



HIGHLIGHT

THE TERRITORIAL SCOPE OF THE RIGHT TO BE FORGOTTEN ONLINE IN THE OPINION OF THE ADVOCATE GENERAL ON THE CASE *GOOGLE CNIL*

GIORGIA BEVILACQUA*

KEYWORDS: right to be forgotten – privacy – freedom of expression – territorial scope – internet – State sovereignty.

On 10 January 2019, the Advocate General of the CJEU delivered his opinion on a new controversial case on the right to be forgotten online (RBF).¹ In its previous judgment on the *Google Spain* case, the Court ruled that, through the RBF, individuals can request search engines to de-reference information about them, which appears following a search for their names, when the search results include information that is “inadequate, irrelevant or no longer relevant, or excessive”.²

This time, the core issue at stake is specifically the interpretation of the territorial scope of this right. Just as in the abovementioned landmark judgment, the case being analysed is between a national data protection authority, the French *Commission Nationale de l'Informatique et des Libertés* (CNIL), and the most widely used internet search engine, Google. Whereas the CNIL ordered the US company to de-reference the relevant pages on all extensions of its search engine domain name, Google removed only search results from the domain name extensions corresponding to EU Member States, such as google.fr, google.it, google.de. The quarrel escalated into a dispute before the *Conseil d'État* which, in turn, on 29 September 2017, submitted a request for a preliminary ruling to the Court of Justice. Essentially, the French highest administrative Court asked whether

* Researcher, Università della Campania Luigi Vanvitelli, giorgia.bevilacqua@unicampania.it.

¹ Opinion of AG Szpunar delivered on 10 January 2019, case C-507/17, *Google LLC*. Cf. A. MIGLIO, *Setting Borders to Forgetfulness: AG Suggests Limiting the Scope of the Search Engine Operators' Obligation to Dereference Personal Data*, in *European Data Protection Law Review*, 2019, p. 136 et seq.

² Court of Justice, judgment of 13 May 2014, case C-131/12, *Google Spain and Google* [GC], para. 93.

a search engine is required to apply de-listing on all domain names, irrespective of the place from which the search, based on the requester's name, is carried out.

In the view of the Advocate General, a search engine operator is not required to implement a request for de-listing of personal information on all extensions of its domain name and "[s]earch requests made outside the territory of the [EU] should not be subject to de-referencing of the search results".³

Preventing worldwide erasure solves several practical, political and legal issues arising from the need to strike a fair balance between the individuals privacy and data protection rights on the one hand, and the freedom of expression rights for both the web publishers and the public on the other hand.⁴ In particular, the Advocate General fears that extraterritorial de-referencing, ruled by a data protection authority (DPA) within the EU, could represent a dangerous precedent for other third States' authorities.⁵ Following the EU example, they could also order global erasure under their own national privacy laws with the consequence of generating internet censorship. Interestingly, just after the judgment in the case *Google Spain*, a law on the RBF entered into force also in Russia.⁶ The fear the Advocate General had could now materialize as this law is being challenged before the Russian Constitutional Court, since it could restrict the free flow of information online in the context of articles on hate crimes that have been removed from Google search results.⁷

The other side of the coin relates to the effectiveness of the RBF. The recommended solution is not consistent with the tendency of DPAs to impose measures with extra-territorial scope in order to provide data subjects with effective and complete protection. As a matter of fact, when de-referencing is limited to EU domains, internet users are still able to access the de-referenced pages by carrying out the search using a non-European extension. Also the IP address geo-localization mechanism proposed by the Advocate General, which varies the protection according to the geographical location of the internet user, is actually ineffective as the de-referenced data remains accessible to all users outside Europe. as well as to those using a foreign IP address.

What seems to be hardly imaginable, is that the RBF can have a geographically limited implementation in the internet which is by its nature worldwide. As clarified in the guidelines adopted by all European DPAs, data subjects are effectively protected against

³ Opinion of AG Szpunar, *Google LLC*, cit., para. 46

⁴ *Ibid.*, para. 58; European Court of Human Rights, judgment of 28 September 2018, no. 60798/10 and 65599/10, *M.L. et W.W. v. Germany*, para. 89.

⁵ Opinion of AG Szpunar, *Google LLC*, cit., para. 61.

⁶ Federal Law no. 264-FZ of 13 July 2015 providing amendments to the Federal Law on information, information technologies and protection of information and to articles 29 and 402 of the Civil Procedure Code of the Russian Federation.

⁷ Article 19, *Russia: ARTICLE 19 Opposes Google in Neo-Nazi 'Right to Be Forgotten' Case*, 28 March 2019, www.article19.org.

the impact of the universal dissemination and accessibility of personal information offered by search engines only when the de-referencing measure affects the whole processing operation carried out by the search engine.⁸ On these grounds, in December 2017 the Italian DPA ordered a worldwide de-listing to effectively protect an Italian citizen resident outside the EU.⁹ In the same year, the Supreme Court of Canada clarified that as “the internet has no borders – its natural habitat is global, [i]f [its] injunction were restricted to Canada alone or to google.ca, the remedy would be deprived of its intended ability to prevent irreparable harm”.¹⁰

In conclusion, the Advocate General tried to set territorial borders in the internet, considering both its growing impact on individuals' private lives and its important contribution to the public debate. Now, the delicate question on whether, and to which extent cyberspace can really be subject to the traditional exercise of State sovereignty is in the hands of the Court.¹¹ In our opinion, long-term effective solutions should consider the peculiar characteristics of such an open and intangible space.

⁸ Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on *Google Spain*, 26 November 2014.

⁹ Garante per la Protezione dei Dati Personali, order of 24 December 2017, no. 557.

¹⁰ Supreme Court of Canada, judgment of 28 June 2017, no. 36602, *Google Inc. v. Equustek Solutions Inc.*

¹¹ M. HILDBRANDT, *Extraterritorial Jurisdiction to Enforce in Cyberspace: Bodin, Schmitt, Grotius in Cyberspace*, in *University of Toronto Law Journal*, 2013, p. 196 *et seq.*

