgment

Recalling the necessity to ensure, through a broad definition of the concept of data controller, effective and complete protection of the persons concerned, the ECJ considered – as was undisputed in the present case – that Facebook had to be regarded as the controller, for it primarily determined the purposes and means of processing the personal data of users of Facebook

[32] Other questions referred to the ECJ by the Federal Administrative Court, concerning inter alia the division of competences between data protection authorities of different EU member States, are not relevant here.

and persons visiting the fan pages hosted on Facebook.[33] However, the Court emphasised that that concept did not necessarily refer to a single entity and may concern several actors taking part in the processing of personal data. It thus went on to examine whether and to what extent Wirtschaftsakademie *itself*, as the administrator of a fan page on Facebook, may also be regarded as a controller, inasmuch as it contributes in the context of that fan page in determining, jointly with Facebook, the purposes and means of processing the personal data of the visitors to the fan page.[34]

The Court answered in the affirmative. First of all, it noted that the processing of personal data at issue was:

> intended in particular to enable Facebook to improve its system of advertising transmitted via its network, and to enable the fan page administrator to obtain statistics produced by Facebook from the visits to the page, for the purposes of managing the promotion of its activity, making it aware, for example, of the profile of the visitors who like its fan page or use its applications, so that it can offer them more relevant content and develop functionalities likely to be of more interest to them.[35]

While, in the Court's view:

> the mere fact of making use of a social network does not make its user a controller jointly responsible for the processing of personal data by that network, […] the administrator of a fan page hosted on Facebook, by creating such a page, gives Facebook the opportunity to place cookies on the computer or other device of a person visiting its fan page, whether or not that person has a Facebook account.[36]

Moreover,

> the creation of a fan page on Facebook involves the definition of parameters by the administrator, depending inter alia on the target audience and the objectives of managing and promoting its activities, which has an influence on the processing of personal data for the purpose of producing statistics based on visits to the fan page. The administrator may, with the help of filters made available by Facebook, define the criteria in accordance with which the statistics are to be drawn up and even designate the categories of persons whose personal data is to be made use of by Facebook. Consequently, the administrator of a fan

---

[33] *Schleswig-Holstein* (n 11) paras 28 and 30.
[34] *Schleswig-Holstein* (n 11) para 31.
[35] *Schleswig-Holstein* (n 11) para 34.
[36] *Schleswig-Holstein* (n 11) para 35.

> page hosted on Facebook contributes to the processing of the personal data of visitors to its page.[37]

The Court added that

> the administrator of the fan page can ask for and thereby request the processing of — demographic data relating to its target audience, including trends in terms of age, sex, relationship and occupation, information on the lifestyles and centres of interest of the target audience and information on the purchases and online purchasing habits of visitors to its page, the categories of goods and services that appeal the most, and geographical data which tell the fan page administrator where to make special offers and where to organise events, and more generally enable it to target best the information it offers.[38]

In contrast, the fact that the audience statistics compiled by Facebook were transmitted to the fan page administrator only in anonymised form was not deemed decisive, given that the production of those statistics was based on the prior collection and processing of the personal data of those visitors for such statistical purposes.[39] Furthermore, the Court explicitly held that the use of a platform like the one operated by Facebook could not exempt a fan page administrator from compliance with data protection rules, given that a Facebook user account is not a precondition for being able to access the page. Rather,

> the fan page administrator's responsibility for the processing of the personal data of those persons appears to be even greater, as the mere consultation of the home page by visitors automatically starts the processing of their personal data.[40]

Therefore, the Court concluded that the administrator of a fan page hosted on Facebook, such as Wirtschaftsakademie, must be regarded as taking part in the determination of the purposes and means of processing the personal data of the visitors to its fan page and must thus be categorised, jointly with Facebook, as a controller responsible for that processing.[41]

---

[37] *Schleswig-Holstein* (n 11) para 36.
[38] *Schleswig-Holstein* (n 11) para 37.
[39] *Schleswig-Holstein* (n 11) para 38.
[40] *Schleswig-Holstein* (n 11) para 41.
[41] *Schleswig-Holstein* (n 11) para 39.

IV. Analysis

A. The Court's *leitmotif*: Effective and Complete Protection

Historically speaking, the enactment of a common EU legal framework on data protection was primarily driven by the desire to facilitate free movement of personal data within the EU.[42] It was expressly emphasised in Article 1(1) of the original DPD that the fundamental rights of individuals, in particular their right to privacy with respect to the processing of personal data, shall be protected.[43] This is repeatedly echoed in the case-law of the ECJ when it is noted that the DPD seeks to ensure a high level of protection.[44] In respect of Wirtschaftsakademie, which was an addressee of an injunctive order issued by a data protection authority, the courts in Germany initially dealing with the matter were well aware of this objective of EU data protection law. In their view though, only Facebook but not Wirtschaftsakademie could be regarded as responsible entity, given that, in essence, the latter was not deemed to exercise any influence on the processing of personal data. It was precisely in order to avoid gaps in protection that the German Federal Administrative Court considered whether the administrator of a Facebook fan page like Wirtschaftsakademie could nonetheless, even if to a lesser extent than a data controller, be made held responsible due to the (poor) choice of the operator of its information offering.[45]

Neither the ECJ, nor its Advocate General tasked with delivering a reasoned opinion on the case prior to the judges' deliberations, agreed with the premise that the German courts had based their reasoning on. Advocate General Bot pointed out that, most fundamentally, the data processing at issue was preconditioned by the decision of the fan page administrator to create and operate the page. Not only does that administrator have a decisive

---

[42] *See*, DPD, Recitals 3, 8 and 10; Case C-518/07 *Commission v Germany* 2010 ECR I-1885 (ECJ, 9 March 2010) para 20; Joined Cases C-465/00, C-138/01 and C-139/01 *Rechnungshof v Österreichischer Rundfunk and Others* and *Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk* 2003 ECR I-4989 (ECJ, 20 May 2003) paras 39 and 70.

[43] Under the regime of the GDPR, Article 1(2) provides that the Regulation "*protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data*."

[44] *See*, *Google Spain* (n 12) para 66; C-362/14 *Maximillian Schrems v Data Protection Commr* 2014 QB 527 (ECJ, 6 October 2015) para 38; C-473/12 *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert* (2014) 2 CMLR 297 (ECJ, 7 November 2013) para 28.

[45] *See*, F Jotzko, 'Case Comment Wirtschaftsakademie Schleswig-Holstein' (2018) 73 Juristenzeitung 1154, 1160.

influence over the commencement of the processing of the visitors' personal data, but it also lies in its hands to end that processing by closing the page down.[46] He further argued that, by using a tool like Facebook Insights, a fan page administrator participates in the determination of the purposes and means of the processing of the personal data of visitors to its page.[47] The administrator is able to influence the specific way in which that tool is put to use by defining the criteria for the compilation of the viewing statistics, thus playing a predominant role in how that data is processed by Facebook and exerting a de facto influence over it.[48]

The ECJ followed this approach and relied less on a textual analysis of the definition of data controller when interpreting the concept and applying it to the case at hand. Instead, it placed emphasis on teleological considerations. In effect, rather than analysing individually the purpose(s) and the means of the data processing induced by the creation of a fan page on Facebook, the Court noted with reference to *Google Spain and Google* that the objective of the provision defining the notion of data controller was to ensure, through a broad definition of that concept, effective and complete protection of the persons concerned. It went on to distinguish between three aspects: First, by creating the fan page, its administrator *enables* data processing by Facebook. Second, the administrator contributes itself to the data processing through defining *parameters* according to which statistics on the page's visitors are produced. Third, the administrator can *request* demographic data relating to its target audience, without it being relevant that this information is transmitted by Facebook only in anonymised form or that the administrator does not have (complete) access to the relevant data. Thus, an entity can meet the requirements for being qualified as data controller if it exerts, to a sufficient degree, influence over the data processed. While the first argument that the Court referred to in this context (*enabling*) would, taken alone, be particularly wide-ranging, it appears that the crucial element is the possibility to define parameters.[49] In fact, the Court concluded that precisely due to the definition of parameters, the administrator of a fan page must be regarded as "*taking part in the determination of the purposes and means*" of processing the personal data of the visitors to its fan page.[50] By contrast, joint responsibility needs to be distinguished from situations in which two or more actors

[46] *Schleswig-Holstein* (n 11) para 56.
[47] *Schleswig-Holstein* (n 11) para 55.
[48] *Schleswig-Holstein* (n 11) para 57.
[49] *See*, J Marosi and L Matthé, 'Case Comment Wirtschaftsakademie Schleswig-Holstein' (2018) Zeitschrift für Datenschutz 357, 362.
[50] *Schleswig-Holstein* (n 11) para 39.

simply collaborate in the processing of personal data, each processing taking place within its own sphere.

Through its broad approach, the Court primarily addresses the risk inherent to multi-tiered information provider relationships where the actors involved circumvent data protection rules and shuffle off responsibility elsewhere, to the detriment of the individuals whose personal data is processed.[51] As the Advocate General pointed out in his Opinion, a narrow interpretation might provide an incentive for an undertaking to have recourse to the services of a third party in order to escape its data protection obligation. In a setting such as the one at issue, an information provider like the fan page administrator could use a platform which might infringe data protection rules, but nonetheless escapes responsibility. In order to achieve a high level of protection, it must therefore be ensured that operators are not able to evade data protection compliance, by using a hosting service for their information offering.[52] In addition, the approach taken is also likely to produce a ripple effect with respect to all the information providers involved. First, operators are called upon to exercise care and diligence in choosing their platform provider and, if necessary, refrain from using its services. Consequently, the platform provider itself is encouraged to comply with data protection rules in order not to jeopardise its commercial success.[53] It is therefore to be seen in light of these aspects that the Court concluded that in a situation such as the one at issue, recognition of joint responsibility in relation to the processing of personal data contributes to *ensuring more complete protection* of the rights of data subjects.[54]

B. One Step Further? The Pending Case *Fashion ID*

To what extent the ECJ's judgment will set a precedent for the assessment of similar situations involving two or more information providers is not fully foreseeable at this point, given that the facts of the case are characterised by certain particularities. In fact, creating and operating a Facebook fan page inevitably entails the use of the platform provided by Facebook and, consequently, the processing of personal data by it. Visitors to the fan page cannot avoid their data being processed by Facebook, except by refraining from accessing the page altogether. The spheres of responsibility of Facebook and

---

[51] *See*, Jotzko (n 45) 1160.

[52] *See*, *Schleswig-Holstein* (n 11) paras 62 and 64.

[53] *Schleswig-Holstein* (n 11) para 4. *See*, to that effect, Nicolas Blanc, 'Wirtschaftsakademie Schleswig-Holstein: Towards a Joint Responsibility of Facebook Fan Page Administrators for Infringements to European Data Protection Law?' (2018) 4 European Data Protection Law Review 120, 124.

[54] *Schleswig-Holstein* (n 11) para 42.

the fan page administrator thus seem inextricably intertwined.[55] Therefore, the judgment must be considered as being directly relevant for settings in which entities using a platform for their information offering (can) exert a certain influence on purposes and means of the data processing performed by the platform provider.

As outlined above, in the present case, this influence appeared to be established for the Court primarily due to the fact that fan page administrators defined parameters and criteria according to which statistics were drawn up, thereby contributing to the processing of the personal data of the visitors. It remains to be seen, however, whether such kind of interference effectively presents a minimum level. In *Fashion ID*, a case currently pending before it, the ECJ has the opportunity to provide further clarifications.[56]

Fashion ID is a German-based online retailer which sells fashion items on its website. The retailer embedded a plugin, the so called 'Like-button', provided by Facebook, on its website. When a visitor accesses the site on which the button appears, this visitor's Internet Protocol address and browser string are automatically sent to Facebook, irrespective of whether the visitor even clicked on it. A consumer protection association brought legal proceedings and sought an order to force Fashion ID to cease integrating the plugin on its website, on the grounds, essentially, of failure to inform about the purpose of the data collection and the use of the data and to obtain the visitors' consent for the transmission of their data. The question arising in this context is whether someone who has embedded a plugin on a website which transmits personal data to a third party is to be considered a data controller, even without being in a position to influence the subsequent processing of the data obtained by that third party.[57]

Unlike in the *Wirtschaftsakademie* case, it does not appear that Fashion ID determines the parameters of any information about its website's visitors which would then be returned to it. The purpose of embedding the 'Like-button' rather consists in optimising advertisement of the products offered by the retailer, by being able to make them visible on Facebook. While the ECJ has not yet rendered its judgment in the case, Advocate General Bobek opined that the crucial criterion for an entity to be considered a data controller, was that that entity made it possible for personal data to be collected and

---

[55] *See*, F Moos and T Rothkegel, 'Case Comment Wirtschaftsakademie Schleswig-Holstein' (2018) 21 Multimedia und Recht 591, 599.

[56] C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* (2020) 1 WLR 969 (ECJ, 26 January 2017) *(Fashion ID)*, initiated by a request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Higher Regional Court Düsseldorf, Germany) .

[57] Oberlandesgericht Düsseldorf, decision of 19 January 2017 I-20 U (40/16).

transferred, without it being necessary that specific input as to the parameters is provided. In his view, (co-)determining the parameters of the data collected already takes place through the simple act of embedding the plug-in, which itself provides parameters of the personal data to be collected.[58]

C. Joint Control – Joint Liability?

In the light of this, it has been critically remarked that by setting the bar low as to the necessary extent of an entity's actual influence on determining the means and purposes of the processing of personal data, there is a risk of over stretching the concept of data controller.[59] In connection with Facebook fan pages, it has been noted in particular that the page administrator has usually no influence at all on the platform's architecture and key features, but is limited to use its services under non-negotiable terms – take it or leave it.[60] A wide understanding of (joint) control might inevitably go along with expanding liability beyond a limit that can be deemed reasonable.

The Court's considerations in *Wirtschaftsakademie* suggest awareness of this tension, given that it is expressly pointed out that "*the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data*." Rather, "*those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case*."[61] However, the Court did not further elaborate on this aspect, given that it was not called upon to examine in more detail the practical consequences of joint responsibility.

Stressing the need for a reasonable correlation between power, control and responsibility, Advocate General Bobek argues that the issue of control is to be assessed with regard to the concrete operation in question. A (joint) controller should therefore be deemed responsible for that operation or set of operations for which it shares or co-determines the purposes and means as far as a given processing operation is concerned.[62] By contrast, liability cannot spill over into any subsequent stages of data processing,

---

[58] Opinion of Advocate General Bobek in *Fashion ID* (n 56) paras 67-69.

[59] Opinion of Advocate General Bobek in *Fashion ID* (n 56) para 71; Hacker (n 27) 779-780; Schulz (n 27) 364; D Klein, 'Case Comment Wirtschaftsakademie Schleswig-Holstein' (2018) Zeitschrift für Internationales Wirtschaftsrecht 224, 226.

[60] *See*, Blanc (n 53) 124.

[61] *Schleswig-Holstein* (n 11) para 43.

[62] Opinion of Advocate General Bobek in *Fashion ID* (n 56) paras 91 and 99-101.

if such processing occurs outside an entity's control and knowledge.[63] In the Advocate General's view, in the case of the Facebook 'Like-button', the relevant stage of the processing corresponds to the collection and transmission of personal data, occurring by means of the plugin.[64] In the same vein, Schroers argues for limiting responsibility of joint controllers to joint processing. In the case of a Facebook fan page such as the one at issue in *Wirtschaftsakademie*, she notes that joint processing will likely relate to the collection of data from visitors of the fan-page and to the processing of this data for statistical purposes for Wirtschaftsakademie, but not to the use of the data by Facebook for Facebook's own analysis and advertising unrelated to Wirtschaftsakademie. Wirtschaftsakademie would therefore need to comply with the responsibilities incumbent on a controller with regard to this processing.[65] However, it has been pointed out that this interpretation might not respect the principle of effective and complete protection of data subjects as emphasised in the ECJ's case-law.[66] In that regard, one feasible option would consist in excluding the external liability of individual controllers in cases in which it can objectively be ascertained that a controller, due to a lack of actual decision-making power, is not in a position to comply with certain legal obligations which, in principle, would result from the classification as controller.[67] Such an interpretation is supported by the ECJ's finding in *Google and Google Spain* according to which a data controller must ensure, "*within the framework of its responsibilities, powers and capabilities*", that data processing complies with data protection rules.[68] In other words, *qui habet commoda, ferre debet onera* must be limited to the extent that *ultra-posse nemo obligatur*: while information providers who take advantage of using the services of a platform or embedding a plugin must also bear the burdens resulting therefrom, i.e. (joint) data protection responsibility vis-à-vis the users, they cannot be obligated beyond what they are able to do.[69] This includes, however, that they could be required to cease operating a fan page or embedding a plugin if such a measure is necessary to ensure effective and complete protection of the interests and rights of data subjects.

---

[63] Opinion of Advocate General Bobek in *Fashion ID* (n 56) para 107.

[64] Opinion of Advocate General Bobek in *Fashion ID* (n 56) para 102.

[65] Jessica Schroers, 'The Wirtschaftsakademie Case: Joint Controllership' (*KU Leuven Centre for IT and IP Law*, 14 August 2018) <https://www.law.kuleuven.be/citip/blog/the-wirtschaftsakademie-case-joint-controllership/> accessed 10 October 2019.

[66] Mahieu and others (n 21) 18. The authors refer to a hypothetical cookie notice saying, "*We collect your IP-address and Browser-ID and transfer this personal data to Facebook. We do not know what Facebook does with the data. Click here to accept and proceed*", which evidently would not amount to meaningful transparency in practice.

[67] *See*, Hacker (n 27) 780.

[68] *Google Spain* (n 12) paras 38 and 83; *See*, Mahieu and others (n 21) 19.

[69] *See*, C-115/16 *N Luxembourg 1 and Others v Skatteministeriet* (ECJ, 26 February 2019) para 143.

It is important to note in this context that both the *Wirtschaftsakademie* and *Fashion ID* cases concern the old DPD and the definition of data controller as retained therein. Nonetheless, given that the notion of data controller is identically defined in both the DPD and the new GDPR, it can reasonably be assumed that the Court's interpretation will in principle remain valid in a GDPR context as well. Unlike the DPD, however, the GDPR explicitly addresses the case of joint controllers. Under Article 26(1), where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. In that case, they are obliged to determine, in a transparent manner and by means of an arrangement between them, their respective responsibilities for data protection compliance in particular as regards the exercise of the rights of the data subject and their respective duties to provide information. According to Article 26(2) GDPR, the arrangement chosen shall duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects and its essence shall be made available to the data subject. If joint controllers fail to determine their respective responsibilities by means of an arrangement, they risk administrative fines under Article 83(4)(a) GDPR.[70]

However, what is crucial is that according to Article 26(3) GDPR, irrespective of the terms of the arrangement concluded between joint controllers, data subjects may exercise the rights conferred to them under the GDPR "*in respect of and against each of the controllers*." Moreover, under Article 82(4) GDPR, where more than one controller is involved in the same processing and where they are responsible for any damage caused by processing, "*each controller shall be held liable for the entire damage*" in order to ensure effective compensation of the data subject. Despite this, according to Article 82(5), a controller is entitled to claim back from the other controllers involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage when he has paid full compensation for the damage suffered.[71] The principle of joint and several liability anchored in Article 26(3) and Article 82(4)GDPR appears to be at odds with the Court's statement in *Wirtschaftsakademie* that the existence of joint responsibility does not necessarily imply equal responsibility.[72] It is possible, though, that the latter might be construed as foreshadowing a restrictive interpretation of

[70] Violations may be subject to administrative fines up to 10,000,000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

[71] In response to the ECJ's judgment in *Wirtschaftsakademie*, German data protection authorities were quick to make clear that, as joint controllers, Facebook fan page administrators must take care of compliance with data protection rules in order not to risk regulatory measures, and that it will not suffice to refer to the responsibility of Facebook.

[72] Moos and Rothkegel (n 55) 597.

the two provisions mentioned, which, however, remains to be verified in the ECJ's future case-law.

V. Conclusion

As is evidenced by the recent case-law of the ECJ, Web 2.0 and the emergence of multi-tiered information provider relationships represent specific challenges to data protection law. The ECJ addresses these challenges by interpreting broadly the concept of data controller, with a view to ensuring effective and complete protection of individuals whose personal data is processed. An entity which exerts, to a sufficient degree, influence over the data processed and therefore participates in determining the purposes and means of the data processing can be considered a (joint) data controller, without it being required that that entity has complete access to the data. However, this extensive interpretation gives rise to questions concerning the allocation of responsibility between joint controllers. While the Court has held that joint responsibility does not necessarily imply equal responsibility, it remains to be seen in future case-law how more specific criteria for the practical implementation of this statement are to be defined and reconciled with the principle of joint and several liability of joint controllers as laid down in Article 26(3) and Article 82(4) GDPR. While the currently discussed Indian Personal Data Protection Bill also provides, through the definition of *data fiduciary*, for the possibility of joint data control, it appears that it does not include specific provisions with regard to the legal consequences arising from such a situation. The recent developments in EU data protection law as outlined in this article may offer an occasion to reflect on the opportunity to further develop the draft bill in that sense.