CJEU in C-597/19 Mircom: users of P2P networks might be infringing the making available right if duly informed

Kluwer Copyright Blog
August 25, 2021

Liliia Oprysk (University of Bergen)

Please refer to this post as: Liliia Oprysk, 'CJEU in C-597/19 Mircom: users of P2P networks might be infringing the making available right if duly informed', Kluwer Copyright Blog, August 25 2021, http://copyrightblog.kluweriplaw.com/2021/08/25/cjeu-in-c-597-19-mircom-users-of-p2p-networks-might-be-infringing-the-making-available-right-if-duly-informed/

On 17 June 2021, the CJEU delivered its judgment in C-597/19 Mircom. It held that uploading (including automatic uploading) of pieces of a file containing a protected work on peer-to-peer (P2P) networks infringes the making available right under article 3(1) and (2) of the InfoSoc Directive when a user actively chooses to use sharing software after having been duly informed of its characteristics. Further, a contractual holder of intellectual property rights may in principle benefit from measures under the Enforcement Directive irrespective of actual use of the rights. Finally, systematic recording of IP addresses of users of P2P networks allegedly engaging in infringing activity to bring a claim for damages is in line with the General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications Directive.

Facts

Mircom is a company holding licenses for communicating to the public erotic films on P2P networks and internet file-sharing platforms. Under those licenses Mircom is required to investigate acts of infringement of film producers' rights and take legal action against infringers, passing on 50% of compensation to the film producers.

Mircom (with the help of a third party) collected IP addresses of users whose Internet connection was used to share the files in question on P2P networks. The company then brought an action before the Belgian court seeking an order that internet service providers provide identification data for their customers based on the collected IP addresses; the internet service providers challenged the claim. The Belgian court stayed the proceedings and referred questions to the CJEU. Those questions relate to the scope of exclusive rights under the InfoSoc Directive, the admissibility of Mircom's request under the Enforcement Directive, and the lawfulness of processing of personal data under the GDPR.

Findings

Communication to the public by users of P2P networks

The first (reformulated) question was whether uploading via a P2P network pieces of a media file containing a protected work, which happens automatically when running sharing software, constitutes making available of that work to the public under the InfoSoc Directive art. 3 (1) and (2).

First, the CJEU held that there is no *de minimis* threshold in the P2P context and that the fact that transmitted pieces form a part of a file and are unusable in themselves is irrelevant; what is made available through transmission is a file containing a work, hence a work in digital format [para. 43]. Even if an individual user might not be possessing or sharing the entire file, he or she contributes to the situation in which users participating in P2P networks have access to the complete file [para 45].

Next, the Court established there was an act of making available, as a work was made available in a way that the public may access it irrespective of whether they avail themselves of that opportunity. The Court referred to C-610/15 Ziggo (The Pirate Bay) concerning P2P networks, where operating a platform indexing metadata of torrent files was performing an act of communication to the public [para. 52]. The existence of the public was further confirmed through a considerable number of persons (as per the list of IP addresses provided), able to access protected works at any time and simultaneously [paras 54-55].

Finally, the Court took a stand on the relevance of users' knowledge of the consequences of using sharing software, namely that such software automatically uploads downloaded pieces of files. The AG in his opinion took the view that the actual knowledge of the consequences was not relevant in the present case as it concerned not an intermediary but rather users performing initial and autonomous communication [paras 54-61]. The CJEU, on the other hand, held that it is for the referring court to determine that the relevant users gave their consent to use the software after having been duly informed of its characteristics [para 49]. Once active consent is established, the deliberate nature of the conduct is confirmed regardless of the fact that uploading is started automatically by the software [49].

Copyright "trolls" benefiting from measures under the Enforcement Directive

The second (reformulated) question was whether a contractual holder of IP rights who does not use the rights themselves may benefit from measures provided under the Enforcement Directive. Here, the national court would have to verify Mircom's standing as a contractual holder of the rights or as a person authorised to use intellectual property [paras 66-69]. Non-use of the rights does not exclude the party from the benefits of the measures as it would be contrary to the objective of the high level of protection of intellectual property [paras 74-77].

A request for information such as that by Mircom could not be regarded as inadmissible on the sole ground that Mircom does not make serious use of the rights. Rather, it would be for the national court to determine whether the request as specifically formulated is well-founded and whether measures are abused [paras 78-93]. In principle, the contractual holder of intellectual property rights not using them herself may benefit from the measures under the Enforcement Directive unless it is established, on the basis of a detailed assessment, that a request is abusive, unjustified or disproportionate [para. 96].

Balance between intellectual property enforcement and safeguarding respect for private life and data protection

The third (reformulated) question asked whether the systematic registration of IP addresses of users on P2P networks who were allegedly involved in an infringement of intellectual property rights, and communication of names and postal addresses of those users to right holders or third parties, enabling them to bring a claim for damages, is precluded under the GDPR. The CJEU found that *upstream* processing, meaning the gathering of IP addresses of P2P network users by a third party on behalf of Mircom, could be regarded as lawful but it would be for the national court to ascertain such processing under national law, in light of the Privacy and Electronic Communications Directive protecting the confidentiality of users of electronic communications [paras 102-119].

The *downstream* processing, meaning the request to provide names and addresses for identified IP addresses, was found consistent with the objective of striking a fair balance between intellectual property and personal data protection rights [paras 120-121]. Although internet service providers do not have an obligation under the GDPR to communicate personal data (here traffic data) to third parties for the purpose of prosecuting for copyright infringements, they could be obliged to communicate data on the basis of the Privacy and Electronic Communications Directive if a Member State adopted measures for retention of data for a limited period [paras 126-127]. Hence, if such data retention measures are in place in national law, and if Mircom has legal standing and its request is justified, proportionate and not abusive (all for the national court to investigate), such processing must be regarded as lawful under the GDPR [para. 131].

Comment

After the C-610/15 Ziggo ruling on the operation of an online sharing platform indexing torrent files, it was only a matter of time until the CJEU had to rule on whether users of P2P networks make works available to the public, even if they do not possess a complete file. In the line of previous development, the judgment allows a finding of infringement of copyright where users of P2P networks automatically upload pieces of files containing a protected work. However, it must be established that that user actively chose to use sharing software by giving consent after being duly informed of its characteristics, so they ought to be informed in some way about the automatic upload of already downloaded pieces.

It is noteworthy that the Court did not fully follow the AG, who considered that an act of making available took place irrespective of the user's knowledge of the consequences of that act. In this author's view, the Court's answer provides a more balanced approach. Even if many internet users would associate the use of P2P networks with piracy or infringing activities and also potentially have knowledge of the automatic uploading feature of such software, it seems too far-reaching to assume a particular level of digital literacy from virtually any internet user. Holding users liable for using software sharing pieces of a file containing a work potentially without them being aware of it would set a precedent for targeting individual users unintentionally engaging in some kind of infringing activity.

In the aftermath of the judgment, it remains to be seen how the parties will argue for the presence or absence of the user's active choice to use the software in full knowledge of its characteristics, as it would possibly require a case-by-case assessment of a particular situation, analysis of the terms of use and of the notion of duly informed. Could it lead to (another) knowledge presumption for particular user groups or software involved in infringing the exclusive rights? The right holders are likely to argue for knowledge presumption in the P2P context, as it would otherwise be difficult to prove an infringement on the sole basis of collected IP addresses. Furthermore, the national court's view on the presence of consent and notion of being duly informed would influence the presence of an alleged infringement and, in turn, grounds for the processing of personal data for the purpose of identifying individuals, such as gathering IP addresses.

The use of a third party for gathering IP addresses in this case is also noteworthy given the CJEU's judgment in C-264/19 Constantin Film Verleih, holding that the concept of address under the Enforcement Directive does not cover IP or email addresses. Consequently, right holders can request service providers to disclose only names and postal addresses of alleged infringers unless the national law allows disclosure of further data such as IP. In the present case, Mircom had used a third party to collect IP addresses and then, in line with Constantin Film Verleih, requested an internet service provider to match them to a name and address. While such a solution is possible for tracking down infringers in the context of P2P networks through tracking down peers, monitoring, for instance, YouTube's upload traffic would hardly be feasible.

On the question of so-called copyright "trolls" and invoking the measures under the Enforcement Directive by a party not using the rights themselves, the Court rightfully did not focus on who suffered prejudice as a result of the alleged infringement, as it is up to the right holder to decide how to assign and exploit the rights. In principle, the Directive does not preclude the contractual holder from benefiting from the measures, but it is for the national court with all the details at hand to examine whether the request is abusive, unjustified or disproportionate.

Finally, collection and matching of IP addresses to names and addresses constitutes lawful processing of personal data when it is done for a legitimate purpose such as to enable raising a claim for damages from allegedly infringing users, as long as there is a lawful basis for retaining such data under the national law. Hence, enforcement of intellectual property rights relies heavily on the national law, in this case on Member States' leeway to sanction retention of traffic data for a reasonable period in line with the GDPR. It remains to

be seen if the Member States will see a need to adopt special measures on the retention of traffic data in the aftermath of the case to the extent such measures are not already in place.

This post is based on an article originally published on IPtrollet.no.