The wider effect of the 'right to be forgotten' case

Eduardo Ustaran, Partner in the global Privacy and Information Management practice at Hogan Lovells, discusses the implications, for all organisations, of the CJEU's ruling in Google Spain v AEPD

Much has been written about the decision of the Court of Justice of the European Union ('CJEU') regarding Google Spain and the right to be forgotten.

The facts of the case have been explained in depth elsewhere in this edition. In summary: the origins go back to early 2010, when Mr Mario Costeja, a Spanish national, asked Google to remove certain search links to newspaper announcements of 1998 regarding the forced sale of properties arising from social security debts which contained his name. As Google did not action Mr Costeja's request, the Spanish data protection authority became involved, and when it ordered Google to honour the request, Google challenged that order in court. Given the legal complexity of the arguments presented by the parties, the National High Court of Spain referred the matter to the CJEU, which in May 2014 ruled in favour of Mr Costeja and the Spanish authority.

The CJEU took the view that when an individual rightfully objects, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name, links to web pages published by third parties and containing information relating to that person. According to the CJEU, this should be the case even where that name or information is not erased beforehand or simultaneously from those web pages, and when its publication on those pages is lawful.

The CJEU went on to say that the data protection rights of the individual, as a rule, override not only the economic interest of the operator of the search engine, but also the interest of the general public in having access to that information upon a search relating to the data subject's name.

Much of the controversy surrounding this case has focused on the impact of the judgment on freedom of expression and the right of access to information, as well as the potentially devastating effect of a large amount of deletion requests. This is understandable, as with the prospect of an even more demanding EU data protection framework looming over the horizon, the decision is a potential game changer for the whole internet industry.

However, the CJEU's decision is not only relevant to search engines or internet companies. The implications of the judgment are much wider.

Applicability of EU data protection law

For starters, this case has radically shaken the basis on which the applicability of EU data protection law has been understood until now.

The CJEU established that Spanish data protection law applied to Google Inc. (a US corporation) on the basis of the rule set out in Article 4(1)(a) of the Data Protection Directive, which relies on data processing carried out in the context of the activities of an establishment of a controller located in an EU Member State.

In practical terms, the CJEU took the view that, under this rule, there were two conditions for the local law of a Member State to apply. The first one involves having an establishment in a particular country. For these purposes, a local subsidiary or branch (in this case, Google Spain) — no matter how modest — will certainly qualify as an establishment. The second condition requires showing that the local establishment is involved in some way in the processing activities, even if that establishment is not actually doing the processing.

Aligning itself with the previous positions of the Article 29 Working Party on search engines and of the CJEU's own Advocate General, the CJEU decided that the sales generated by Google's local establishment in Spain were linked to the profit generated through the data processing activities — irrespective of where these actually took place — and that link was sufficient to trigger the applicability of Spanish law.

The key point is that even if the local establishment is not making any real data processing decisions — as was acknowledged to be the case in this instance — that local subsidiary may still bring the whole data activity within the scope of application of the law, as long as there is some commercial connection with the data uses.

What is potentially very significant about the CJEU's interpretation of this rule is

that each and every local subsidiary in the EU may be capable of triggering the applicability of local data protection law. Something that could be affected by this doctrine is the long standing argument and legal position that a controller operating throughout the EU but headquartered in an EU country only needs to comply with the data protection law of that country.

Whilst the CJEU did not address this issue, it pointed out that one of the reasons for taking the approach it took was that the Data Protection Directive sought to prevent individuals from being deprived of the protection guaranteed by the Directive and from that protection from being circumvented. This would suggest that publicly appointing an EU-based entity as a data controller should still allow global businesses to operate across the EU whilst only being subject to the data protection laws of one Member State.

The right to be forgotten

The CJEU also ruled that, under the existing Data Protection Directive, the so-called 'right to be forgotten' can be exercised through two Articles of the Directive:

- Article 12(b) — right of rectification, erasure or blocking of data, where the processing does not comply with the provisions of the Directive; and
- Article 14(a) — right to object to the processing on compelling legitimate grounds.

The CJEU mainly focused on Article 12(b) of the Directive, and stressed that this right should be honoured in the event of any instance of non-compliance, such as:

- processing data in a way incompatible with specified, explicit and legitimate purposes (Article 6(1)(b));
- processing data in an inadequate, irrelevant or excessive manner (Article 6(1)(c));
- processing inaccurate data, or not keeping it up-to-date (Article 6(1)(d));
- processing data for longer than necessary (Article 6(1)(e)); and
- not meeting any of the criteria for making the processing legitimate (Article 7).

The CJEU found that in this particular situation, the processing by Google was no longer relevant because the original publication was 16 years old and it could not be justified in the public interest or otherwise.

The CJEU made the important point that, whilst the legal basis for a 'right to be forgotten' exists under the Directive, its exercise needs to be considered on a case-by-case basis. However, when considering each case, it must be accepted that as a general rule, Articles 12(b) and 14(a) override a data controller's entitlement to the processing that simply relies on that controller's legitimate interest. This is a major rebalancing act by the CJEU which puts data controllers in a very weak position to deny the exercise of the 'right to be forgotten' under existing EU data protection law.

In practical terms, an individual could argue that the processing of their data by a data controller is inadequate, irrelevant or excessive; such data are not kept up-to-date; or the data are being kept for longer than necessary. In that situation, the doctrine of the CJEU on the Google case would be applicable and most data controllers would find themselves in the same position as Google, where they would need to assess and decide whether any of the conditions triggering the right are present.

What next?

The forthcoming EU Data Protection Regulation may of course make the effects of the ruling redundant, but that is unlikely. Given that the draft Regulation will apply to the whole of the EU, the applicability of the law issue as discussed earlier will only be relevant from the point of view of which data protection authority will be entitled to claim jurisdiction over a data controller that operates across the EU.

Although this point is subject to the outcome of the ongoing debate regarding the 'One Stop Shop' ('OSS') provisions, at the very least it can be assumed that all data protection authorities will be empowered to deal with queries or complaints by their local data subjects. To what extent a local authority is then able to take any measures against an EU-wide data controller will entirely depend on the final version of the OSS provisions.

As to the right to be forgotten, the draft Regulation puts data controllers in the same situation as under the Directive as interpreted by the CJEU, although the ability for an individual to exercise this right under the Regulation is potentially wider given that the Regulation contains more obligations and hence more opportunities for non-compliance than the Directive.

The draft approved by the European Parliament in March 2014 was marginally less stringent in this respect, as it referred to a right to erasure which is triggered where the data have been 'unlawfully processed', but it does not radically change the position. In summary, the outcome of the current legislative reform will determine the scope of this right, but it seems fair to assume that the general principle established by the CJEU under the Directive in this respect will remain valid and equally far-reaching.

Eduardo Ustaran
Hogan Lovells
eduardo.ustaran@hoganlovells.com