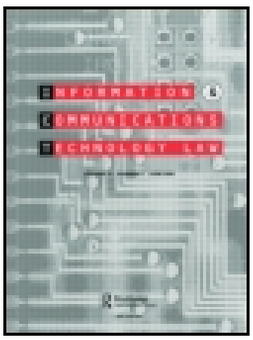

Routledge
Taylor & Francis Group

Information & Communications Technology Law

ISSN: 1360-0834 (Print) 1469-8404 (Online) Journal homepage: https://www.tandfonline.com/loi/cict20

Who controls our data? The legal reasoning of the European Court of Justice in *Wirtschaftsakademie Schleswig-Holstein* and *Tietosuojavaltuutettu v Jehovan todistajat*

Susanna Lindroos-Hovinheimo

To cite this article: Susanna Lindroos-Hovinheimo (2019): Who controls our data? The legal reasoning of the European Court of Justice in *Wirtschaftsakademie Schleswig-Holstein* and *Tietosuojavaltuutettu v Jehovan todistajat*, Information & Communications Technology Law, DOI: 10.1080/13600834.2019.1623447

To link to this article: https://doi.org/10.1080/13600834.2019.1623447

Published online: 25 May 2019.

INFORMATION & COMMUNICATIONS TECHNOLOGY LAW
https://doi.org/10.1080/13600834.2019.1623447

Routledge
Taylor & Francis Group

CASE COMMENT

Who controls our data? The legal reasoning of the European Court of Justice in *Wirtschaftsakademie Schleswig-Holstein* and *Tietosuojavaltuutettu v Jehovan todistajat*

Susanna Lindroos-Hovinheimo

Faculty of Law, University of Helsinki, Helsinki, Finland

ABSTRACT

This paper analyses two judgments from the European Court of Justice. Both were delivered soon after the new Data Protection Regulation became applicable. The argumentation in the judgments provides timely clarification on certain key concepts in European data protection law. As the analysis will show, the ECJ continues its broad interpretation of the parties responsible for data processing. The judgments are generally compatible with the Court's previous case law, which seeks to fill any potential gaps in the protection of individuals' privacy rights. Hence, the aims of data protection rules are predominately interpreted by the Court within a fundamental rights framework. Even though the cases have certain significant differences, the conclusions to be drawn are similar: the argumentation of the Court is focused on data protection throughout. Moreover, the Court emphasises strong protection of personal data in all kinds of situations, even those where other rights could also be relevant.

KEYWORDS

European Court of Justice; general data protection regulation; legal reasoning; privacy rights; processing of personal data; controller; balancing of rights

Introduction

Recent developments in European data protection law cannot have escaped the notice of lawyers, nor indeed the public at large. The General Data Protection Regulation[1] became applicable in late May 2018, and although it does not completely revolutionise the field – as many of the main principles and rules include extensions or clarifications to its preceding Data Protection Directive[2] – the Regulation does also introduce new norms for the protection of individuals' informational privacy.[3]

CONTACT Susanna Lindroos-Hovinheimo susanna.lindroos@helsinki.fi

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

[2]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.

[3]On data protection and privacy generally, see e.g. Federico Ferretti, 'Data Protection and the Legitimate Interest of Data Controllers: Much Ado about Nothing or the Winter of Rights?' (2014) 51 CMLR 843; Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 IDPL 222.

Arguably, the European Court of Justice has played a major role in the development of personal data protection into a proper fundamental right – a right that is enforced in both the private and public sector.[4] For instance, in some prominent cases, the Court has balanced data protection against other rights and consequently strengthened data protection. Other landmark cases have resulted in more thorough definitions of the different actors' duties and responsibilities.

The importance of the ECJ in elucidating the meaning and scope of privacy rights did not end after the hype surrounding the GDPR reached its zenith last May. Indeed, the Court gave two judgments during the summer of 2018 that continue to shape the definition, strength and limits of personal data protection law. The first was the *Wirtschaftsakademie* judgment that the Court delivered in June 2018,[5] which provides some extremely important definitions of the responsibilities of different data processing parties with regard to individuals' rights. The outcome, in a nutshell, is that organisations providing services via a Facebook fan page are co-responsible for the data that is processed by Facebook. Conversely, the social media platform was found to be responsible for (at least some of) the processing it performs at the request of another party. The issue is timely because it concerns the gathering of information with the help of cookies and is thus likely to have an impact on the future ePrivacy Regulation being prepared in Brussels.

The ECJ delivered its second post-GDPR judgment, *Jehovan todistajat*,[6] soon after. Here, the Court was faced with the task of analysing door-to-door data collection by preachers from the Jehovah's Witness Community. This case concerned a more old-fashioned scenario devoid of any complicated technological issues. Nevertheless, here too the case raised difficult questions about data protection and the associated responsibilities.

While the two new decisions differ in some respects and also deal with partly different questions, the general lesson that can be learned from both is that the ECJ takes data protection very seriously. In both cases it sets the tone for GDPR interpretation in a privacy-friendly key.

Before examining the Court's reasoning in these cases, a few general words might be helpful on the interpretation of the old DPD as well as the current GDPR. As is well-established in EU legal scholarship, the EU forms a legal system *sui generis*, and its interpretation, as performed by the EU Courts, follows its own logic.[7] In order to predict the outcome of a specific case – following the aims of legal research established by the realist schools – it is thus necessary to understand the methods of reasoning utilised by the ECJ. In the ECJ's case law, contextual, teleological and systemic arguments tend to rank higher than

[4]See e.g. *Österreichischer Rundfunk and Others* (C-465/00, C-138/01 and C-139/01, EU:C:2003:294); *Google Spain and Google* (C-131/12, EU:C:2014:317); *Ryneš* (C-212/13, EU:C:2014:2428); *Schrems* (C-362/14, EU:C:2015:650); *Manni* (C-398/15, EU:C:2017:197). On the development of the right to personal data protection in the EU, see Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer, 2014).

[5]*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* (C-210/16, EU:C:2018:388). The judgment can be found here: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CJ0210>. For the German proceedings, see Beschluss vom 25.02.2016 – BVerwG 1 C 28.14, ECLI:DE:BVerwG:2016:250216B1C28.14.0.

[6]*Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta* (C-25/17, EU:C:2018:551). The judgment can be found here: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1557832755134&uri=CELEX:62017CJ0025>. For the Finnish proceedings, see KHO:2016:208, ECLI:FI:KHO:2016:208 and KHO:2018:171, ECLI:FI:KHO:2018:171.

[7]See e.g. Joxerramon Bengoetxea, *The Legal Reasoning of the European Court of Justice – Towards a European Jurisprudence* (Clarendon Press, 1993); Gunnar Beck, *The Legal Reasoning of the Court of Justice of the EU* (Hart Publishing, 2012); Suvi Sankari, *European Court of Justice Legal Reasoning in Context* (Europa Law Publishing, 2013).

semantic ones.[8] Hence, when interpreting data protection rules, it is critical to determine the context, as well as the *telos,* of the legal instrument being interpreted.

What, then, is the context here?[9] In terms of primary law, the most evident context for data protection is fundamental rights protection. Both Article 16 of the Treaty on the Functioning of the European Union and Article 8 of the Charter of Fundamental rights include the principle of data protection. Secondary law, such as the DPD and now the GDPR, add detailed provisions on the protection of a right that is expressed in primary law.[10] The ECJ has held that the provisions of the DPD and now the GDPR must necessarily be interpreted in the light of the fundamental rights guaranteed by the Charter.[11] Hence it is the Charter, and especially the fundamental right to private life, that guides interpretation.

The context and the purpose of the instruments have repeatedly been expressed by the ECJ as leading interpretational principles. During the time of the Directive, the Court announced that 'according to settled case-law of the Court, the provisions of a directive must be interpreted in the light of the aims pursued by the directive and the system which it establishes'.[12] This statement has recently been repeated by the Court in, for instance, the Buivids judgment from 2019.[13]

The purpose or *telos* of data protection is, however, a tricky question. Arguably, it is this issue that lies at the heart of some of the most difficult interpretation situations concerning the Directive and the Regulation. Generally, when legal rules are unclear, or their applicability with regards to the facts of the case is uncertain, the aim of the rules can help guide the interpreter towards a sound interpretation. If the context is fundamental rights protection, it would be reasonable to define the *telos* accordingly. However, the GDPR (just like the DPD) has *two* explicit aims: to protect individuals' right to the protection of personal data *and* to ensure the free flow of data and thus promote the functioning of the internal market. The tension between these two causes what Orla Lynskey has called the 'split personality' of data protection regulation.[14]

The ECJ has nevertheless eased the burden of legal decision-makers somewhat by developing case law in a coherent and mostly predictable way. It has made choices that can, at times, been seen as creative, but have nevertheless clarified the law and increased legal certainty. This it has done by focusing on the context – data protection seen as a fundamental right – and thereby prioritising the *telos* of protecting individuals'

[8]Koen Lenaerts and Jose A Gutierrez-Fons, 'To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice' (2014) 20 CJEL 3; Elina Paunio and Susanna Lindroos-Hovinheimo, 'Taking Language Seriously: An Analysis of Linguistic Reasoning and Its Implications in EU Law' (2010) ELJ 395.

[9]Contexts are notoriously difficult to define, but it is possible to argue for the choice of one primary context over another. On the indeterminacy of contexts, see e.g. Jacques Derrida, *Limited Inc.* (Northwestern University Press, 1988).

[10]See Hielke Hijmans, *The European Union as Guardian of Internet Privacy – The Story of Art 16 TFEU* (Springer, 2016), 66. According to Hijmans, the right to privacy represents a normative value, whereas the right to data protection includes a legal structure that enables individuals to claim that data should be processed fairly and lawfully. Hence privacy may be understood as a principle-based right and data protection as a rule-based right. For a critique of current data protection law, see Audrey Guinchard, who has recently argued that the ECJ has not been successful in its proportionality analyses. Audrey Guinchard, 'Taking Proportionality Seriously: The Use of Contextual Integrity for a More Informed and Transparent Analysis in EU Data Protection Law' (2018) ELJ 434.

[11]See judgments in *Österreichischer Rundfunk and Others* (C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 68); *Google Spain and Google* (C-131/12, EU:C:2014:317, paragraph 68); and *Ryneš* (C-212/13, EU:C:2014:2428, paragraph 29).

[12]*Satakunnan Markkinapörssi and Satamedia* (C-73/07, EU:C:2008:727, paragraph 51).

[13]*Sergejs Buivids v. Datu valsts inspekcija* (C-345/17, EU:C:2019:131, paragraph 49).

[14]Orla Lynskey, 'From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis' in Serge Gutwirth, Ronald Leenes, Paul de Hert and Yves Poullet (eds), *European Data Protection: Coming of Age* (Springer, 2013) 59–84.

data rights over free flow of data. This is the background against which the two cases in this annotation become understandable.

Balancing cases and definitions cases

The judgments in both *Jehovan todistajat* and *Wirtschaftsakademie* are likely to prove significant for future application of data protection rules, even though they still concern the old Directive. Both deal in their respective ways with the definition of the 'controller', who is the entity responsible for ensuring that data protection rules are followed.[15] However, the way personal data is gathered, processed and stored is different in the two cases, as are many other facts.

The architecture of the DPD was similar in many ways to the Regulation now applicable: in order for the rules of data protection to apply, the situation must be of a certain kind. First, the data being processed must be personal data. Personal data is any data by which an individual person is, or can be, identified. Second, the processing of such data, i.e. collection, storage, movement or even deletion, can only be performed on certain conditions and in certain ways laid down by the Regulation (and the previous Directive). Moreover, it is necessary in every data processing situation to ascertain which party bears the main burden for ensuring that individuals' personal data is protected.

The parties handling personal data can occupy the role of a controller, which is the technical term for the party who bears the main responsibility for ensuring data protection. However, they can also occupy the role of a processor, who is responsible in a more limited capacity. The definition of these roles is key to understanding data protection rules, and hence it needs to be clear in the myriad of forms in which personal data is collected, stored, used, sold, exchanged, and deleted in various technological situations. Nevertheless, the wording of the Directive, as well as the Regulation, has arguably been insufficiently clear and comprehensive to provide a full picture of how these roles are to be understood. Hence the two judgments from 2018 add much needed clarification.

The analysis presented in this case annotation utilises a classification instrument that divides ECJ data protection into two main types. The typology is meant as a simple heuristic tool that can be helpful for understanding the Court's reasoning in privacy and data protection law. The two main types of cases are definitions cases, on the one hand, and balancing cases, on the other.

Several previous judgments, such as the early but significant *Lindqvist*[16] and the more tech-related *Breyer*,[17] can be read as definitions cases. Furthermore, *Digital Rights Ireland*[18] also falls into this general category. In such cases, I argue, the main issues that the Court decides to consider are definitional. In these judgments, the Court considers the central problems of the case to be uncertainties about the meaning of specific concepts in the Directive or the correct understanding of the rules on scope and applicability. Hence, in

[15]The question of who should carry the responsibility for data protection in complex networks of data flows is extremely significant also because the GDPR introduced a system of administrative fines that can be severe. It will become increasingly important to be able to define who the liable party is when data protection breaches are considered.
[16]*Criminal proceedings against Bodil Lindqvist* (C-101/01, EU:C:2003:596).
[17]*Patrick Breyer v Bundesrepublik Deutschland* (C-582/14, EU:C:2016:779).
[18]*Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (Joined Cases C-293/12 and C-594/12, EU:C:2014:238).

definitions cases judgments usually aim to add clarification on the interpretation of specific articles in the Directive.

Balancing cases, on the other hand, are cases where the ECJ clearly recognises the need to balance data protection (and sometimes privacy more generally) against other rights and freedoms.[19] In these judgments, the main focus of the Court's argumentation is not the classification, interpretation and clarification of legal texts, but rather the evaluation of the appropriate strength of privacy rights compared to other rights and values.[20] *Google Spain*[21] is a prime example of a balancing case, even though the judgment also defines certain aspects of controllership. In *Google Spain*, the central question was whether a person's right to be forgotten could override the public's right to information, a clear balancing exercise where privacy was ultimately considered to outweigh other concerns. Another example of a rather straight-forward balancing case is *Bavarian Lager*,[22] where the Court compared the interests of privacy against transparency.

With this background in mind, let us examine the two judgments, beginning with the first, *Wirtscahftsakademie Schleswig-Holstein*.

Wirtschaftsakademie: processing of personal data on Facebook fan pages

Judgment was delivered in the Grand Chamber on 5 June 2018. The main issue in the case concerns the distribution of responsibility to ensure data protection in a situation where many different actors participate in the data's processing. The case came to the Court as a request for a preliminary ruling by the German Bundesverwaltungsgericht in 2016.

The main rule on controllership is simple: the controller is the party who decides how processing is performed. According to Article 4 of the Regulation, 'controller' means 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. Note, of particular relevance to the case at hand is that the controller may operate 'alone or jointly with others'.

The controller can, moreover, decide to outsource processing activities to other parties. In such instances, these parties are called processors. According to Article 4, 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. From this definition, it follows that a processor acts in accordance with the orders of the controller. If processors were to perform their own independent data processing as well, they would become controllers.

It is vital to discern the roles in which each party operates because it is the controller who bears a larger part of the responsibility for ensuring that personal data is protected. This is emphasised throughout the GDPR but is especially evident in Article 24, which defines the responsibility of the controller. The protection of individuals' privacy is

[19]See also the intriguing discussion on balancing in data protection law that was published in the European Data Protection Law Review. Raphael Gellert, 'On Risk, Balancing, and Data Protection: A Response to van der Sloot' (2017) 3 EDPL 180; Bart van der Sloot, 'Ten Questions about Balancing' (2017) 3 EDPL 187.

[20]Occasionally these cases also revolve around the idea of the essence of rights. An example is *Schrems v Data Protection Commissioner* (C-362/14, EU:C:2015:650). For analysis, see e.g. Maja Brkan, 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core' (2018) 14 EuConst 332.

[21]*Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (C-131/12, EU:C:2014:317).

[22]*European Commission v The Bavarian Lager Co. Ltd* (C-28/08 P, EU:C:2010:378).

constructed in such a manner that the person ('data subject') and the controller form the primary relationship that data protection rules are intended to regulate.[23] This idea is prominent throughout data protection law.

The main rules concerning the responsibilities of controllers and processors are relatively clear in both the Directive and the Regulation, but the same cannot be said of real-life situations. Today, data processing often occurs in highly complex and (for lawyers at least) technologically obscure networks, where a large number of operators do various things with the data. EU legislation recognises that there may be situations where data is processed by many controllers and processors simultaneously. Nonetheless, the legal definition and classification of such labyrinthine data flows is challenging, and it is for this purpose that the Court's decision in *Wirtschaftsakademie* is useful.

The parties in the German proceedings were the data protection authority of Schleswig-Holstein and the private company Wirtschaftsakademie Schleswig-Holstein. The company's Facebook fan page offered educational services, but neither Wirtschaftsakademie nor Facebook informed visitors to the page that Facebook, by means of cookies, collected and subsequently processed personal data concerning them. Wirtschaftsakademie nonetheless argued that it was not responsible for the processing performed by Facebook. The dispute found its way to the Bundesverwaltungsgericht (Federal Administrative Court), which decided to refer several questions to the EU Court for a preliminary ruling.

Advocate General Bot, when considering the case, focused on the fact that cookies were used in the data processing. Hence, at the beginning of his opinion, he located the case in a particular context:

> The background to the present case is the phenomenon known as 'web tracking', which consists in the observation and analysis of the behaviour of Internet users for commercial and marketing purposes. Web tracking helps identify the centres of interest of Internet users, through observation of their browsing habits. This is referred to as behavioural web tracking and it is usually carried out with the aid of cookies.[24]

The Advocate General observed that web tracking was not completely prohibited by the Directive. Nevertheless, the collection of user information for statistics and marketing purposes needed to fulfil certain conditions in order to be compatible with the Directive. The Advocate General drew the clear conclusion that this kind of data processing was forbidden unless the data subject provided consent.[25] The new Regulation does not introduce differences in this matter, although it does include more definition on the criteria for consent.

According to the Advocate General, the next step in the decision of the case was to identify the controller.[26] The questions that were referred to the ECJ presupposed that Wirtschaftskademie *was not* the controller for the operations performed by Facebook. The Advocate General, however, disagreed with this. His interpretation, which has significant ramifications for future application of data protection law, was that Wirtschaftsakademie and Facebook should be regarded as *mutually responsible* for the protection of data: 'Wirtschaftsakademie must, in my opinion, be regarded as jointly responsible for the phase

[23]Also the processor has responsibility for its own operations, as stated in for instance Article 28 of the GDPR.
[24]Opinion of Advocate General Bot delivered on 24 October 2017, paragraph 4. The opinion can be found here: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1557832820808&uri=CELEX:62016CC0210>.
[25]Opinion of Advocate General Bot delivered on 24 October 2017, paragraph 9.
[26]ibid, paragraph 11.

of the data processing which consists in the collection by Facebook of personal data'.[27] This interpretation may seem rather radical given the Advocate General's acknowledgement that Wirtschaftsakademie was primarily a user of Facebook – a fan page administrator. Nevertheless, he concluded that such a fan page administrator can also be regarded as responsible for collection of personal data performed by Facebook.[28]

The Advocate General thus argued for a broad definition of the concept of 'controller', the most important reason being that such a broad definition would ensure effective and complete protection of data subjects. Here the context and the *telos* of data protection law were mobilised. In deciding which party or parties are controllers of data processing, it was thus necessary to consider why and how data was processed. Moreover, the decisive factor was not any possible agreement between the two companies; rather, it was the actual roles of the parties. The administrator of a fan page played a predominant role in determining how data was processed by Facebook. It participated in determining the means and purposes of the data processing and therefore had *de facto* influence over it. Also, the idea that both parties were controllers was supported by the fact that Wirtschaftsakademie and Facebook pursued closely related objectives. Wirtschaftsakademie wished to obtain statistics that required the processing of personal data, and that same data processing also enabled Facebook to target the advertising that it publishes on its network.[29]

The conclusion was that both companies shared responsibility for the data processing performed by Facebook. However, the Advocate General nonetheless observed that 'the existence of shared responsibility does not imply equal responsibility. On the contrary, the various controllers may be involved in the processing of personal data at different stages and to differing degrees'.[30] This point is significant and may prove especially important in future cases.

Judgment: Wirtschaftsakademie and Facebook are both responsible for processing

The Advocate General's opinion may be seen as a clear indication of a teleological interpretation. He emphasises the aim of protecting individuals' personal data, which is the primary purpose of the Directive as well as the Regulation. In so doing, he follows earlier interpretations of the Court. Hence, his reasoning also reveals an attempt to add coherence to a rapidly evolving area of EU law. There is, however, little balancing to be seen in the Advocate General's opinion. The definition of controllership is developed explicitly to ensure the protection of individuals.

The Court agreed with the Advocate General on most issues. However, it began by defining the context of the case as explicitly that of fundamental rights protection. Where the Advocate General had begun his opinion with a discussion of cookies, the Court commenced its analysis by arguing that fundamental rights and freedoms were at the heart of the case:

[27]ibid, paragraph 42.
[28]ibid, paragraph 53.
[29]ibid, paragraphs 53–60.
[30]ibid, paragraph 75.

> [I]t must be recalled that, as is apparent from Article 1(1) and recital 10 of Directive 95/46, the directive aims to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data.[31]

As for the responsibility of the two companies, the Court agreed with the Advocate General: they were jointly responsible. The fact that an administrator of a fan page uses a platform provided by Facebook in order to benefit from its services did not exempt the administrator from its obligations to ensure the protection of personal data. The Court also noted in passing that fan pages hosted on Facebook could also be visited by non-Facebook users without a user account on that social network. In such instances, the fan page administrator's responsibility for the processing of personal data may be even greater, as merely visiting the homepage automatically triggers the processing of their personal data.

The Court concluded, as did the Advocate General, that the existence of joint responsibility does not necessarily imply equal responsibility. Both operators may be responsible, but in different ways and to different degrees because the

> 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.[32]

In the reasoning of the Court, the strongest argument for the conclusion of joint responsibility was that it ensured complete protection of rights, the idea being that if both operators were not considered responsible in such a situation, gaps might appear in the protection of individuals' rights and freedoms. Hence the broad definitions of controller, as well as the broad application of joint controllership, advance the *telos* of strong protection of natural persons' data.

Analysis

Following the typology above, it is evident that *Wirtschaftsakademie* is predominantly a definitions case, as very little balancing occurred in the Court's reasoning. The Court's analysis was first conceptualised with the clear purpose of protecting data subjects' rights, and the definition of the various operators' roles and responsibilities was made within that framework. Nonetheless, even though the case can be classed as a definitions case, it is by no means insignificant. On the contrary, through its definitions of key concepts, the Court drew important lines that affect the legal relationship of individuals, companies and social media service providers. However, if the Court had considered the balancing of individuals' rights against the interests of the operators, its reasoning could have been even more helpful for data protection lawyers. As such, it is still unclear when and how operators' interests may override any of the personal data rights established by the Directive and the Regulation.

The case is particularly topical because it concerns cookies, on which there are few authoritative interpretations in EU law.[33] Moreover, as the ePrivacy rules are currently

[31] Judgment, paragraph 26.
[32] ibid, paragraph 43.
[33] See, however, Article 29 Working Party, Opinion 2/2010 on online behavioural advertising, adopted on 22 June 2010; Article 29 Working Party, Opinion 01/2017 on the proposed e-Privacy Regulation, adopted on 4 April 2017; European

being revised, the Court's stand may have a significant effect on future legislation. Indeed, such a development is by no means foreign to this field of law. For instance, in *Google Spain*, the Court considered the right to be forgotten, which had yet to be codified, and ultimately held that the right did enjoy protection in the Union. Shortly afterwards, the new Regulation was passed with said right expressed in Article 17.

The Court's reasoning in *Wirtschaftsakademie Schleswig Holstein* is not particularly extensive.[34] Instead, the judgment is concise and the analysis follows a clear and logical form. It conforms to the Advocate General's views on many points. As such, the judgment helps clarify the way the concept of 'controller' and the idea of joint controllership should be understood in future cases, and the result is satisfying both in this respect and because of the direction in which it continues to develop data protection law in Europe. In this judgment, as in many preceding it, data subjects' fundamental right to informational privacy is the compass by which data processing rules are to be navigated.

Both the Advocate General and the Court itself began their reasoning by defining the context of the case. The context then led to the choice and definition of the legal issues to be solved. Only some of the questions posed to the Court were discussed in detail, and the Court also disagreed with the referring court's understanding of the roles of the operators. Through these choices, the Court delivered a judgment on the issues that it deemed important. In this sense, the case displays creative reasoning.

The judgment is relevant in the light of current political pressures. Facebook – and social media giants more generally – are sometimes seen as the most pressing privacy threat, occasionally with good reason. Scandal after scandal seem to show that these companies cannot be trusted and should be strongly regulated. Nevertheless, the Court seems relatively immune to such fears, as it clearly stated that Facebook was not to be held solely responsible for the data that it processed. Instead, companies that use Facebook's services are also liable for the data processing that Facebook performs.

At the time of writing, another similar case is pending before the ECJ.[35] Here, a German court has requested a preliminary ruling on, inter alia, the definition of controllership. The issue concerns Fashion ID, an online retailer which embedded Facebook's 'Like' button on its website. As a result, when a user visits the Fashion ID website, information about that user's IP address and browser string is transferred to Facebook. This transfer occurs regardless of whether the user has clicked 'Like' or whether the user even possesses a Facebook account. The central question of the case concerns which party should be considered the controller in this scenario, Facebook or Fashion ID.

In December 2018, Advocate General Bobek issued his opinion on the matter: Fashion ID should be seen as a controller for the collection and transmission of users' personal data. However, the company's (joint) responsibility should be limited to those operations for which it effectively co-decides on the means and purposes of the processing of the personal data.[36] When issuing his opinion, the Advocate General referred to

Data Protection Board, Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications, 2018.

[34]For analysis, see also Nicolas Blanc, 'Wirtschaftsakademie Schleswig-Holstein: Towards a Joint Responsibility of Facebook Fan Page Administrators for Infringements to European Data Protection Law' (2018) 4 EDPL 120.

[35]*Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V. joined parties: Facebook Ireland Limited, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen* (Case C-40/17).

[36]Opinion of Advocate General Bobek delivered on 19 December 2018, paragraph 142. The opinion can be found here: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1557832951095&uri=CELEX:62017CC0040>.

Wirtschaftsakademie Schleswig-Holstein several times. For instance, according to him, the Court's statement that joint responsibility did not necessarily imply equal responsibility of the various operators involved in the processing of personal data suggested the need to limit the liability of a (joint) controller.[37] The Advocate General also raised the concern that under the new system of joint liability introduced in Article 26 of the GDPR, it might be difficult to envisage how joint responsibility could imply non-equal responsibility.[38] Nonetheless, as methods are required to limit the responsibility of the controllers, the AG continued by considering the two key elements that comprise the definition of controller: means and purpose. The result is a step-by-step tool for analysing processing situations and thereby resolving the issue of which party or parties should be regarded as controllers and how much responsibility each of them should bear.[39]

> I consider that the liability of the Defendant (Fashion ID) has to be limited to the stage of the data processing in which it is engaged and that it cannot spill over into any potential subsequent stages of data processing, if such processing occurs outside the control and, it would appear, also without the knowledge of the Defendant.[40]

What is also interesting in the Advocate General's opinion is that he explicitly calls for the balancing of rights and interests when applying data protection rules. He argues that in order to assess the legitimacy of data processing, as set out in Article 7(f) of Directive 95/46, the legitimate interests of both joint controllers must be taken into account and balanced against the rights of the data subjects.[41] Here the opinion continues the Court's practice of using data subjects' rights as the yardstick for legitimacy. However, those rights are not seen to automatically override the interests of the controllers.

Jehovan todistajat: are religious communities exempt from data protection regulation?

In the following, I will discuss the *Jehovan todistajat* judgment, which is also a Grand Chamber decision. The main issue is very similar to that of *Wirtschaftsakademie*: the scope of protection of personal data and the actors responsible for that protection. In its decision, the Court also took a stand on certain procedural issues that may be of interest to experts on EU procedural law. They are, however, not the focus of this commentary and will not be discussed in detail.

The case concerns Jehovah's Witnesses, a religious community that preaches door-to-door. Members of the community gather notes about the individuals that they have visited, with the data consisting, among other things, of the names and addresses of those contacted as well as information concerning their religious beliefs and their family circumstances. This information is collected as a memory aid and is stored in order to be retrieved for another visit. This is done without the knowledge or the consent of the persons concerned.

The religious community was the defendant in the case, whose main proceedings took place in Finland. The national Data Protection Supervisor (Tietosuojavaltuutettu) was the

[37]Opinion of Advocate General Bobek delivered on 19 December 2018, paragraph 94.
[38]ibid, paragraph 96.
[39]ibid, paragraph 102.
[40]ibid, paragraph 107.
[41]ibid, paragraphs 125–127.

applicant. According to the referring court, the case required consideration of both the rights to privacy and personal data protection and also freedom of religion and association as guaranteed by the Charter and the European Convention for the Protection of Human Rights and Fundamental Freedoms and by the Finnish Constitution. In its decision, however, the ECJ paid little attention to freedom of religion.

The first two questions concerned the scope of application of the Data Protection Directive. Of particular relevance was whether the activity of door-to-door preaching could be considered a purely personal or household activity and thereby outside the scope of application of the Directive. Such a household exemption is also included in the new Regulation. In turn, questions three and four, which were relevant if the Directive was to be applied, concerned the definition of controller, as the referring court was unsure whether the Jehovah's Witnesses Community should be regarded as a controller at all.

Judgment: preachers and the community are both responsible for processing

According to the so-called household exemption in Article 3(2) of the Directive, the Directive does not apply to the processing of personal data performed by a natural person in the course of a purely personal or household activity. Hence, if the data collection performed by the Jehovah's Witnesses Community or its preachers had been seen as a purely personal activity, as suggested by the defendant, the data protection rules in the Directive would not have applied at all.[42] Here, the religious circumstances of the case make it particular, as, in effect, the ECJ had to decide whether the fact that the data had been collected in a *preaching situation* was relevant.

The ECJ noted that personal data was collected by members of the Jehovah's Witnesses Community with the intention of spreading the faith. Therefore, data collection from preaching door-to-door occurred outside the private setting of the community. Furthermore, according to the facts of the case before the Court, some of the data collected by the members of the community was sent to the congregations, which compiled lists of persons who no longer wished to receive visits. Thus, the Court observed that in the course of their preaching, community members had made at least some of the data collected accessible to a potentially unlimited number of persons.[43] In other words, the data had not remained within any household.

The Court also stated that although door-to-door preaching activities were protected by Article 10(1) of the Charter as an expression of faith, this did not imply that the activity had an exclusively personal or household character.[44] Thus, the Court concluded that the household exemption did not apply in the case.[45]

On the basis of this reasoning, as well as on certain more technical considerations concerning the way the community had filed the data, the Court held that the Directive

[42]The defining case for interpreting the household exemption is *Lindqvist* from 2003. Advocate General Mengozzi engages in an interesting comparison between the *Lindqvist* case and *Jehovan todistajat*. By coincidence, also *Lindqvist* happened to have a religious connection. See Opinion of Advocate General Mengozzi delivered on 1 February 2018. The opinion can be found here: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1557833027967&uri=CELEX:62017CC0025>.

[43]Judgment, paragraphs 44–45.

[44]ibid, paragraph 49. Advocate General Mengozzi points out that recital 165 of the GDPR implies that religious communities are subject to data protection rules in the same manner as any other controllers. Opinion of Advocate General Mengozzi delivered on 1 February 2018, paragraph 34.

[45]Judgment, paragraph 51.

applied to the activities of the Jehovah's Witnesses. Therefore all the data protection rules and principles of the Directive needed to be respected in regard to their data processing activities. However, the Court still needed to decide which party was responsible for data processing. The religious community claimed that only individual members who engaged in preaching had access to the data that they gathered.

The Court's argumentation centred on whether the Jehovah's Witnesses Community could be considered a controller only in case it had taken specific measures, such as the issuing of written instructions or orders about the collection of data. Here, the answer was no. The community was assigned controller status because the purpose of door-to-door preaching was to achieve the aims of the community. Moreover, the Court paid attention to the fact that preaching was *de facto* organised, coordinated and encouraged by the community.[46] Thus, whether the community had provided members with specific guidelines or orders was not decisive.

Here, the Court referred to *Wirtschaftsakademie Schleswig-Holstein* and repeated the formula developed there: through a broad definition of the concept of 'controller', effective and complete protection of persons can be ensured. This functional interpretation of controller status quite naturally led to the conclusion that both the community and the members were to be regarded as controllers and thus jointly responsible for the processing of data. While leaving the referring court to verify the specific circumstances, the Court ultimately held that a religious community was a controller jointly with its members who engage in preaching door-to-door if the community encouraged, coordinated and organised the activity, even if the community did not have access to the data.[47] Joint responsibility, however, does not necessarily imply equal responsibility. Thus in this case too, it was necessary to assess the level of responsibility of each party with regard to all the relevant circumstances.[48]

Analysis

According to the definitions versus balancing typology, it seems clear that *Jehovan todistajat* is a rather clear-cut definitions case. This is remarkable for two reasons: firstly, there were no difficult technological solutions for the Court to entangle, only notes made with pen and paper; it was not a complex, high-profile platform capitalism case. Nevertheless, the case demonstrated that challenging personal data protection issues can arise in quite mundane circumstances. The Court apparently thought it necessary to deliver a well-argued decision – in Grand Chamber no less – on what data protection law required in the situation.

Secondly, it is worth noting that the case *could have become a balancing case* if the Court had so wished. As it was, the judgment contained little discussion on freedom of thought, conscience or religion, as defined in Article 10 of the Charter. Nor was the Court overly concerned with the autonomy of religious organisations, which is protected under Article 17 TFEU. The Court did mention, in passing, that a religious community's responsibility as a controller could not be challenged by appealing to the principle of the organisational autonomy of religious communities. This is because the universal

[46]ibid, paragraphs 70–71.
[47]ibid, paragraphs 73 and 75.
[48]ibid, paragraphs 66–67.

obligation to comply with EU law on the protection of personal data cannot be regarded as interference in the organisational autonomy of such communities.[49] Still, the Court placed little importance on whether data is processed in relation to religious activities; data protection rules apply just as they would in any other situation. Consequently, no real balancing between data protection and religious rights occurred in the Court's ruling.

The Court did not, for instance, consider whether the promulgation or maintenance of a faith or religious belief was hindered by the need of all religious communities and preachers to comply with data protection rules – such considerations seemed more or less irrelevant in the eyes of the Court. This is noteworthy because it demonstrates the strong protection currently enjoyed by privacy rights in the Union. Thus, even though the GDPR does not apply to every activity, its scope is very extensive.

This judgment continues the Court's previous line of reasoning, upheld by legislators when drafting the GDPR, that the context in which data processing occurs – be it for commercial or other purposes – plays a very minor role. Indeed, in this case, one could argue that the Court's argumentation would have been little different if the controllers had been companies or any other kind of organisations. Hence the Court solidified existing data protection rules by delivering a judgment that was consistent with previous interpretations. Consequently, the judgment can be seen to add legal certainty. Nonetheless, the reasoning of the Court fails to address a number of matters. For instance, by not engaging in a rigorous balancing of rights, which this case invited the Court to do, the Court avoided the most difficult issue: how far does the Directive and now the Regulation take data protection? And how should the aim of data protection be balanced with other interests and other rights?

Jehovan todistajat is an intriguing case because it includes a conflict between *two rights to private life*: the right to religious freedom (or the freedom of religious organisations to operate), and the right to protection of personal data. Without engaging in in-depth argumentation, the Court held that religious freedom was still protected in the EU and was not infringed upon by the requirement that religious communities process data in accordance with data protection rules. Such an interpretation is by no means the only possible one. However, it clearly demonstrates the strength of the far more recent privacy right, the right to protection of personal data. We may conclude that even if this were a balancing case, it would not necessarily involve one right being weighed against another; instead, it could equally involve the collision of one aspect of a right with another aspect of the same right. And in the EU today, it is very likely that if one of these aspects is personal data protection, the Court tends to deem it the strongest.

Concluding remarks

The general trend in EU law points towards tougher privacy protection, and this is nothing new. The ECJ has been one of the main players in this development, although certainly not the only one. In both *Wirtschaftsakademie Schleswig Holstein* and *Tietosuojavaltuutettu v Jehovan todistajat*, it upheld its previous interpretations and continued on an already established route. The judgments themselves are therefore unsurprising. Nevertheless, their predictability in a situation where the law has recently changed is a reason to consider them noteworthy.

[49]ibid, paragraphs 74.

All the DPD definitions upon which the Court has delivered judgments have tended to be broad, and these new judgments are no exception. 'Personal data' and 'controller' are just a few of the concepts that are defined in broad terms, thereby granting data protection rules a very wide scope. This line of interpretation has been palpable for quite some time now, and, for that reason alone, the outcome of these cases is predictable. Furthermore, in the *Jehovan todistajat* judgment, the Court also continued its habit of narrowly interpreting exceptions, in this instance the household exemption.

Both cases indicate that a clear need existed for clarification of the main definitions of data protection law, and the main issue at stake is indeed important: the scope of the protection of personal data and who is responsible for it. When read together, these judgments clarify the law a great deal, and in their wake it is also clear that privacy is a strong fundamental right whose protection encompasses most areas of life.[50]

However, in the hands of the Court, both cases became predominantly focused on definitions. Hence the judgments were able to avoid the most difficult issues in EU data protection law, the hardest of which is how to balance individuals' right to data protection with other rights and with the second purpose of data protection: the free flow of data.[51] In both cases, context and *telos* became significant in the reasoning of the Court, and both pointed in the same direction: ensuring that individuals' personal data rights are protected. When the cases were framed this way, the question of controllership became the question of who should be defined as the controller in order for fundamental rights protection to be achieved.

We see that the framing of a case is important for the outcome of ECJ judgments. These two cases became definitions cases and were solved accordingly. My argument is not that clarification and definition of data protection rules would not be valuable, they certainly are, but both cases offered the Court a possibility to do more. Some degree of balancing would have been helpful for the further development of European privacy law.

Disclosure statement

No potential conflict of interest was reported by the author.

Funding

This work was supported by the University of Helsinki Research Grants project funding for *Reconfiguring Privacy – The Political Foundations of Privacy Regulation 2017–2019*.

[50] Bilyana Petkova's understanding of privacy as a leading right in the EU is indeed compelling. Bilyana Petkova, 'Privacy as Europe's First Amendment' (2019) 25 ELJ 140.

[51] A reference to H.L.A Hart's and Ronald Dworkin's differences comes to mind. Where Hart sees the law as comprising of rules, Dworkin recognises also principles as a part of modern law. Principles, however, require balancing. It is not the case that interpreting and applying a rule would be easier than balancing principles, but it is different. And Dworkin does have a point in saying that principles are often needed in order to solve hard cases because these are often the kinds of cases where rules are not enough. In the two annotated cases, defining data protection rules was done but not the balancing of rights and freedoms.