

A Hidden Revolution

Merlin Gömann

2021-06-17T18:24:26

European data protection law has become (in-)famously known as one of the main tools for both the European legislature and the European Court of Justice (ECJ) to push the boundaries of European integration. The most recent decision of the Court in [Case C-645/19](#), 15 June 2021 – Facebook Ireland continues this well-established tradition. By contrast to other ground-breaking judgments such as [Digital Rights Ireland](#), [Google Spain](#) or [Schrems I](#) and [II](#), its revolutionary aspects do however not catch the eye, but lie in the consequences of what may at first glance appear as a rather technical ruling. Thus, the following analysis will not limit itself to the direct consequences of the judgement, but shed some light on its revolutionary implications for the conflict of Member States' GDPR adaptation laws. Under the complex system of international competence set up by the GDPR, national data protection authorities (DPAs) may find themselves obliged to enforce foreign (public) law domestically – an unprecedented step for the ever-closer integration of the EU's legal order.

The ECJ's Judgment in Case C-645/19 – Facebook Ireland

Backdrop to the decision is another dispute about the processing of personal data by Facebook, established on EU territory with two entities relevant to the case, one in Ireland – where art. 4(16)(a) GDPR considers Facebook's "main establishment" – and one in Belgium. Unlike the former, assuming full responsibility for all processing operations concerning European users (para. 86), the latter primarily allows the group to engage with EU institutions and secondarily promotes advertising and marketing in Belgium (paras. 92 et seq.). Both entities had initially been sued under the GDPR's predecessor, the [Data Protection Directive](#), by what under the GDPR has become the Belgian DPA in front of Belgian courts for infringing substantive (Belgian) data protection law. With the entry into force of the GDPR, the defendants claimed that the Belgian DPA had lost its competence to bring the action, relying on the so-called "one-stop-shop" mechanism set up under art. 56, 60 GDPR. According to Facebook, only the lead supervisory authority at its main establishment, i.e. the Irish Data Protection Commission, was entitled to enforce the GDPR against it, including by initiating court proceedings under art. 58(5) GDPR. The referring [Brussels Court of Appeal](#) therefore essentially inquired whether the GDPR actually prevented other national DPAs from pursuing court proceedings for GDPR violations arising from cross-border processing operations (for further information on the facts of the case see [here](#)).

Based on a thorough analysis of the GDPR's competence regime (art. 55 et seq GDPR, paras. 47 et seq.) and its compatibility with art. 7, 8 and 47 of the Charter of Fundamental Rights (paras. 66 et seq.), the ECJ holds that Member States' supervisory authorities merely "concerned" by a certain processing operation

(art. 4(22) GDPR) may indeed take their own enforcement action after mutual assistance of the lead supervisory authority has been sought unsuccessfully, i.e. because the latter does not provide the requested information in due time (para. 71). In such a situation, the concerned DPA may immediately adopt a provisional measure for the territory of its own Member State under art. 61(8), 66(1) GDPR (cf. [this](#) recent preliminary order by the DPA of Hamburg). However, to adopt final measures such as the initiation of court proceedings under art. 58(5) GDPR, it is bound by art. 66(2) GDPR to first request an affirmative urgent opinion or binding decision from the European Data Protection Board (EDPB). In less urgent cases of insufficient cooperation, the necessary approval by the EDPB can however only be requested under the additional conditions of art. 64(2) GDPR, i.e. that the matter is of general application or produces effects in more than one Member State. Once again,¹⁾Cf. [Case C-210/16](#), 5 June 2018 – Wirtschaftsakademie Schleswig-Holstein, paras. 50 et seq. the Court eventually refuses to further address the remaining risk of conflicting decisions on the same processing operation arising from different national DPAs acting under such parallel (urgency) competence (paras. 114 et seq.).

Overall, the ECJ's decision breathes real life into the complex structure of international cooperation between European data protection authorities set up by the GDPR. First and foremost, the ECJ, in line with [AG Bobek](#) (paras. 53 et seq.), emphasises the primacy of the one-stop-shop mechanism established by art. 56, 60 GDPR (paras. 50 et seq., 65). Simultaneously, the Court significantly increases the pressure on lead supervisory authorities popular among corporate controllers to neither delay (joint) enforcement action nor to settle too early or for too little (paras. 71, 74). In doing so, the ECJ joins a long list of opponents to the current enforcement practice of certain one-stop-shops, including the Irish and the Luxemburgish DPA (see, amongst others, the [European Parliament](#), the [German Federal Commissioner for Data Protection Ulrich Kelber](#) and [noyb](#)). Notably, the Court does not stop at highlighting the one-stop-shop mechanism's reliance on "effective" cooperation between the lead and other supervisory authorities concerned, but additionally demands "sincere" cooperation (paras. 53, 60, 63, 72), thereby going beyond the pure letter of the GDPR (see [here](#), as well as art. 4(3) TEU). However, as the primacy of the one-stop-shop is also strengthened by the emphasis on the procedural hurdles other DPAs are confronted with when considering to take action, the judgment can indeed be described as striking a fair balance with regard to the much disputed international competence of DPAs (cf. [here](#), [here](#) and [here](#)).

The Hidden Revolution

The much less discussed but much more decisive question for European integration is however left unexamined by the ECJ: If a supervisory authority merely "concerned" in the sense of art. 4(22) GDPR – such as the Belgian DPA in the case at hand – becomes (exceptionally) competent to assess a given processing operation under art. 56(2), 66 GDPR, according to which law is this assessment to be conducted? Only at first sight can this question be answered by turning to art. 288(2) TFEU, according to which the GDPR's harmonising provisions are uniformly and directly applicable to any processing within its (external) scope of

application. At a second glance, however, it becomes apparent that the GDPR forms a so-called “limping” regulation. Despite the restrictive interpretation advisable in this regard, Member States frequently enjoy a broad regulatory leeway (see, for instance, art. 6(3), art. 8(1), art. 9(4), art. 23(1), art. 85 GDPR). Thus, for the vast majority of processing operations – including those at stake in case C-645/19 – the (internal or intra-European) conflict of laws question arises as to which supplementary national adaptation law to apply.

1. Convergence between Competence and Applicable Law?

An obvious answer would be for each competent DPA to apply the adaptation law of its respective Member State. In the situation at hand in Case C-645/19, however, this would have meant that the applicable national adaptation law would have changed with the rejection of competence by the Irish authority, making the Belgian DPA competent and thus Belgian adaptation law applicable. This solution would leave it in the hands of the respective one-stop-shop to either subject certain processing operations to their own or to foreign adaptation law by assuming or rejecting the lead under art. 56(3) GDPR. Such a situation would already be incompatible with the principle of legal certainty, requiring both the data subject and the controller be able to determine which rights and obligations they are subject to prior to a processing operation. The urgency competences under art. 66 GDPR would lead to a further multiplication of (potentially) applicable adaptation laws, only (and suddenly) becoming decisive whenever a DPA deemed itself competent to act. Lastly, on top of the *forum shopping* rightly undesired by the Court (para. 68), this approach would in principle allow the controllers to *statute shop* the applicable national adaptation law, potentially leading to a *race to the bottom* with devastating consequences for the overall protective level of national adaptation law.

2. National Conflict Rules?

To fill the looming gap, several – but not all (cf. Irish Data Protection Act 2018; [Romanian Lege nr.190 din 18 iulie 2018](#)) – Member States have adopted autonomous conflict rules, providing for their national adaptation laws to be applicable under very different circumstances (cf. art. 4 [Belgian Loi du 30.7.2018](#); art. 3 [French Loi n° 78-17](#); § 1(4) [German BDSG](#); Art. 1 S. 1 [Polish Ustawa z dnia 10 maja 2018](#); to name just a few). If valid, such divergent national rules would however lead to several *accumulations* as well as to *lacks* of applicable national adaptation laws, equally incompatible with the GDPR’s twofold main objective of effectively protecting fundamental rights (art. 1(1), (2) GDPR) while ensuring free movement of personal data within the internal market (art. 1(1), (3) GDPR). By enacting several provisions such as art. 6(3)(b) GDPR, providing for an application of the “law to which the *controller* is subject”, and art. 61(4)(b) GDPR, declaring applicable the “law to which the *supervisory authority* [...] is subject”, the EU legislature has however exercised its (shared) competence under art. 16(2)(1) TFEU to adopt internal conflict of laws rules within the scope of the GDPR. Despite their high degree of abstraction, intra-EU conflict of (adaptation) laws is therefore a Union-regulated element barred for the Member States according to art. 2(2) TFEU. Thus, insofar as they concern the application of national adaptation laws, the conflict rules nevertheless adopted by the Member States are inapplicable and must be repealed.

3. Applying Private International Law?

No further concretisation of the GDPR's abstract internal conflict results either from direct or indirect recourse to the rules of European Private International Law (PIL) – mainly Regulations Rome I and II. This is because, first, due to diverging aims and fundamental methodological discrepancies no *lex specialis* relationship can be established between these private and the public conflict of law rules required to determine the applicable national adaptation law under the GDPR, traditionally unilateral and more abstract in scope. Second, these discrepancies also impede recourse to single PIL provisions to solve the internal conflicts of public (adaptation) laws arising under the GDPR by way of systematic interpretation. Third, only a very limited gain in concretisation would follow from such an exercise anyway.

4. The Application of art. 3 GDPR by Analogy

As explained in more detail [here](#), the only viable solution to this dilemma consists in a Union-wide uniform definition of exactly one applicable national adaptation law per processing operation. This alone ensures that substantive (adaptation) law does not change with the competent authority and that legal certainty as well as the GDPR's main objectives are not undermined by an accumulation or lack of applicable laws. Although the GDPR – by contrast to its predecessor (cf. art. 4(1) DPD) – does not provide for a rule explicitly addressing such internal conflicts, it does regularly point at the application of the “law to which the controller is subject” (i.e. at art. 6(3)(b), art. 14(5)(c), art. 17(1)(e), (3)(b), art. 22(2)(b) GDPR etc.). Still vague in itself, this intra-EU conflicts rule must be fleshed out by applying the external conflict provisions of art. 3 GDPR by analogy, based on the traditional principle of qualified establishment (art. 3(1), (3) GDPR) as well as the newly introduced targeting approach (art. 3(2) GDPR). Although these only concern the territorial scope of application of the GDPR, their underlying concepts are equally suitable to address internal conflicts. Consequently, the national adaptation law applicable to a processing operation falling within the GDPR's territorial scope according to art. 3(1) or (3) GDPR is the one of the Member State in which the controller is qualifiedly established, whereas operations within the scope of application of art. 3(2) GDPR are governed by the adaptation law of the Member State(s) targeted by the controller.

The ECJ's openness to this solution is reflected by the fact that it surprisingly invokes art. 3 GDPR to allow the supervisory authority concerned to “exercise [...] the power conferred [...] in Article 58(5) [GDPR]” (para. 90). As the territorial applicability of the GDPR under art. 3(1) GDPR is indisputably triggered by the Irish main establishment anyhow, establishing this additional prerequisite for an enforcement action of the Belgian DPA shows that the ECJ (rightly) strives to ensure a sufficiently close connection between the processing operation at stake and the DPA in charge. That said, the Court immediately renders its legitimate concern absurd by applying its usual extensive interpretation of art. 3(1) GDPR (paras. 91-95), thereby virtually abandoning any limiting effect of the newly introduced condition. Instead, a more restrictive interpretation of art. 3(1) GDPR departing from the ECJ's case law²⁾ [Case C-210/16](#), 5 June 2018 – Wirtschaftsakademie Schleswig-Holstein, para. 56, [Case C-230/14](#), 1 October 2015 – Weltimmo, para. 25, [Case](#)

[C-131/12](#), 13 May 2014 – Google Spain, para. 53. would be called for, not least to limit the GDPR's (extra#)territorial scope of application (cf., amongst others, [here](#), [here](#) and [here](#)). What is more, even the most legitimate concern cannot hide the fact that neither art. 58(5) GDPR nor art. 55(1), 56, 60 GDPR require the local establishment in the Member State of the competent authority to trigger art. 3(1) GDPR by itself. Thus, the missing territorial link should not have been sought in (the restriction of) the supervisory authority's competence, but rather in identifying the applicable national adaptation law.

Consequences

Even if a merely “concerned” supervisory authority (art. 4(22) GDPR) is exceptionally vested with competence under art. 56(2), 66 GDPR for a specific processing operation under the conditions outlined by the ECJ, the applicable adaptation law is to be determined separately, applying art. 3 GDPR by analogy as outlined above. In consequence, within the regulatory leeway left by the GDPR – which, as mentioned, is considerable – the DPA thus competent may have to enforce *foreign substantive adaptation law*. Since this primarily concerns provisions of *public law* balancing the relationship between the fundamental right to data protection and conflicting fundamental rights such as the freedoms of expression, information and press (Art. 85 GDPR), this represents an unprecedented step for European integration (which was, however, already anticipated by [AG Cruz Villalón](#))³⁾ Opinion in Case C-230/14, 25 June 2015 – Weltimmo, para. 50.. Unlike traditional (European) PIL, which governs the application of foreign *private law* mostly by civil courts, in this case the conflicts rules primarily address the DPAs required to enforce foreign public (data protection) law (as well as, secondarily, the courts overseeing them), and in doing so having to consider the influence of foreign fundamental rights. This is perfectly illustrated by the case at hand: if the Belgian DPA were competent to examine certain processing operations on the exceptional grounds specified by the ECJ, it would have to do so by enforcing Irish adaptation law applicable to these operations according to art. 6(3)(b) GDPR et al. read in conjunction with art. 3(1) GDPR, applied by analogy.

The application of foreign *substantive law* is however without prejudice to the *procedural law* governing the administrative procedure initiated by the competent DPA. By contrast to the former, the latter does indeed follow the provisions on the competence of the national supervisory authorities (art. 55 GDPR et seq.), in full compliance with the principle of Member States' procedural autonomy rooted in art. 291(1) TFEU. When enforcing the applicable (foreign) substantive adaptation law, competent DPAs thus continue to adhere to their national procedural rules (cf. art. 61(4)(b): “Member State law to which the supervisory authority [...] is subject”, as well as art. 58(1)(f), (4), art. 62(3), recital 143 s. 7 GDPR). What emerges is a schism between applicable substantial and procedural law, already familiar from PIL (*forum regit processum* or *lex fori* principle). This entails the need to qualify a specific national provision as procedural or substantive, a task that cannot be accomplished in the abstract but only with due regard to the regulatory content of the provision concerned.

Conclusion

By not addressing which national adaptation law is to be applied to a certain processing operation and, thus, enforced by the competent DPA, the ECJ in its most recent decision ignores the key element for a coherent and consistent application of data protection law under the GDPR. This is especially regrettable given that the Court appears particularly concerned to ensure a sufficient intra-European connection between the processing operation at stake and the data protection authority (subsidiarily) competent for its supervision.

However, the hidden revolution triggered by the special legal structure of the “limping” GDPR with both its broad regulatory leeway and complex system of international competence does not fail to materialise: for the first time in the history of the EU, Member State (data protection) authorities, as well as the courts overseeing their activities are required to systematically enforce foreign public law domestically. It remains to be seen whether this will set a new precedent for the ever-closer integration of the EU or lead to a greater willingness of the Member States to abolish the GDPR’s regulatory leeway, thereby further harmonising data protection law at EU level.

The key arguments of this post build upon the author’s doctoral thesis, which is [about to be published](#) in German.

The author wishes to sincerely thank Maxim Bönnemann, Filippo Mattioli and Andrew Wright for their very valuable comments on an earlier draft of this post.

References

- Cf. Case C-210/16, 5 June 2018 – Wirtschaftsakademie Schleswig-Holstein, paras. 50 et seq.
- Case C-210/16, 5 June 2018 – Wirtschaftsakademie Schleswig-Holstein, para. 56, Case C-230/14, 1 October 2015 – Weltimmo, para. 25, Case C-131/12, 13 May 2014 – Google Spain, para. 53.
- Opinion in Case C-230/14, 25 June 2015 – Weltimmo, para. 50.

