Google LLC v Commission nationale de l'informatique et des libertés (CNIL) [C-507/17]

The Commission nationale de l'informatique et des libertés (CNIL) served formal notice on Google that, where that company grants a request for dereferencing, it must derefence the complainant's results on all its search engines. When Google refused to comply, the CNIL imposed a EUR 100 000 penalty.

The Conseil d'État asked the European Court of Justice to specify the territorial scope of the right to dereferencing under Directive 95/46. More specifically, CNIL asked whether Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 and Article 17(1) of Regulation 2016/679 mean that, where a search engine operator grants a dereferencing request, that operator is required to dereference on a) all versions of its search engine; b) only on the versions of that search engine corresponding to all the Member States; or c) only on the version corresponding to the Member State in which the request for dereferencing was made, using, where appropriate, geoblocking to prevent users from accessing the links from the complainant's Member State of residence.

The Court observed that the objective of recital 10 of Directive 95/46 and recitals 10, 11 and 13 of Regulation 2016/679 is to guarantee a high level of protection of personal data throughout the European Union and that a dereferencing carried out on all the versions of a search engine would meet that objective in full, given the borderless nature of search results.

However, the Court noted that numerous third States do not recognize the right to dereferencing or have a different approach to that right. Moreover, the right to personal data protection is not absolute, but must be balanced against societal interests and other rights in accordance with the principle of proportionality. The balance between these rights is likely to vary around the world. The Court held that while the EU legislature has, in Article 17(3)(a) of Regulation 2016/679, struck a balance between these rights in the EU, it has yet to strike such a balance for dereferencing outside the EU.

The Court noted that the wording of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 or Article 17 of Regulation 2016/679 do not confer a scope on the rights enshrined therein which would go beyond the territory of the Member States. Moreover, although Regulation 2016/679 gives Member State authorities cooperative mechanisms for balancing privacy rights and the public interest, EU law does not provide such instruments for dereferencing outside the EU.

The Court thus found that a search engine operator cannot be required, under Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 and Article 17(1) of Regulation 2016/679, to conduct dereferencing on all the versions of its search engine.

The Court then considered whether dereferencing must occur throughout all Member States, or only for the search engine corresponding to the Member State of residence of the complainant. It found that, because the EU legislature passed laws applying to all Member States to ensure a consistent level of protection across the EU and to ensure personal data flow within the EU, dereferencing must occur for all Member States. However, the balance of privacy rights and the public interest will be weighed differently across Member States because Article 9 of Directive 95/46 and Article 85 of Regulation 2016/679 leaves it to Member States to make exemptions reconciling privacy and the freedom of information.

Finally, the Court noted while that EU law does not currently require that the dereferencing granted concern all search engine versions, it does not prohibit it. Accordingly, a supervisory or judicial authority of a Member State remains competent to weigh privacy rights and the freedom of information to order a search engine to deference on all versions of the search engine.

In conclusion, the Court interpreted Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 and Article 17(1) of Regulation 2016/679 to say that an operator is not required to dereference on all versions of it search engine, but on the versions of the search engine corresponding EU Member States. (However, it must use, where necessary, measures preventing or seriously discouraging EU users from accessing the complainant's search results.)

***

Eva Glawischnig- Piesczek v. Facebook Ireland Limited [C-18/18]

A Facebook user shared a disparaging article on Glawischnig-Piesczek (GP) (an Austrian politician), which generated a 'thumbnail' of the original site, containing the title and a brief summary of the article, and a photograph of GP. They also published a comment which the referring court found to be harmful to GP's the reputation, and which insulted and defamed her. GP asked Facebook to delete the comment. When Facebook did not delete the comment, GP brought an action before Austria's Commercial Court, which directed Facebook to cease and desist from disseminating photographs showing GP if the accompanying text contained the assertions, verbatim and/or using words having an equivalent meaning to the initial defamatory content. Facebook disabled access in Austria to the content initially published.

On appeal, Austria's Higher Regional Court upheld the decision regarding the identical allegations. However, it held that the dissemination of equivalent allegations had to cease only in regard to those brought to the knowledge of Facebook by others. The case was appealed to the Austrian Supreme Court, which was called to decide whether a cease and desist order made against a social media host provider with many users may also be extended to statements with identical wording and/or having equivalent content of which it is not aware.

The Supreme Court stayed proceedings and referred three questions to the European Court of Justice concerning Article 15(1) of Directive 2000/31, which provides that Member States shall not impose a general obligation on service providers to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity. It asked whether Article 15(1) precludes a court of a Member State from: a) ordering a host provider to remove/black access to information which it stores, the content of which is identical to the content of information which was previously declared to be illegal, or to block access to that information; b): ordering a host provider to remove/block access to information which it stores, the content of which is equivalent to the content of information which was previously declared to be illegal, and; c) extending the effects of that injunction worldwide.

The Court recalled that Article 14(1) exempts the host provider from liability if it satisfies one of two conditions: a) not having knowledge of the illegal activity or information, or b) acting expeditiously to remove or to disable access to that information as soon as it becomes aware of it. The Court further inferred from Article 14(3) that the exemption is without prejudice to the power of national courts/administrative authorities to require the host provider to terminate or prevent an infringement, including by removing/blocking access to the illegal information. Injunctions may thus be ordered against providers on the basis of a Member State's national law, even if it sets out an Article 14(1) condition. Furthermore, Article 18 provides that Member States must ensure that court actions available under national law concerning information society services' activities allow for the rapid adoption of measures designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.

The Court first addressed whether Article 15(1) precludes a Member State court from ordering a host provider to remove or block access to information which it stores, the content of which is identical to the content declared illegal. While Article 15(1) prohibits Member States from imposing on host providers a general obligation to monitor information which they transmit or store, or a general obligation to actively seek facts or circumstances indicating illegal activity, such a prohibition does not concern the monitoring obligations 'in a specific case'. A specific case may be found in a particular piece of information concerning a user that was previously declared illegal. Given the nature of social media, there is a genuine risk that the illegal information could be reproduced and shared again. To prevent further impairment of interests, courts may require the host provider to remove/block access to the information stored, the content of which is identical to the content previously declared to be illegal. The injunction cannot be regarded as imposing on the host provider an obligation to monitor generally the information which it stores, or a general obligation actively to seek facts or circumstances indicating illegal activity.

The Court then addressed whether Article 15(1) precludes a Member State court from ordering a host provider to remove/block access to information which it stores, the content of which is equivalent to the content of information declared to be illegal. It held that for an injunction to effectively end the illegal act and stop further impairment of interests, it must be able to extend to information that conveys the same message as the illegal content but is worded differently—provided that the differences in the wording of that equivalent content, compared with the wording of the information declared illegal, are not such as to require the host provider to carry out an independent assessment of that content.

Finally, the Court addressed whether Article 15(1) precludes such injunctions from being able to produce effects which extend worldwide. It observed that Article 18(1) does not provide for any limitation, including a territorial limitation, on the scope of the measures which Member States are entitled to adopt in accordance with the directive. Consequently, Directive 2000/31 does not preclude those injunction measures from producing effects worldwide. However, Member States must ensure that the measures which they adopt and which produce effects worldwide take due account of rules at the international level.

Analysis

On their face, the *Google* and *Facebook* case appear to arrive at different conclusions. Yet on closer inspection, they say the same thing. Both decisions give Member State authorities the power to grant take-down orders transcending jurisdictional boundaries against intermediaries, but through different legal regimes. In *Facebook*, the Court does so through an analysis of the Electronic Commerce Directive. Meanwhile, the decision in *Google* is based on the Data Protection Directive, as well as the *Google Spain* decision establishing the right to be forgotten.

In the *Facebook* decision, the European Court of Justice concludes that the platform liability shield in Directive 2000/31 does not preclude authorities from ordering host providers to remove or block access to information whose content is identical or similar to information previously declared unlawful, and that such orders may be made on a global scale.

In *Google*, the Court holds that the search engine is not required by Directive 95/46 to dereference search results concerning a complainant on all versions of its search engine—that is, globally. However, the Court observes that, while global dereferencing is not required, it is not prohibited either. Thus Member State authorities may still, based on their respective balances of privacy and access rights, order search engines to dereference results on all versions of the search engine across the world.