SIMONT | BRAUN

JURISDICTION, TERRITORIALITY AND DATA PROTECTION

Christopher Dumont & Eric De Gryse | Sept. 2020

The Belgian Google case: an interesting take on the application of European data protection law to transnational companies

Executive summary | This article deals with the private international law aspects in the Belgian Google case. With its decision of 14 July 2020, the Belgian Data Protection Authority confirms it is competent to hear a complaint filed against Google's Belgian subsidiary, Google Belgium SA, even though the latter does not determine the purposes and means for the processing - which is determined solely by Google LLC, the mother company located in California. The reasoning of the Authority is three-ponged. First, it establishes that European data protection rules apply to the processing activity in question by applying the case law of the European Court of Justice. This results in the Authority having jurisdiction over the alleged infringement, conditional on the fact that the "one-stop-mechanism" would not be applicable. Then, the Authority establishes that the "one-stop-mechanism" does not apply and that there is thus no lead supervisory authority as the company responsible for the processing activity in question (i.e. Google LLC) is not established in the European Union. Lastly, it establishes that the complainant could bring a complaint only against Google Belgium SA because of the inextricable link between Google Belgium SA and its mother company Google LLC, the ambiguity created by Google itself and the need for effective recourse for European data subjects. An appeal against the decision is currently pending before the Brussels Court of Appeal, section Market Court. A decision definitely worth keeping an eye out for.

INTRODUCTION

Old, but not forgotten. On 14 July 2020, the Belgian Data Protection Authority (Autorité de protection des données / Gegevensbeschermingsautoriteit, hereinafter "BDPA" or the "Authority") published a decision in a case involving Google following a failure to erase personal data as requested by a data subject (you can read the decision here). Google was found to breach multiple provisions of the General Data Protection Regulation (hereinafter "GDPR"). After an extensive review of the facts and interests at

stake, the BDPA imposed a fine of 600k. Not surprisingly, the decision of the BDPA received widespread media attention. The fine imposed on Google is the highest fine to date.

The decision comprises an interesting aspect of private international law. Transnational companies pose multiple problems for national authorities. One of them is the complexity to determine where the processing takes place. The division of tasks within those companies is not always clear. Those questions were precisely what the Authority had to address in the case at hand. Before establishing a breach and being able to impose a fine, the BDPA first had to address whether it had jurisdiction as to such a breach under the GDPR. This is not new. The debate takes place in the bigger context of European countries struggling to ensure proper application of their national rules against transnational companies. It provides us the opportunity to review the rules of jurisdiction and their functioning in the context of data protection.

The analysis of the BDPA is without a doubt of keen interest to many data protection lawyers, data protection officers, academics and companies, not only in Belgium but across the world.

After a short description of the case at hand **(I)**, we will remind the applicable rules of jurisdiction and applicable law and its evolution in the context of data protection **(II)**. Finally, we will describe how the BDPA applied them in its decision **(III)**.

I. FACTS

The facts leading to the case are quite simple and resemble a common scenario. When looking for information about the complainant on Google - by using his name and surname -, the search results referenced websites revealing personal information about the complainant that he wished others would not see when "googling" his name. The search results were deemed harmful to his honour and reputation.

More concretely, the case concerned a Belgian citizen, heading a big company at the time of the dispute, who had previously been in charge of several public positions and was a member of a Belgian political party, which a series of google search results referred to. In addition to that, some search results referred to articles that described how a complaint for harassment had been directed against him, which had been dismissed. Those websites were all referenced on Google.

The complainant sent Google a request to dereference a number of websites. He used the online form made available by the Google search engine created specifically for people to exercise their "right to be forgotten", which is directly managed by Google LLC, the parent company located in California.

After examining the request, Google refused for various reasons, such as pages that were inaccessible, or which did not meet Google's criteria for removal, but also on the ground of the public's right to information, with considerations for the fact that the complainant is a public figure.

Following Google's refusal, the complainant filed a complaint against Google's Belgian subsidiary, Google Belgium SA, with the BDPA, aimed at obtaining the effective dereferencing of the websites at stake.

Preliminary central points of discussion during the proceedings were whether or not the complaint should have been directed against Google Belgium SA, Google LLC or Google Ireland Ltd and whether or not the BDPA had jurisdiction with regard to those parties.

II. RULES OF JURISDICTION AND APPLICABLE LAW

Although the question of jurisdiction of Member States' courts and authorities is not new and many issues had already been raised and solved under the regime of Directive 95/46/EC (see more in detail below), it is the first time the question of the BDPA's jurisdiction is dealt with in Belgium.

Under the directive it was not mandatory for the Member States to grant corrective powers to their data protection authorities, such decision being left at their own appreciation. In Belgium, no such powers had been recognised to the Authority under the Privacy Act of 8 June 1992. Its role at the time was mainly advisory. One exception was the ability of the President of the Authority to file a suit with civil courts in Belgium.

Such power had been used to launch a case against Facebook Belgium BVBA, Facebook Ireland Ltd and Facebook Inc[1]. At the time, the Brussels Court of Appeal had dismissed it on grounds of lack of jurisdiction of the Belgian courts. Facing the absence of clear rules of jurisdiction, the Brussels Court of Appeal had applied the general regime of private international law to consider that:

- The action of the Authority was of a public nature, which excluded the application of both the Brussels Ibis Regulation[2] and of the Belgian Code of Private International Law;
- Such exclusion still allowed the Court to have jurisdiction as to the complaints directed towards Facebook Belgium BVBA when it comes to its own behaviour since it was a purely internal situation. This, however,

1 Brussel, 8 mei 2018, R.D.C.-T.B.H., 2020, nr. 1, p. 75.

2 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, Pb.L. 20 december 2012, issue 351, 1.

could only lead to sentencing actions which the Belgian company was directly and personally responsible for;

- Also, the Court found no ground of jurisdiction as to the case filed against Facebook Ireland Ltd and Facebook Inc and, therefore, declared itself incompetent.

This approach, combined with the lack of power of the Authority to impose administrative fines, actually led to a lack of effective recourse in Belgium against breaches committed by transnational companies.

The GDPR brought forward an improvement in this regard:

- First, it gave corrective powers to all national data protection authorities of the different Members States, effectively offering an additional recourse to data subjects;

- It drew clear rules of jurisdiction and applicable law, building upon earlier case law of the European Court of Justice (hereinafter "CJEU") under Directive 95/46/EC; and

- It created a general competence for "lead supervisory authority" when it comes to cross-border processing carried out by data controllers or processors whose main establishment is located in their territory.

Under the GDPR, the European data protection rules are applicable to "*processing of personal data in the context of the activities of an establishment of a controller or a processor in the European Union, regardless of whether the processing takes place in the European Union or not*" (art. 3.1 GDPR). They are also applicable to "*processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the European Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the European Union*" (art. 3.2 GDPR).

Article 55 GDPR provides that "*each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State*". Recital 122 of the GDPR clarifies that this should cover in particular "*processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing on its territory*".

These provisions result from previous case law of the CJEU under Directive 95/46/EC. The first and most well-known case rendered was the Google Spain judgment (CJEU, 13 May 2020, C-131/12, *Google Spain et Google Inc v. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*).

In this decision, the Court considered that the promotion of the processing activities of Google Inc by its Spanish subsidiary (offering advertising space to make the search engine profitable) was sufficient for considering the latter as an establishment in the sense of Directive 95/46/EC. Consequently, in this case, Spanish law was applicable to the processing undertaken by Google.

Later, in its *Weltimmo* judgement, the CJEU stated that any national law on the protection of personal data applies where the data controller exercises, "*through stable arrangements in the territory of that Member State, a real and effective activity — even a minimal one — in the context of which that processing is carried out*" (CJEU, 1 October 2015, C-230/14, *Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*). Where their national law is applicable, data protection authorities may exercise effective powers of intervention (e.g. impose penalties) on the data controller or processor within the territory of their own Member State.

The combined effect of those cases strengthened the power of data protection authorities to enforce European data protection law on transnational companies, provided that the transnational companies exercised part of their activity through an establishment in that territory. This would apply even if the local entity's activities merely consists in advertising the services of its parent company (the data controller). It is, therefore, not required that the said establishment actively participates in the processing of personal data, as later confirmed in the *Wirtschaftsakademie* judgment (CJEU, 5 June 2018, C-2010/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH*).

It is the application of those rules that the BDPA had to consider for the first time in the present decision.

III. THE ANALYSIS OF THE BDPA

As explained above, in the case at hand, the BDPA had to determine whether or not it had jurisdiction with regard to the refusal of Google to dereference the websites at stake.

First, the BDPA examined whether or not the GDPR was to be applied. Territoriality is an important principle of the GDPR. The territorial competence stems from the principle in international public law where a State only has competence to enforce the law on its own territory. On that point, when interpreting article 3 GDPR, the BDPA observed a legal gap. The law does not address the situation where a data controller having an establishment in the European Union, does not process personal data as part of the activities of that establishment. Applying the case law of the CJEU, the BDPA concluded that the GDPR was applicable because (i) the complainant resided in the

European Union, and that (ii) otherwise, if the GDPR did not apply, no adequate, nor full protection could be offered to data subjects.

The next step consisted in determining whether the "one-stop shop" mechanism of article 56 GDPR applied. In other words, whether the BDPA lacked competence because another data protection authority enjoyed a prevailing jurisdiction as a lead supervisory authority. Google argued that this was the case, since the company had chosen its main establishment in Ireland through Google Ireland Ltd. Going through a detailed analysis of the division of tasks between the various companies (Google Inc LLC, Google Ireland Ltd, Google Belgium SA) the BDPA concluded that Google Ireland was not responsible for the processing at stake, i.e. (de)referencing results on the Google search engine. The responsibility for the functioning of the Google search engine and its three phases, namely exploration, indexation and selection of results, falls solely with Google LLC. Google Ireland only processes data for modifying the search results based on the search history of users. It thus concerned a different processing activity than the one in dispute, for which Google Ireland Ltd could not be seen as the main establishment in the sense of article 4.16 GDPR. This line of reasoning has been confirmed by the Council of State in a parallel case against Google in France by a decision of 19 June 2020. The Council of State held that the "one-stop shop" mechanism was not applicable. It confirmed that the French data protection authority ("CNIL") was competent to impose a €50 million sanction on Google LLC (you can read the decision here).

Finally, the BDPA had to consider whether or not it was competent to hear the complaint filed specifically against Google Belgium SA and not against Google Inc or Google Ireland Ltd. For this part, the BDPA relied on the Google/CNIL judgement of the CJEU (CJEU 24 September 2019, C-507/17, *Google LLC v. Commission Nationale de l'Informatique et des Libertés (CNIL)*) to allow the complaint by virtue of the inextricable link between Google LLC and Google Belgium SA, and the requirement of adequate and complete protection of data subjects. It was not disputed that Google Belgium SA constituted a "stable establishment" in Belgium. It was also established that the processing was indeed carried out in the context of the activities of the Belgian establishment. The BDPA highlights the international reach and the ambiguity created by Google itself which made it difficult to clearly differentiate the responsibilities of the different entities within the Google group. Therefore, even though Google Belgium SA does not determine the purposes and means for the processing - which is determined solely by Google LLC – the inextricable link and the need for effective recourses that had been highlighted in the *Wirtschaftsakademie* judgement justified that the complainant directed his complaint to Google Belgium SA alone. In the BDPA's view, it is of little importance whether the processing of the data is actually performed outside the European Union by Google LLC employees.

Particular in the reasoning of the BDPA, is that "*as its activities are inextricably linked to those of Google LLC, the Belgian subsidiary – given the role*

it plays and itself describes – can be treated in the same way as a data controller for processing conducted within the context of the operation of Google's search engine and responses to delisting requests in Belgium". In these circumstances, Google Belgium SA is responsible for ensuring the compliance of the GDPR in Belgium.

IV. OTHER ASPECTS OF THE DECISION

The decision also deals with other interesting aspects such as the balance of interests between the "right to information" and the "right to be forgotten", the territorial reach of the dereferencing request (cf. Google/CNIL judgement) and the criteria for determining the height of the fine.

The decision was published on the website of the BDPA because of "*the importance of transparency in decision-making process and the decisions of the Litigation Chamber, and in light of the scope of this decision, which concerns a very large number of data subjects – i.e. all Belgian residents, and by extension all residents of the EEA – who might be listed by Google's search engine in search queries using their first and last names as keywords*". In the case at hand, the BDPA has decided not to redact Google's identifying information. This is exceptional. The BDPA is of the opinion "*that these redactions are necessary to the pursuit of plaintiff's objective, which is to be delisted by Google*". The argumentation of Google Belgium SA that the publication of the decision would be counterproductive and would stigmatise Google was rejected. In the reasoning of the BDPA "*it is relevant to give this decision sufficient publicity to raise awareness among internet users of their rights under the GDPR*".

V. CONCLUSION

The decision, the first one by the BDPA addressing its international jurisdiction since the GDPR entered into force, gives much food for thought. The BDPA confirms it is competent to hear a complaint filed against Google's Belgian subsidiary, Google Belgium SA, even though the latter does not determine the purposes and means for the processing - which is determined solely by Google LLC, the mother company located in California -.

In its reasoning, the BDPA considers all the existing case law and incorporates it in the recent legal development of data protection law. The BDPA comes up with a practical solution combining a strict legal formalism and the needed considerations for the right to an effective recourse recognised by the GDPR. For David Stevens, the president of the BDPA, this case is of great importance:

> *"This decision is not only important for our Belgian citizens, it also demonstrates our ambition to better protect online privacy together with our fellow European regulators. Concrete actions against such global players are therefore required. In this way, we want to actively contribute to a true data protection culture on a European level as well."* (you can read the article here)

The decision of the BDPA has the potential to significantly impact the way in which global organisations should be thinking about their data protection strategy in Europe.

It remains to be seen if this line of reasoning will be confirmed by the Brussels Court of Appeal, section Market Court. In appeal, it is highly likely that a prejudicial question will be asked to the CJEU regarding the interpretation of the GDPR. In the parallel case in France, Google requested the Council of State - but was denied - that the following question would be asked:

> *"Can a controller established in a country outside the European Union with several establishments in the European Union and a designated European registered office in the territory of a Member State have a "main establishment" within the meaning of Article 4(16) of the GDPR in that Member State in the event that decisions on the purposes and means of processing are taken in that third country?"*

We look forward to seeing more development on this matter.

Christopher Dumont and Eric De Gryse

With the contribution of **Viktor Francq**, summer intern 2020 at Simont Braun

You may always contact us should you have any questions.

edg@simontbraun.eu – +32 2 533 17 52

cdu@simontbraun.eu – +32 2 533 17 58

SIMONT BRAUN

Avenue Louise 250 / 10
1050 Brussels

+32 (0)2 543 70 80

www.simontbraun.eu
Follow us on