Provisional text

OPINION OF ADVOCATE GENERAL
BOBEK
delivered on 19 December 2018(1)

Case C-40/17

Fashion ID GmbH & Co. KG
v
Verbraucherzentrale NRW e.V.
joined parties:
Facebook Ireland Limited,
Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

(Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany))

(Reference for a preliminary ruling — Directive 95/46/EC — Protection of personal data of website users — Standing of a consumer protection association to bring a claim — Liability of a website operator — Transfer of personal data to a third party — Embedded plug-in — Facebook 'Like' button — Legitimate interests — Consent of the data subject — Duty to provide information)

I. Introduction

1. Fashion ID GmbH & Co. KG is an online retailer which sells fashion items. It embedded a plug-in in its website: Facebook's 'Like' button. As a result, when a user lands on Fashion ID's website, information about that user's IP address and browser string is transferred to Facebook. That transfer occurs automatically when Fashion ID's website has loaded, irrespective of whether the user has clicked on the 'Like' button and whether or not he has a Facebook account.

2. Verbraucherzentrale NRW e.V, a German consumer protection association, brought legal proceedings for an injunction against Fashion ID on the ground that the use of that plug-in results in a breach of data protection legislation.

3. Seised of the case, the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany), seeks the interpretation of several provisions of Directive 95/46/EC ('Directive 95/46'). (2) As a preliminary issue, the referring court enquires whether that directive allows national legislation to grant standing to a consumer association to bring a claim such as the one in this case. Turning to the substance,

the core question posed is whether Fashion ID must be classified as a 'controller' with regard to the data processing taking place, and if so, how exactly are the individual obligations imposed by Directive 95/46 to be met in such a scenario. Whose legitimate interests are to be considered under the balancing exercise required by Article 7(f) of Directive 95/46? Does Fashion ID have a duty to inform data subjects about the processing? And is it also Fashion ID that must collect the informed consent of data subjects in this respect?

II. Legal framework

A. EU law

Directive 95/46

4. The objective of Directive 95/46 is set out in its first article. The first paragraph of that article reads: 'Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data'. Pursuant to paragraph 2 of the same provision, 'Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1'.

5. Article 2 contains the following definitions:

'(a) "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

…

(d) "controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

…

(h) "the data subject's consent" shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.'

6. Article 7 provides criteria that must be met for data processing to be legitimate: 'Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

…

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by

the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).'

7. Article 10 sets out the minimum information that must be provided to the data subject:

'Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such as

the recipients or categories of recipients of the data,

– whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,

– the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.'

8. Chapter III of Directive 95/46 concerns judicial remedies, liability and sanctions. Articles 22 to 24 contained therein provide as follows:

'Article 22

Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23

Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24

Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.'

B. German law

Gesetz gegen den unlauteren Wettbewerb

9. Paragraph 3(1) of the Gesetz gegen den unlauteren Wettbewerb (Law against unfair competition) ('the UWG') provides that unlawful commercial practices shall be prohibited.

10. Paragraph 8(1) and (3) (3) of the UWG sets out that a commercial practice which is unlawful may give rise to an order to cease and desist, or a prohibition order applied for by 'qualified entities' listed in the *Unterlassungsklagengesetz* (Law on Injunctions) or on the European Commission's list, pursuant to Article 4(3) of Directive 2009/22/EC on injunctions for the protection of consumers' interests. (3)

Unterlassungsklagengesetz

11. Paragraph 2(1) and (2) (11) of the Unterlassungsklagengesetz (Law on Injunctions) provides:

'(1) Any person who infringes the provisions in place to protect consumers (consumer protection laws), other than in the application or recommendation of general conditions of sale, may have an order to cease and desist and a prohibition order imposed on him in the interests of consumer protection.

(2) For the purposes of this provision, "consumer protection laws" shall mean, in particular:

…

11. the provisions that regulate the lawfulness

(a) of the collection of a consumer's personal data by a trader, or

(b) of the processing or use of personal data collected about a consumer by a trader

if the data are collected, processed or used for the purposes of publicity, market and opinion research, operation of a credit agency, preparation of personality and usage profiles, address trading, other data trading or comparable commercial purposes.'

Telemediengesetz

12. Paragraph 2(1) of the Telemediengesetz (Law on telemedia) ('the TMG') provides as follows:

'For the purpose of this Law,

1. a service provider is any natural person or legal entity who holds his own or third-party telemedia for use or mediates access to use; …'

13. Paragraph 12(1) of the TMG states that: 'A service provider may collect and use personal data to make telemedia available only in so far as this Law or another legislative provision expressly relating to telemedia so permits or the user has consented to it.'

14. Paragraph 13(1) of the TMG provides as follows:

'At the beginning of the session the service provider shall inform the user, in a generally understandable manner, about the nature, extent and purpose of the collection and use of personal data and about the processing of his data in States outside the scope of application of [Directive 95/46/], unless the user has already been informed thereof. In the case of an automated procedure which allows subsequent identification of the user and which prepares the collection or use of personal data, the user shall be informed at the beginning of this procedure. The content of this information must be accessible to the user at any time.'

15. Pursuant to Paragraph 15(1) of the TMG:

‘A service provider may collect and use the personal data of a user only to the extent necessary in order to facilitate, and charge for, the use of telemedia (data concerning use). Data concerning use include, in particular:

1. features allowing identification of the user,

2. information about the beginning, end and extent of the particular use, and

3. information about the telemedia used by the user.’

III. Facts, proceedings, and questions referred

16. Fashion ID (‘the Defendant’)’ is an online retailer. It sells fashion items on its website. The Defendant embedded the ‘Like’ plug-in supplied by Facebook Ireland Limited (‘Facebook Ireland’)(4) in its website. As a result the so-called Facebook ‘Like’ button appears on the Defendant’s website.

17. The order for reference further explains how the (non-visible) part of the plug-in functions: when a visitor lands on the Defendant’s website on which the Facebook ‘Like’ button is placed, his browser automatically sends information concerning his IP address and browser string to Facebook Ireland. The transmission of this information occurs without it being necessary to actually click on the Facebook ‘Like’ button. It also seems to follow from the order for reference that when the Defendant’s website is visited, Facebook Ireland places different kinds of cookies (session, datr and fr cookies) on the user’s device.

18. Verbraucherzentrale NRW (‘the Applicant’), a consumer protection association, brought judicial proceedings against the Defendant before a Landgericht (District Court, Germany). The Applicant sought an order to force the Defendant to cease integrating the social plug-in ‘Like’ from Facebook on the grounds that the Defendant allegedly did not:

– ‘expressly and clearly explain the purpose of the collection and use of the data transmitted in that way to users of the internet page before the provider of the plug-in begins to access the user’s IP address and browser string, and/or

– obtain the consent of users of the internet page to access to their IP address and browser string by the plug-in provider and to the data usage, in each case prior to the access occurring, and/or

– inform users who have given their consent within the meaning of second head of claim that this can be revoked at any time with effect for the future, and/or

– inform that “If you are a user of a social network and do not wish that social network to collect data about you via our website and link these to your user data saved on the social network, you must log out of the social network before visiting our website”.’

19. The Applicant claimed that Facebook Inc. or Facebook Ireland saves the IP address and browser string and links them to a specific user (member or non-member). The Defendant’s argument in response is a lack of knowledge in this respect. Facebook Ireland argues that the IP address is converted to a generic IP address and is saved only in this form and that there is no allocation of the IP address and browser string to user accounts.

20. The Landgericht (District Court) ruled against the Defendant on the first three pleas. The Defendant appealed. A cross-appeal was lodged by the Applicant in respect of the fourth plea.

21. It is within that factual and legal context that the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf) decided to refer the following questions to the Court:

‘(1) Do the rules in Articles 22, 23 and 24 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) preclude national legislation which, in addition to the powers of intervention conferred on the data-protection authorities and the remedies available to the data subject, grants public-service associations the power to take action against the infringer in the event of an infringement in order to safeguard the interests of consumers?

If Question 1 is answered in the negative:

(2) In a case such as the present one, in which someone has embedded a programming code in his website which causes the user’s browser to request content from a third party and, to this end, transmits personal data to the third party, is the person embedding the content the “controller” within the meaning of Article 2(d) of [Directive 95/46] if that person is himself unable to influence this data- processing operation?

(3) If Question 2 is answered in the negative: Is Article 2(d) of [Directive 95/46] to be interpreted as meaning that it definitively regulates liability and responsibility in such a way that it precludes civil claims against a third party who, although not a “controller”, nonetheless creates the cause for the processing operation, without influencing it?

(4) Whose “legitimate interests”, in a situation such as the present one, are the decisive ones in the balancing of interests to be undertaken pursuant to Article 7(f) of [Directive 95/46]? Is it the interests in embedding third-party content or the interests of the third party?

(5) To whom must the consent to be declared under Articles 7(a) and 2(h) of [Directive 95/46] be made in a situation such as that in the present case?

(6) Does the duty to inform under Article 10 of [Directive 95/46] also apply in a situation such as that in the present case to the operator of the website who has embedded the content of a third party and thus creates the cause for the processing of personal data by the third party?’

22. Written submissions have been lodged by the Applicant, the Defendant, Facebook Ireland, the Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (State Commissioner for Data Protection and Freedom of Information North Rhine-Westphalia, Germany) (‘LDI NW'), Belgium, German, Italian, Austrian, and Polish Governments as well as the Commission. Oral submissions were made by the Applicant, the Defendant, Facebook Ireland, the LDI NW, Belgium, Germany, Austria, and the Commission at the hearing held on 6 September 2018.

IV. Assessment

23. In this Opinion, I propose that Directive 95/46 does not preclude national legislation granting an association tasked with the protection of consumers, such as the Applicant, standing to bring an action against an alleged infringer of data protection laws (A). I also consider that the Defendant is a joint controller, along with Facebook Ireland, its liability being limited however to a specific stage of the data processing (B). Third, I am of the view that the balancing exercise provided for in Article 7(f) of Directive 95/46 requires the legitimate interests of not only the Defendant but also of Facebook Ireland to be taken into account (as well as, of course, the rights of data subjects) (C). Fourth, the data subject’s informed consent for a given data processing stage must be declared to the Defendant. The Defendant also has the obligation to provide information to the data subject (D).

A. National legislation granting standing to associations tasked with protection of interests of consumers

24. By the first question posed, the referring court asks in essence whether Directive 95/46 precludes a national rule allowing associations for the protection of consumers' interests to commence legal proceedings against a person allegedly breaching data protection laws. In this respect, the referring court cites Articles 22 to 24 of Directive 95/46 specifically. It notes that the national legislation at issue could be considered as a 'suitable measure' under Article 24. In addition it emphasises that Regulation (EU) 2016/679 ('the GDPR'), (5) which has replaced Directive 95/46, now explicitly confers such a right on associations in its Article 80(2). (6)

25. The Defendant and Facebook Ireland argue that Directive 95/46 does not allow for standing of such associations, because no such standing is expressly provided for, as Directive 95/46 aims, in their view, at full harmonisation. According to the Defendant, allowing standing in this way would threaten the independence of supervisory authorities due to the public pressure to which those authorities would be exposed.

26. The Applicant, the LDI NW, and all the governments that have taken a position in the present case share the view that Directive 95/46 does not preclude the legislation at issue.

27. I agree with the latter view.(7)

28. I consider it important to recall, at the outset, the (default) constitutional rule embedded in the third paragraph of Article 288 TFEU according to which a 'directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods' which best ensure the result to be achieved by the directive. (8)

29. It follows that in order to implement obligations under a directive, the Member States are free to adopt any measures they deem fit, as long as those measures are not expressly excluded by the directive itself, or do not conflict with that directive's aims.

30. The *text* of Directive 95/46 does not expressly exclude the possibility under national law to grant standing to associations tasked with the protection of consumers' rights.

31. Looking at the *objectives* pursued by Directive 95/46, these include 'ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data'. (9) Moreover, pursuant to the 10th recital of Directive 95/46 'the approximation of the national laws applicable in this area must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community'. (10)

32. It can be understood from the order for reference that Germany has granted standing for associations such as the Applicant to challenge what those associations consider to be an unlawful commercial practice or a practice infringing consumer protection laws, the latter including data protection legislation.

33. In this context, I fail to see how granting such standing would in any way contradict the aims of Directive 95/46 or weaken the effort to achieve those objectives. If anything, allowing standing to this kind of association seems rather to enhance such achievement of the aims and implementation of the directive in actually contributing to strengthening the rights of data subjects through the means of collective redress. (11)

34. I consider that the Member States are thus not precluded from providing for a rule for the standing of associations, such as the one allowing the Applicant to bring the action at issue in the main proceedings, if the Member States wish to do so.

35. In view of this answer, I consider the discussion that unfolded in the course of these proceedings, focusing on whether the national legislation in question should fall specifically under Article 24 of Directive 95/46 as a type of 'suitable measure', or whether it could fall under Article 22, a bit of a red

herring. If the Member States are supposed to implement a directive by any means they see fit, and that particular way of implementation is not precluded either by the text or by the aim and purpose of the directive, the specific article of the directive under which a particular national measure can be categorised is of secondary importance. (12) Nevertheless, for what it is worth, 'suitable measures to ensure the full implementation of the provisions of this Directive' under Article 24 could certainly be construed as including national provisions such as those at issue in the present case.

36. I do not think that this general conclusion is in any way undermined by the following considerations, which were discussed in the course of these proceedings.

37. First, it is true that Directive 95/46 does not appear on the list provided for in Annex I to Directive 2009/22. The latter lays down rules on injunctions that can be brought by so called 'qualified entities' to enhance the protection of the collective interests of consumers. (13) The list in Annex I contains several directives and Directive 95/46 is not amongst them.

38. Nevertheless, and as the German Government submits, the list in Annex I to Directive 2002/29 cannot be viewed as exhaustive in the sense that it would preclude national legislation providing for injunctive actions concerning the respect of rules contained in directives other than those listed in Annex I to Directive 2002/29. A fortiori, it would be rather surprising if such an illustrative list contained in a piece of secondary legislation were to be suddenly construed as depriving Member States of their choice in how to implement a directive, provided for by the Treaty.

39. Second, I turn to the argument submitted by the Defendant and Facebook Ireland concerning the full harmonisation effected by Directive 95/46, which would, in their view, exclude any explicitly unforeseen action.

40. It is true that the Court has consistently stated that the harmonisation flowing from Directive 95/46 is not limited to minimal harmonisation but amounts to harmonisation which is 'generally complete'. (14) At the same time, it has also been acknowledged that the same directive 'allows the Member States a margin for manoeuvre in certain areas', provided that Directive 95/46 is complied with. (15)

41. As I suggested elsewhere, (16) the question whether there is a 'full harmonisation' at EU law level (in the sense of legislative preemption, precluding any legislative action on the part of the Member States) cannot be addressed in general, with regard to an entire field of law or a subject matter of a directive. Instead, that assessment is to be carried out with regard to each specific provision (a certain rule or a specific aspect) of the directive in question.

42. Looking at the specific 'procedural' provisions of Directive 95/46 which are at issue in the present case, namely Articles 22 to 24, these are worded in very general terms. (17) Taking into account the level of generality and abstraction of those provisions, it would indeed be quite striking to suggest that those provisions generate the effect of legislative preemption, excluding any measures which can be taken by the Member States but which are not specifically mentioned in those articles. (18)

43. Third, another argument raised by the Defendant concerned the threat to the independence of supervisory authorities. (19) It essentially suggested that if the standing of consumer associations were allowed, those associations would bring actions in parallel with, and/or instead of, the supervisory authority, which would lead to public pressure and bias on the part of the supervisory authority, and eventually contravene the requirement of the complete independence of supervisory authorities set out in Article 28(1) of the directive.

44. This argument has no weight. Provided that such a supervisory authority were in fact truly independent in the first place, (20) I fail to see, like the German Government, how an action such as the one in the main proceedings could threaten its independence. An association cannot enforce the law in the sense of making its view binding on the supervisory authorities. That is the exclusive province of the courts. A consumer association can only, in this way like any individual consumer, bring an action.

Therefore, the claim that any and every (private) action brought by an individual or by a consumer association would put pressure on the bodies tasked with (public) enforcement and thus cannot be allowed to co-exist in parallel with the system of public enforcement is of such a peculiar nature that there is little need to address this argument any further. (21)

45. Fourth and finally, I turn to the argument according to which Article 80(2) of the GDPR has to be understood as modifying (and reversing) the previous situation by allowing for something (standing of associations) that was not permitted before.

46. That argument is unconvincing.

47. It is important to recall that with the GDPR replacing Directive 95/46, the nature of the legal instrument in which the rules are found changed from that of a directive to that of a regulation. That change also meant that in contrast to a directive, where Member States remain free to choose how to implement the content of that legislative instrument, national rules implementing a regulation may, in principle, only be adopted when expressly authorised.

48. Viewed from this perspective, the argument that the explicit provision on standing of associations, now included in the GDPR, means that that standing was excluded under Directive 95/46, is questionable. If an argument could be drawn from such a juxtaposition, (22) then it would rather be to the contrary: if providing rules to allow such standing was not precluded by the latter directive (based on the arguments I presented above), the change of legal form from directive to regulation would justify including such a provision in order to make it clear that such a possibility indeed remains.

49. Therefore, in the light of the above, my first interim conclusion is that Directive 95/46 does not preclude national legislation which grants public-service associations standing to commence legal proceedings against the alleged infringer of data protection legislation in order to safeguard the interests of consumers.

B. Is Fashion ID a data controller?

50. By its second question, the referring court is asking whether the Defendant, because it embedded a plug-in in its website which causes the user's browser to request content from a third party and transmits personal data to that third party, is to be considered a 'controller' within the meaning of Article 2(d) of Directive 95/46, even if the Defendant is unable to influence the data-processing operation.

51. By the lack of *ability to influence the data processing operation*, stated by the referring court in its question, I understand that in the context of the present case, this does not relate to the *causing* of the process of transmission of that data (and on the factual level, the Defendant clearly has an influence because it has embedded the plug-in concerned). It seems rather to relate to the possible *subsequent processing* of the data by Facebook Ireland.

52. As the referring court notes, the response to its second question has implications that go well beyond the present case and the social network operated by Facebook Ireland. A number of websites embed third-party content of varying nature. If a person such as the Defendant were to be classified as a 'controller', (co-)responsible for any (subsequent) processing that takes place in respect of the data collected because that website operator embedded third-party content enabling the transfer of such data, then such a statement would indeed have wider implications for the way third-party content is handled.

53. Within the structure of the present case, the second question is also the key question which goes to the heart of the issue: in cases of embedded third-party content on a website, *who* bears the responsibility and *for what* exactly? It is also the (im)precision in answering this question that has an impact on the answers to the following questions on legitimate interests, consent, and duty to inform.

54. In this section, I will first make a few introductory remarks on the notion of personal data relevant for the present case (1). I will then present recent case-law of the Court, suggesting how the second question could be answered, if the Court's previous decisions are to be embraced with no further questions asked (2). I will then explain why more questions should perhaps be asked and, in the context of the present case, the analysis somewhat refined (3). I will conclude by stressing, for the purposes of the definition of the notion of (joint) control, the importance of the unity of 'purposes and means' that ought to exist amongst the (joint) controllers with regard to the respective stage of processing of personal data (data processing operation) in question (4).

1. Personal data in the present case

55. It ought to be recalled that the notion of 'personal data' is defined in Article 2(a) of Directive 95/46 as being 'any information relating to an identified or identifiable natural person ("data subject")'. Recital 26 of the same directive explains in this respect that 'to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person'.

56. The Court has already clarified that an IP address can, under certain circumstances, constitute personal data. (23) The Court further stated that for these purposes, for there to be an 'identifiable person' within the meaning of Article 2(a) of Directive 95/46, 'it is not necessary that that information alone allows the data subject to be identified', and that recourse to additional data may thus be necessary. It also stated that 'it is not required that all the information enabling the identification of the data subject must be in the hands of one person' as far as the possibility to combine the respective data 'constitutes a means likely reasonably to be used to identify the data subject'. (24)

57. The referring court does not discuss whether the IP address, alone or in combination with the browser string which is also transmitted, constitute personal data in the sense of that criteria. Facebook Ireland appears to be disputing that qualification. (25)

58. It is clear that such an assessment is for the national court to carry out. In general, with regard to any plug-ins that may be embedded or any other third-party content, for information to be classed as personal it is indispensable that that data allows the data subject to be identified (be it directly or indirectly). For the purposes of the present case, I shall take as given that, as it appears to follow from the questions asked by the referring court, in the circumstances of the main proceedings, the IP address and the browser string do indeed *constitute* personal data and fulfil the criteria of Article 2(a) of Directive 95/46 as clarified by the Court.

2. Wirtschaftsakademie Schleswig-Holstein locuta, causa finita?

59. As far as the answer to the second question is concerned, the Defendant and Facebook Ireland submit that the Defendant cannot be considered as being a controller because it has no influence over the personal data that will be processed. Thus, only Facebook Ireland can be classified as such. As a subsidiary argument, Facebook Ireland puts forward that the Defendant acts together with it, as joint controller, the responsibility of a person such as the Defendant however being limited to its actual zone of influence.

60. The Applicant**,** the LDI NW, and all the governments that have intervened in the present case as well as the Commission share, in essence, the position that the notion of 'controller' has a broad meaning and includes the Defendant. However, their views as to the exact scope of the Defendant's responsibility vary considerably in those submissions. The differences concern the question whether (or not) the Defendant and Facebook Ireland should be held jointly responsible, whether or not their joint responsibility should be limited to the stage of the processing of personal data in which the Defendant is actually involved, and whether a distinction shall be made in this context between the visitors to the Defendant's website that have a Facebook account and those who do not.

61. As a starting point, it is clear that under Article 2(d) of Directive 95/46, the notion of 'controller' covers a person that '*alone or jointly* with others determines the *purposes and means* of the processing of personal data'. (26) The notion of controller can thus refer to several actors taking part in the personal data processing (27) and should be interpreted broadly. (28)

62. The issue of joint control has recently been addressed by the Court in the judgment in *Wirtschaftsakademie Schleswig-Holstein*. (29)With regard to the role of the administrator of a Facebook fan page, the Court concluded that that administrator acted as a controller, jointly with Facebook Ireland, within the meaning of Article 2(d) of Directive 95/46. This was because the administrator contributed to determining, jointly with Facebook Ireland, the purposes and means of processing the personal data of visitors to the fan page. (30)

63. More specifically, the Court noted that by creating the fan page at issue, the administrator gave Facebook Ireland 'the opportunity to place cookies on the computer or other device of a person visiting its fan page', and thus process personal data. (31) The Court pointed out that 'the creation of a fan page on Facebook Ireland 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'. (32) The processing at issue enabled Facebook Ireland 'to improve its system of advertising' while it provided the administrator with the means to manage better, via anonymised statistics, the promotion of its own activity. (33)

64. The Court concluded that by 'its definition of parameters', the administrator at issue took part in the determination of the purposes and means of processing the personal data of the visitors to its fan page. Therefore, it had to be considered as a controller responsible for that processing jointly with Facebook Ireland (with 'even greater' responsibility with regard to the personal data of Facebook Ireland non-users). (34)

65. In *Jehovan todistajat*,the Court underlined another important clarification with regard to the notion of joint controller: for there to be joint control and joint responsibility, it is not required that each of the controllers must have access to (all of) the personal data concerned. Thus, a religious community could also be a joint controller in cases in which the community itself apparently had no access to the collected data in question. In that case it was the individual members of the community of Jehovah's Witnesses who were in physical possession of the personal data. It was enough that the preaching activity, in the course of which personal data was apparently being collected, was organised, coordinated and encouraged by that community. (35)

66. If considered at a higher level of abstraction, and if focusing only on the notion of joint control, I am bound to agree that in view of such recent judicial pronouncements, it is to be concluded that the Defendant acts as a controller, and is jointly responsible together with Facebook Ireland for data processing. (36)

67. First, it appears that the Defendant made it possible for Facebook Ireland to obtain the personal data of the users of the Defendant's website by using the plug-in at issue.

68. Second, it is true that, as opposed to the administrator concerned in *Wirtschaftsakademie Schleswig-Holstein,* the Defendant does not appear to be determining the parameters of any information about its website's users which would be returned to it in an anonymised or other form. The sought-after 'benefit' appears to be free advertisement of its products that allegedly occurs when the user of its website decides to click on the Facebook 'Like' button to share, via its Facebook account, her thoughts concerning, let's say, a black cocktail dress. Thus, and subject to factual verification by the referring court, the use of the plug-in allows the Defendant to optimise the advertisement of its products by being able to make them visible on Facebook.

69. Alternatively, viewed in a different light, the Defendant could be said to be (co-)determining the parameters of the data collected by the simple act of embedding the plug-in at issue in its website. It is the plug-in itself that provides parameters of the personal data to be collected. Thus, by voluntarily integrating that tool into its website, the Defendant has set those parameters with regard to any visitors to its website.

70. Third and in any case, in the light of *Jehovan todistajat*, a joint controller can be still classified as such without even having access to any 'fruits of joint labour'. Thus, the fact that the Defendant does not have access to the data passed on to Facebook or that it apparently does not receive any tailored or aggregated statistics in return, does not appear to be decisive.

3. The problems: who then is not a joint controller?

71. Will effective protection be enhanced if everyone is made responsible for ensuring it?

72. That, in a nutshell, is the deeper moral and practical dilemma demonstrated by the present case and expressed in legal terms by the scope of the definition of (joint) controller. In the understandable desire to secure the effective protection of personal data, the recent case-law of the Court has been very inclusive when being asked to define, in one way or another, the notion of (joint) controller. So far, however, the Court has not been faced with the practical implications of such a sweeping definitional approach with regard to the subsequent steps of exact duties and specific liability of parties who are classified as joint controllers. Since this case offers precisely such an opportunity, I would suggest seizing it in order to enhance the preciseness in the definitions that ought to be exist for the notion of (joint) controller.

(a) On obligation and responsibility

73. When looking at the applicable test to identify a 'joint controller' with a critical eye, it seems that the crucial criterion after *Wirtschaftsakademie Schleswig-Holstein*and *Jehovan todistajat* is that the person in question 'made it possible' for personal data to be collected and transferred, potentially coupled with some input that such a joint controller has as to the parameters (or at least where there is silent endorsement of them). (37) If that is indeed the case, then in spite of a clearly stated intention to that effect to exclude it in *Wirtschaftsakademie Schleswig-Holstein*, (38)it is difficult to see how normal users of an online (based) application, be it a social network or any other collaborative platform, but also other programmes, (39) would not also become joint controllers. A user will typically set up his account, providing parameters to the administrator as to how his account is to be structured, what information he wishes to receive, on what subjects and from whom. He will also invite his friends, colleagues and others to share information in the form of (often quite sensitive) personal data, via the application, thus not only providing data concerning those persons, but also inviting those persons to become involved themselves, in this way clearly contributing to the obtaining and processing of personal data of those persons.

74. Furthermore, what about the other parties in a 'personal data chain'? When pushed to an extreme, if the only relevant criterion for joint control is to have made the data processing possible, thus in effect contributing to that processing at any stage, would the internet service provider, which makes the data processing possible because it provides access to the internet, or even the electricity provider, then not also be joint controllers potentially jointly liable for the processing of personal data?

75. The intuitive answer is of course 'no'. The problem is that the delineation of responsibility so far does not follow from the broad definition of a controller. The danger of that definition being too broad is that it results in a number of persons being co-responsible for the processing of personal data.

76. However, in contrast to the cases outlined in the previous section, the questions posed by the referring court in the present case do not stop at how to define 'controller'. They pick up on and continue exploration of related issues in terms of the allocation of actual obligations imposed by Directive 95/46. Those issues themselves demonstrate the problems of an over-inclusive definition of a controller, especially when coupled with the lack of a precise rule as to what exactly the specific duties and responsibilities of controllers are under Directive 95/46. The interested parties' submissions in response to

questions 5 and 6, which are concerned with the exact allocation of responsibilities under the directive, illustrate this well.

77. Question 5 essentially enquires as to *who* is supposed to obtain the data subject's consent and *for what purpose*. The suggested answers to that question vary considerably.

78. The Applicant and the LDI NW consider that the obligation to obtain the data subject's informed consent is on the Defendant, which decided to integrate the plug-in at issue. That is, in the Applicant's view, all the more important for non-Facebook users who have not accepted the general terms and conditions of Facebook. The Defendant's position is that the consent must be given to the third party providing the embedded content, namely Facebook Ireland. Facebook Irelandconsiders that the consent does not have to be given to a particular addressee, as Directive 95/46 specifies only that the consent has to be free, specific and informed.

79. Austria, Germany and Poland put forward that the consent must be given before the processing of the data occurs and, according to Austria it must relate both to the collection and possible transmission of data. Poland stresses that consent must be given to the Defendant. Germany considersthat it must be given to the Defendant or to the third party providing the embedded content (Facebook Ireland) because both are co-responsible for the processing. The Defendant only has to receive the consent for transmission of the data to the third party because for all other processing and use of the collected data, it no longer acts as the controller. That does not, however, exclude the possibility for the website operator to receive consent concerning the processing by the third party, which can be governed by an agreement between both of them. Italy submits that the consent must be given to all those who take part in the processing of the personal data, namely the Defendant and Facebook Ireland. Belgium and the Commission stress that Directive 95/46 does not specify to whom the consent must be given.

80. A similar diversity of views exists with regard to the issue of *who* bears the obligation to inform under Article 10 of Directive 95/46 and with regard to *what* exactly, addressed by the sixth question posed by the referring court.

81. According to the Applicant, it is the website operator who has the obligation to communicate the necessary information to the data subject. The Defendant has made the opposite argument, stressing that it is for Facebook Ireland to provide information as the Defendant does not have accurate knowledge. Similarly, Facebook Ireland stresses that it has the information obligation, as that obligation is addressed only to the controller (or its representative). It notes that the reply to question 6 is closely linked to whether the website operator is a controller. Article 10 shows that it is inappropriate to classify the website operator as a controller because the latter is not in a position to provide that information. The LDI NW considers that the information must be given by the website operator, but acknowledges the difficulty in determining what information should be given, as the Defendant has no influence over the processing of data by Facebook Ireland. The interweaving of the data processing objectives suggests that the website operator should be co-responsible for the processing that it has made possible.

82. Belgium, Italy and Poland state that the obligation to inform also applies to the website operator such as the one at issue, given that it qualifies as a controller. Belgium adds that the website operator may also have an obligation to verify the purpose of the subsequent data processing and take appropriate measures to guarantee the protection of natural persons. The German Government argues that the information obligation applies to the website operator to the extent that it is responsible for the processing, namely for the transmission of data to the external supplier of the embedded content, but not for all subsequent data processing stages, which are the responsibility of that external supplier. In the view of Austria and of the Commission both the website operator and external supplier are subject to the obligation to provide information under Article 10 of Directive 95/46.

83. Beyond the issues raised by questions 5 and 6, it might be added that similar conceptual difficulties are likely to arise also when considering other obligations defined by Directive 95/46 such as the right of access under Article 12 thereof. It is true that the Court stated in *Wirtschaftsakademie Schleswig-*

*Holstein*that 'Directive 95/46 does not, where several operators are jointly responsible for the same processing, require each of them to have access to the personal data concerned'. (40) However, a controller that does not itself have access to data for which it is nevertheless categorised as a (joint) controller cannot, quite logically, provide that access to any data subject (not to mention any further operations, such as rectification or erasure).

84. Thus, at this stage, the conceptual lack of clarity upstream (who is the controller and with regard to what exactly) that may lead in some instances to the lack of clarity downstream (who is subject to what obligation), crosses into the realm of actual impossibility for a potential joint controller to comply with valid legislation.

85. It could certainly be suggested that for the exact allocation of responsibility amongst the (potentially rather numerous joint) controllers, contracts should be concluded. This would not only provide for the allocation of responsibility, but also identify the party that is supposed to comply with each of the obligations provided for by the directive, including those that can be physically exercised by only one party.

86. I find such a proposition deeply problematic. First, it is completely unrealistic, taking into account the dense web of formal, standard contracts that would have to be signed by any kind of party, including, most likely, a number of normal users. (41) Second, the application of valid legislation, and the allocation of responsibility it provides for would be made conditional upon private agreements, to which third parties seeking to enforce their rights might not have access.

87. Third, perhaps partially pre-empting some of these issues, the GDPR appears to be introducing a new regime of joint liability in its Article 26. It is certainly true that the GDPR was not applicable *ratione temporis* to the cases discussed in this section, or in the present case. However, unless there is a specific or systematic derogation in the new legislation with regard to the relevant definitions, which appears not to be the case as Article 4 of the GDPR largely retains the same key terms as Article 2 of Directive 95/46 (while adding a number of new ones), it would be rather surprising if the interpretation of such key notions, including the notion of controller, processing, or personal data, were to significantly depart (without a very good reason) from the extant case-law.

88. If that was indeed the case, then what seems to be a regime of joint liability for joint controllers introduced in Article 26(3) of the GDPR could turn into quite a challenge. On the one hand, Article 26(1) of the GDPR makes it possible for joint controllers to 'determine their respective responsibilities for compliance with the obligations'. On the other hand, however, Article 26(3) of the GDPR makes it clear that the 'data subject may exercise his or her rights' 'in respect of and against each of the controllers' irrespective of any such arrangement. Any of the joint controllers can thus be held liable for the data processing in question.

(b) The bigger picture

89. A long time ago (the fans of a certain sci-fi franchise might wish to add 'in a galaxy far, far away'), it was cool to be on a social network. Then gradually, it started to be cool not to be on a social network. Nowadays, it appears to be a crime to be on one (and for which novel forms of vicarious liability have to be put in place).

90. There is no denying that judicial decision-making occurs in an evolving social context. It should certainly react to that context, but not be controlled by it. A social network, like any other application or programme, is a tool. Similar to a knife or a car, it can be used in a number of ways. There is also no doubt that if used for the wrong purposes, that use must be prosecuted. But it might perhaps not be the best idea to punish anyone and everyone who has ever used a knife. One normally prosecutes the person(s) controlling the knife when it caused harm.

91. Thus, there ought to be, perhaps not always an exact match, but at least a reasonable correlation between power, control, and responsibility. Modern law naturally includes various forms of objective liability, which will be triggered merely by certain results occurring. But those tend to be justified exceptions. If, without any reasoned explanation, responsibility is attributed to someone who had no control over the result, such allocation of liability will typically be seen as unreasonable or unjust. (42)

92. Moreover, in answering the question posed at the beginning of this section (point 71), a sceptical person from the more eastern parts of the European Union might perhaps suggest, considering his historical experience, that effective protection of something tends to dramatically decrease if everyone is made responsible for it. Making everyone responsible means that no-one will in fact be responsible. Or rather, the one party that should have been held responsible for a certain course of action, the one actually exercising control, is likely to hide behind all those others nominally 'co-responsible', with effective protection likely to be significantly diluted.

93. Finally, no good (interpretation of the) law should reach a result in which the obligations provided therein cannot actually be carried out by its addressees. Thus, unless the robust definition of (joint) control is not supposed to turn into a judicially sponsored command to disconnect which is applicable to all actors, and to refrain from using any social networks, plug-ins, and potentially other third-party content for that matter, then in defining the obligations and responsibilities, reality must play a role, again including issues of knowledge and genuine bargaining power and the ability to influence any of the imputed activities. (43)

4. Back to the (legislative) roots: unity of purposes and means with regard to a certain processing operation

94. Although rather robust in its approach to the definition of joint control in *Wirtschaftsakademie Schleswig-Holstein*, the Court also hinted at the need to limit the liability of a (joint) controller. More specifically, the Court noted 'that the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. … 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'. (44)

95. While there was no need to address that specific issue in *Wirtschaftsakademie Schleswig-Holstein*, there is in the present case, in which the referring court directly invites the Court to ascertain the possible obligations on the Defendant which follow from its status as a controller.

96. In view of the newly introduced system of joint liability in Article 26 of the GDPR, it might be difficult to envisage how *joint responsibility* could imply, with regard to the same result in terms of potentially (il)licit treatment of personal data, *non-equal responsibility*. This is in particular in view of Article 26(3) of the GDPR, which appears to steer in the direction of joint (and several) liability. (45)

97. I think however that the key statement of the Court is the second one, namely that 'operators may be involved at different stages of that processing of personal data and to different degrees'. Such a suggestion finds support in the definitions contained in Directive 95/46, in particular with regard to the definition of (i) the notion of processing in Article 2(b), and (ii) the notion of controller in Article 2(d).

98. First, the notion of personal data processing contains 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'.

99. Even if the notion of processing is, similar to the notion of controller, rather broad, (46) it clearly underlines and aims at a *stage* in the processing: it refers to an *operation* or a *set of operations*, with an illustrative list of what such individual operations might be. But then logically, the issue of control should

rather be assessed with regard to the discrete operation in question, not with regard to an undetermined bundle of everything and anything called processing. (47)

100. Second, the notion of joint control is not specifically defined by Directive 95/46. But logically, that notion builds on the notion of controller in Article 2(d): the situation of joint control appears when two or more persons determine the *means and the purposes of processing* of personal data together. (48) In other words, for two (or more) persons to qualify as joint controllers, there must be *identity of the purposes and means* of the personal data processing between them.

101. It is the combination of these two definitions that ought, from my point of view, to determine the obligations and potential liability of joint controllers. A (joint) controller is 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. By contrast, that person cannot be held liable for either the preceding stages or subsequent stages of the overall chain of processing, for which it was not in a position to determine either the purposes or means of that stage of processing.

102. In the present case, the relevant stage (operations) of the processing corresponds to the *collection* and *transmission* of personal data that occurs by means of the Facebook 'Like' button.

103. First, as far as the *means* of those data processing operations are concerned, as suggested by the Applicant, the LDI NW and the German Government, it seems to be established that the Defendant decides on the use of the plug-in at issue, which serves as a vehicle for the collection and transmission of the personal data. That collection and transmission is triggered by visiting the Defendant's website. That plug-in was provided to the Defendant by Facebook Ireland. Both Facebook Ireland and the Defendant thus appear to have voluntarily caused the collection and transmission stage of the data processing. That of course remains, at the factual level, for the national court to verify.

104. Second, looking at the *purpose* of the data processing, the order for reference does not state the reasons for which the Defendant decided to embed the Facebook 'Like' button in its website. However, and subject to the referring court's verification, that decision appears to be inspired by the wish to increase visibility of the Defendant's products via the social network. At the same time, it would also appear that the data transferred to Facebook Ireland are used for the latter's own commercial purposes.

105. Despite the fact that the specific commercial use of the data may not be the same, in general both the Defendant and Facebook Ireland seem to pursue commercial purposes in a way that appears to be mutually complementary. In this way, although not identical, there is unity of purpose: there is a commercial and advertising purpose.

106. On the facts in the present case, it thus appears that the Defendant and Facebook Ireland co-decide on the means and purposes of the data processing at the stage of the collection and transmission of the personal data at issue. To that extent, the Defendant acts as a controller and its liability is, to that extent as well, joint with that of Facebook Ireland.

107. At the same time, I consider that the liability of the Defendant 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.

108. In the light of the above, my second interim conclusion is therefore that a person, such as the Defendant, that has embedded a third-party plug-in in its website, which causes the collection and transmission of the user's personal data (that third party having provided the plug-in), shall be considered to be a controller within the meaning of Article 2(d) of Directive 95/46. However, that controller's (joint) responsibility is limited to those operations for which it effectively co-decides on the means and purposes of the processing of the personal data.

109. It ought to be added that that conclusion also answers to the third question posed. By that question the referring court wishes to ascertain, in essence, whether Directive 95/46 precludes the application of the national-law concept of *Störer* (disrupter) on the Defendant should it be established that the Defendant *cannot be considered* as controller. Pursuant to the order for reference, the concept of *Störer* requires the person who does not infringe a right but who has created or increased the risk of such an infringement by a third party to do everything that is reasonable and within its power to prevent that infringement. If the Defendant cannot be considered to be a controller, the referring court suggests that the prerequisites for the application of the concept of *Störer* have been met because, by embedding the plug-in for the Facebook 'Like' button, the Defendant has, at the very least, created the risk of an infringement by Facebook.

110. In view of the answer provided to the referring court's second question, there is no need to address the third one. Once it is established that a given person is to be categorised as a controller within the scope of Directive 95/46, its obligations as controller have to be assessed in the light of the obligations defined by that directive. The opposite conclusion would lead to a differentiated liability of controllers for a particular infringement across the different Member States. In this sense, and with regard to the definition of controller, Directive 95/46 indeed effects full harmonisation with regard to the addressees of the defined obligations. (49)

C. Legitimate interests to be taken into account under Article 7(f) of Directive 95/46

111. The fourth question asked in the present case concerns the legitimacy of the processing of personal data in the absence of data subject's consent within meaning of Article 7(a) of Directive 95/46.

112. In this respect, the referring court points to Article 7(f) of Directive 95/46 under which the personal data may be processed if this is 'necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject …'. More specifically the referring court wishes to ascertain *whose* legitimate interests should be taken into account in the context of the present case: those of the Defendant that has embedded the third-party content, or those of that third party (namely Facebook Ireland). (50)

113. As a preliminary point it ought to be noted that the Commission considers that the fourth question is irrelevant because *in casu* the user's consent must be provided anyway, by application of the legislation implementing Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector ('E-Privacy Directive'). (51)

114. I agree with the Commission that the E-Privacy Directive (which pursuant to Article 1(2) thereof clarifies and supplements Directive 95/46 in the electronic communications sector) (52) seems to apply to the situation at hand, to the extent that placement of cookies on the users' devices takes place. (53) Furthermore Article 2(f) and recital 17 of the E-Privacy Directive define the consent by reference to the notion of consent in Directive 95/46.

115. Whether the placement of cookies occurred in the case in the main proceedings was the subject of ample debate at the hearing. That factual clarification is for the national court to make. However, and in any case, as described in the order for reference, the referring court considers that the data transmitted constitutes personal data. (54) The issue of cookies does not appear therefore to provide the response to all the issues that apparently arise in the present case in relation to the data processing. (55)

116. I am thus of the view that question 4 requires further consideration.

117. The Applicant puts forward that the legitimate interest to be taken into account is that of the Defendant. It adds that neither the Defendant nor Facebook Ireland can claim a legitimate interest in the present case.

118. The Defendant and Facebook Ireland argue, in essence, that the legitimate interests to be considered are those of the person embedding the third-party content as well as that of the third party, while considering the interests of the website visitors whose fundamental rights may be affected.

119. The LDI NW, Poland, Germany and Italy consider that the legitimate interests of both the Defendant and Facebook Ireland should be taken into account as both of them have made the processing at issue possible. Austria embraces a similar view. Similarly, and by referring to the judgment of the Court in *Google Spain*, Belgium stresses that the legitimate interests to be taken into account are those of the controller as well as of the third parties to whom the personal data concerned have been communicated.

120. It ought to be recalled at the outset that all processing of personal data must in principle comply, among other conditions, with one of the criteria which make data processing legitimate, which are listed in Article 7 of Directive 95/46. (56)

121. Specifically regarding Article 7(f), the Court recalled that that provision 'lays down three cumulative conditions so that the processing of personal data is lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence'. (57)

122. Directive 95/46 does not define or enumerate 'legitimate interests'. That notion appears to be rather elastic and open-ended. (58) There is no type of interest that is excluded per se, as long of course as they are themselves legal. As was in essence discussed at the hearing and as stated above, (59) what seems to be at issue in the present case is the collection and the transmission of personal data for the purpose of advertising optimisation, although the precise ultimate goals of both the Defendant and Facebook Ireland may not be exactly the same.

123. With those considerations in mind, I would agree that marketing or advertising can, as such, constitute such a legitimate interest. (60) It is rather difficult to go beyond that statement in the context of the present case, as there is no specific information as to the exact ways in which the data transmitted and obtained is being used, beyond those general statements.

124. That being said, the referring court does not discuss nor request guidance concerning the assessment to be made of the specific legitimate interests put forward in the main proceedings. In its question 4, the referring court wishes to ascertain merely *whose* legitimate interests should be considered so that the balancing exercise under Article 7(f) of Directive 95/46 can be made.

125. In the light of my suggested reply to question 2 above, I consider that the legitimate *interests of both* the Defendant and Facebook Ireland have to be taken into account because *both of them act as joint controllers* for the respective personal data processing operation.

126. As their status of joint controllers implies that they also share the aims of personal data processing, the existence of a legitimate interest must be established in respect of both of them, at least at the general level as explained above. That interest must then be balanced against the rights of the data subjects as provided for in the last part of Article 7(f) of Directive 95/46, (61) that balancing depending 'in principle on the specific circumstances of the particular case'. (62) I recall that the data processing under such circumstances must also be subjected to the condition of necessity. (63)

127. In the light of the above, my third interim conclusion is that for the purpose of the assessment of the possibility to process personal data under the conditions set out in Article 7(f) of Directive 95/46, the legitimate interests of both joint controllers at issue have to be taken into account and balanced against the rights of the data subjects.

D. The Defendant's obligations concerning the consent to be received from, and information to be provided to, the data subject

128. By question 5, the referring court wishes to know to whom the consent which has to be declared under Article 7(a) and Article 2(h) of Directive 95/46 must be provided in the circumstances of the present case.

129. By question 6 the referring court wishes to know whether the obligation to inform under Article 10 of the Directive 95/46 applies, in the situation at hand, to the operator of a website (such as the Defendant) which has embedded the content of a third party and thus caused the processing of personal data by that third party.

130. As seen above, (64) there are a multitude of proposed answers to these questions. However, once the exact nature of the obligation under question 2 has been determined, both with regard to the bearer (*who*) and nature of the obligation (for *what*), and that issue is thus clarified upstream, then the answers to questions 5 and 6, which concern certain obligations downstream, become clearer.

131. First of all, I consider that both the consent and the information provided must cover all the aspects of the data processing operation(s) for which the joint controllers are jointly liable, namely the collection and the transmission. Conversely, those consent and information obligations do not extend to subsequent stages of the data processing in which the Defendant is not involved and for which it logically does not determine either means or purposes.

132. Second, under those conditions, one could suggest that the consent may be provided to either of the joint controllers. However, considering the particular situation at hand, that consent has to be provided to the Defendant, because it is when its website is actually visited that the processing operation is triggered. It would obviously not be in line with efficient and timely protection of data subjects' rights if the consent were to be given only to the joint controller that is involved later (if at all), once the collection and transmission has already taken place.

133. A similar answer is to be given with regard to the information obligation that the Defendant has under Article 10 of Directive 95/46. That provision defines a minimum list of information that must be communicated to the data subject by the controller (or by its representative). It contains the following elements: the controller's (or its representative's) identity, the purposes of the processing for which the data are intended and any further information where this is 'necessary having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject'. Article 10 provides examples of such further information which include, in what might be relevant in the present case, information about the recipient of the data or about the existence of the right of access and the right to rectify the data concerning the data subject.

134. Considering that list, the Defendant clearly appears to be in a position to provide information about the identity of the joint controllers, about the purpose of the respective stage of the processing (the operation(s) over which it has joint control); and also about the fact that those data will be transferred.

135. By contrast, as far as the right of access and the right to rectify are concerned, I understand that the Defendant itself does not have such access to the data being transferred to Facebook Ireland, since it is in no way involved in the storage of data. Thus, it could for instance be suggested that that matter would have to be the subject of an agreement with Facebook Ireland.

136. But such proposals would, beyond the arguments set out above, (65) again seek to extend the obligations and liability of a (joint) controller(s) to operations for which they are not responsible. If joint control means responsibility for those operation(s) for which there is the unity of purposes and means amongst the controllers, then logically the other ensuing obligations under the directive, such as consent, information, access or rectification ought to correspond to the scope of that original obligation. (66)

137. It was also noted by the Commission at the hearing that those of the visitors who have a Facebook account may have previously consented to such a transfer occurring. That could lead to a differentiated

liability of the Defendant, with the Commission apparently suggesting the Defendant's duty to inform and require consent would then apply only to Facebook non-users visiting the website of the Defendant.

138. I do not agree. I find it difficult to accept the idea that there should be differentiated (less protective) treatment in respect of 'Facebook users' in the circumstances of the present case because they would have already accepted the possibility of (any and all of) their personal data being processed by Facebook. Indeed, such an argument implies that upon opening a Facebook account one accepts in advance any data processing with regard to any online activity of such 'Facebook users' by any third party having whatever connection with Facebook. That is so even in a situation in which there is no visible sign of such data processing occurring (as seems to be the case when one simply visits the Defendant's website). In other words, accepting the Commission's suggestion would in effect mean that by opening a Facebook account, a user has actually waived any protection of personal data online vis-à-vis Facebook.

139. I thus consider that the liability and the ensuing consent and information obligations of the Defendant should be the same vis-a-vis the data subjects irrespective of whether or not they have a Facebook account.

140. Furthermore, it is again clear that that consent has to be given and information provided *before* the data are collected and transferred. (67)

141. Thus, in the light of the above, my final interim conclusion in response to questions 5 and 6 is that, in a situation such as that in the present case, the consent of the data subject obtained under Article 7(a) of Directive 95/46 has to be given to a website operator, such as the Defendant, which has embedded the content of a third party. Article 10 of Directive 95/46 shall be interpreted as meaning that the obligation to inform under that provision also applies to that website operator. The consent of the data subject under Article 7(a) of Directive 95/46 has to be given, and information within the meaning of Article 10 of the same directive provided, before the data are collected and transferred. However, the extent of those obligations shall correspond with that operator's joint responsibility for the collection and transmission of the personal data.

V. Conclusion

142. In the light of the above, I suggest that the Court respond to questions posed by Oberlandesgericht Düsseldorf ((Higher Regional Court, Düsseldorf, Germany) as follows:

– 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 does not preclude national legislation which grants public-service associations standing to commence legal proceedings against the alleged infringer of data protection legislation in order to safeguard the interests of consumers.

– A person that has embedded a third-party plug-in in its website, which causes the collection and transmission of the user's personal data (that third party having provided the plug-in), shall be considered to be a controller within the meaning of Article 2(d) of Directive 95/46. However, that controller's (joint) responsibility is limited to those operations for which it effectively co-decides on the means and purposes of the processing of the personal data.

– For the purpose of the assessment of the possibility to process personal data under the conditions set out in Article 7(f) of Directive 95/46, the legitimate interests of both joint controllers at issue have to be taken into account and balanced against the rights of the data subjects.

– The consent of the data subject obtained under Article 7(a) of Directive 95/46 has to be given to a website operator which has embedded the content of a third party. Article 10 of Directive 95/46 shall be interpreted as meaning that the obligation to inform under that provision also applies to that website operator. The consent of the data subject under Article 7(a) of Directive 95/46 has to be

given, and information within the meaning of Article 10 of the same directive provided, before the data are collected and transferred. However, the extent of those obligations shall correspond with that operator's joint responsibility for the collection and transmission of the personal data.

---

1 Original language: English.

---

2 Directive 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 (OJ 1995 L 281, p. 31).

---

3 Directive of the European Parliament and of the Council of 23 April 2009 (OJ 2009 L 110, p. 30).

---

4 I note that the order for reference states that the plug-in was made available to the Defendant by Facebook Ireland *or* by the latter's parent company, Facebook Inc., incorporated in the United States of America. However, it would appear that both before the referring court, and also in the proceedings before this Court, Facebook Ireland assumes possible liability under Directive 95/46 in the context of the present proceedings. I thus see no reason to discuss the potential applicability of Directive 95/46 in respect of Facebook Ireland's parent company.

---

5 Regulation 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 (General Data Protection Regulation) (OJ 2016 L 119, p. 1).

---

6 'Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.'

---

7 While adding, for the sake of completeness, that although the judgment of 28 July 2016, *Verein für Konsumenteninformation* (C−191/15, EU:C:2016:612) concerned a question of interpretation of Directive 95/46 that arose in national proceedings brought by an association, the Court did not consider the issue of the standing of the association in that case, simply because that specific question was not raised.

---

8 As restated for instance in the judgments of 23 May 1985, *Commission* v *Germany* (C−29/84, EU:C:1985:229, paragraph 22); of 14 February 2012, *Flachglas Torgau* (C−204/09, EU:C:2012:71, paragraph 60); and of 19 April 2018, *CMR* (C−645/16, EU:C:2018:262, paragraph 19).

---

9 Judgment of 13 May 2014, *Google Spain and Google* (C−131/12, EU:C:2014:317, paragraph 53).

---

10 See also judgment of 16 December 2008, *Huber* (C−524/06, EU:C:2008:724, paragraph 50).

---

11 Thus, in contrast to the judgment of 25 January 2018, *Schrems* (C−498/16, EU:C:2018:37), not involving any assignment of claims to a particular person and having apparently a clear legal basis in national law for what seems to be a type representation of the collective interest of consumers.

---

12 Or, to put it differently, Member States will also need to provide, especially as far as the institutional structure or procedures are concerned, for a number of other matters, which would also not be explicitly referred to in a directive (such as, in terms of judicial enforcement of a right, not just the issues of standing, but also for example time limits for bringing an action; court fees (if any); jurisdiction of courts; etc.). Could it then also be claimed that since neither Article 22, nor Article 24 of the Directive 95/46 mention any of these issues, the Member State is also precluded from providing for such matters in national law?

---

13 As defined in Article 3 of Directive 2009/22.

---

14 See for instance, judgments of 6 November 2003, *Lindqvist* (C−101/01, EU:C:2003:596, paragraph 96); of 16 December 2008, *Huber* (C−524/06, EU:C:2008:724, paragraph 51); of 24 November 2011, *Asociación Nacional de Establecimientos Financieros de Crédito* (C−468/10 and C−469/10, EU:C:2011:777, paragraph 29); and of 7 November 2013, *IPI* (C−473/12, EU:C:2013:715, paragraph 31).

---

15 Judgment of 6 November 2003, *Lindqvist* (C−101/01, EU:C:2003:596, paragraph 97).

---

16 See my Opinion in *Dzivev* (C−310/16, EU:C:2018:623, points 72 and 74).

---

17 Reproduced above at point 8.

---

18 See again the examples given above, footnote 12.

---

19 Which are, pursuant to Article 28 of Directive 95/46, responsible for monitoring the application of the provisions adopted pursuant to that directive.

---

20 On the standard required under Article 28(1) of Directive 95/46, see judgments of 9 March 2010, *Commission* v *Germany* (C−518/07, EU:C:2010:125, paragraphs 18 to 30), and of 16 October 2012, *Commission* v *Austria* (C−614/10, EU:C:2012:631, paragraphs 41 to 66).

---

21 By analogy with another area of law, would for example private enforcement of competition law then also threaten the independence of (national) competition authorities? See judgments of 20 September 2001, *Courage and Crehan* (C−453/99, EU:C:2001:465, paragraphs 26 to 27 and 29), and of 13 July 2006, *Manfredi and Others* (C−295/04 to C−298/04, EU:C:2006:461, paragraphs 59 to 60). See also recital 5 of Directive 2014/104/EU of the European Parliament and of the Council of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union (OJ 2014 L 349, p. 1).

---

22 In general (irrespective of the specific issue of changed legal form), what does the fact that the legislature inserted something into a subsequent piece of legislation, that was not present in the previous embodiments of the same, mean for the interpretation of the latter? It may well be that that principle was indeed ‘inherently present’ in the previous embodiment and now has just been clarified. But it may also mean that precisely because that provision was not previously present, the new one is an amendment. In view of the frequent and questionable (mis)use of the argument ‘it has always been there, now it is just explicit’, in effect amounting to an extension of the new rule well before its temporal scope of application, such type of arguments should be used with caution, if at all.

23 Concerning the issue of *dynamic* IP addresses, see judgment of 19 October 2016, *Breyer* (C−582/14, EU:C:2016:779, paragraph 33 et seq.). See also judgment of 24 November 2011, *Scarlet Extended*(C−70/10, EU:C:2011:771, paragraph 51).

24 Judgment of 19 October 2016, *Breyer* (C−582/14, EU:C:2016:779, paragraphs 41 to 45).

25 Above, point 19.

26 Emphasis added.

27 Judgments of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein* (C−210/16, EU:C:2018:388, paragraph 29), and of 10 July 2018, *Jehovan todistajat* (C−25/17, EU:C:2018:551, paragraph 65).

28 See judgments of 13 May 2014, *Google Spain and Google* (C−131/12, EU:C:2014:317, paragraph 34), and of 10 July 2018, *Jehovan todistajat* (C−25/17, EU:C:2018:551, paragraph 66).

29 Judgment of 5 June 2018 (C−210/16, EU:C:2018:388).

30 Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein* (C−210/16, EU:C:2018:388, paragraph 39).

31 Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein* (C−210/16, EU:C:2018:388, paragraph 35).

32 Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein* (C−210/16, EU:C:2018:388, paragraph 36).

33 Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein* (C−210/16, EU:C:2018:388, paragraphs 34 and 38).

34 Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein* (C−210/16, EU:C:2018:388, paragraphs 39 and 41).

35 Judgment of 10 July 2018 (C−25/17, EU:C:2018:551, paragraphs 68 to 72).

36 As suggested by Advocate General Bot in his Opinion in *Wirtschaftsakademie Schleswig-Holstein* (C−210/16, EU:C:2017:796, points 66 to 72).

37 With apparently an analogy with consumer protection, meaning that in terms of negotiation, the ‘non-professional’ party should have same genuine say in negotiating the terms, does not appear to be applicable in

this context. Thus, it is open to debate how much actual 'definition of parameters' there is for a fan page administrator (and how much is just mechanical clicking and choice between prepared options, as with any other 'consumer').

38 Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein* (C−210/16, EU:C:2018:388, paragraph 35).

39 A number of programmes and applications nowadays, with the sometimes explicit, sometimes perhaps less explicit, agreement of the user, transmit analytical information, that may include personal data, to the developer or software vendor.

40 Judgment of 5 June 2018 (C−210/16, EU:C:2018:388, paragraph 38).

41 Again, under what exact conditions and with what negotiation power might indeed be open to debate (see also above footnote 37).

42 Or, as put in less candid terms by Sir Humphrey Appleby (himself apparently relying on an older, unattributed quote): 'Responsibility without power — the prerogative of the eunuch throughout the ages' (In *Yes, Prime Minister*, Season 2, Episode 7, 'The National Education Service', first aired 21 January 1988).

43 Also in the sense outlined above at point 73 and footnotes 38 and 42.

44 Judgment of 5 June 2018 (C−210/16, EU:C:2018:388, paragraph 43).

45 See above, points 87 to 88.

46 See also Article 29 Data Protection Working Party (an advisory body established by Article 29 of Directive 95/46, now replaced by the European Data Protection Board, set up under Article 68 of the GDPR) Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, 20 June 2007, p. 4.

47 Also in view of the simple fact that processing will hardly ever be linear, going through all of the operations listed in Article 2(b) one by one, in sequence, and by one person. Rather, the life of personal data is likely to be cyclical, running in loops, with bifurcations here and there, with data sets collected at different ends, consulted by a different person, subsequently merged and consulted, then later, again perhaps re-combined and retransmitted to different persons, and so on.

48 The Article 29 Data Protection Working Party suggested that 'joint control will arise when different parties determine with regard to specific processing operations either the purpose or [the] essential elements of the means'. See Opinion 1/2010 on the concepts of 'controller' and 'processor', adopted on 16 February 2010, Article 29 Data Protection Working Party, doc. 00264/10/EN WP 169, p. 19.

49 In contrast to the situation discussed with regard to question 1 above at points 39 to 42.

50 Reading the original German version of the fourth question, I understand the scope of the question posed by the referring court as being limited to the identification of interests that are *to be taken into account* and not, as the English translation of the German question would imply, *are decisive* (in the potential sense of carrying more weight) in that balancing of interests. The question thus appears to be enquiring into the input of the balancing exercise, not what its output ought to be.

---

51 Directive of the European Parliament and of the Council of 12 July 2002 (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37).

---

52 See also judgment of 5 May 2011, *Deutsche Telekom* (C−543/09, EU:C:2011:279, paragraph 50). Pursuant to recital 10 of the E-Privacy Directive, 'in the electronic communications sector, Directive [95/46] applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. Directive [95/46] applies to non-public communications services'.

---

53 See, in this context, Article 5(3) of the E-Privacy Directive which states that 'Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive [95/46], inter alia about the purposes of the processing. […]'.

---

54 In this context again cross-referring to the introductory Section B.1. (points 55 to 58 above) and the need for factual verification of what exactly is being transmitted and whether that information in fact amounts to personal data.

---

55 See also Article 29 Data Protection Working Party Document 02/2013 providing guidance on obtaining consent for cookies, 1676/13/EN WP 208, 2 October 2013, pp. 5 to 6, suggesting that 'since storing information or gaining the information already stored on users' devices by way of cookies can entail the processing of personal data, in this case data protection rules clearly apply'.

---

56 See, in this sense, judgments of 13 May 2014, *Google Spain and Google*(C−131/12, EU:C:2014:317, paragraph 71 and the case-law cited), and of 4 May 2017, *Rīgas satiksme* (C−13/16, EU:C:2017:336, paragraph 25).

---

57 Judgment of 4 May 2017, *Rīgas satiksme* (C−13/16, EU:C:2017:336, paragraph 28). See also judgment of 24 November 2011, *Asociación Nacional de Establecimientos Financieros de Crédito* (C−468/10 and C−469/10, EU:C:2011:777, paragraph 38).

---

58 See my Opinion in *Rīgas satiksme* (C−13/16, EU:C:2017:43, points 64 and 65). As I recalled there, transparency (judgment of 9 November 2010, *Volker und Markus Schecke and Eifert* (C−92/09 and C−93/09, EU:C:2010:662, paragraph 77)), protection of the property, health and family life (judgment of 11 December 2014, *Ryneš* (C−212/13, EU:C:2014:2428, paragraph 34)) have been acknowledged as such by the Court. See also judgments of 29 January 2008, *Promusicae* (C−275/06, EU:C:2008:54, paragraph 53), and of 4 May 2017, *Rīgas satiksme* (C−13/16, EU:C:2017:336, paragraph 29).

---

59 See above, points 104 to 105 of this Opinion.

60 See also Opinion 06/2014 of Article 29 Data Protection Working Party on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (844/14/EN WP 217), p. 25.

61 As I suggested elsewhere, the respective 'competing legitimate interests need not only to be established, but also to outweigh the interests or rights and freedoms of the data subject', arising from Articles 7 and 8 of the Charter. See my Opinion in *Rīgas satiksme* (C−13/16, EU:C:2017:43, point 56 and points 66 to 69 and the case-law cited).

62 Judgment of 4 May 2017, *Rīgas satiksme* (C−13/16, EU:C:2017:336, paragraph 31 and the case-law cited).

63 There must thus be an adequate relationship between the aims (the claimed legitimate interest) and chosen means (personal data processed). See in this sense judgment of 4 May 2017, *Rīgas satiksme* (C−13/16, EU:C:2017:336, paragraph 30 and the case-law cited).

64 Above, points 76 to 82 of this Opinion.

65 Above, points 84 to 88.

66 Which of course does not preclude, other potential (and subsequent) controllers having that duty with regard to their respective data processing operations.

67 Above, point 132. See Article 29 Data Protection Working Party Document 02/2013 providing guidance on obtaining consent for cookies, 1676/13/EN WP 208, 2 October 2013, p. 4. See also Article 29 Data Protection Working Party Document Opinion 15/2011 on the definition of consent 1197/11/EN WP187, 13 July 2011, p. 9.