Kluwer Copyright Blog

AG Szpunar's Opinion in Grand Production: "Grande première" for the VPN legal saga in the context of geoblocked streaming

Tatiana Synodinou (University of Cyprus) · Tuesday, February 28th, 2023

Grand Production d.o.o. v GO4YU GmbH (Case C?423/21)

The facts of the case are representative of the grey areas of the application of copyright territoriality in the digital era. The applicant, Grand Production d.o.o., is a Serbian company which produces television programs that are broadcast in Serbia by a TV channel, Prva Srpska Televizija. Another Serbian company, GO4YU d.o.o Beograd, has been licenced by Prva Srpska Televizija to broadcast on its streaming platform the broadcaster's program in Serbia and Montenegro. For all other audiences outside these two countries, the shows must be 'blacked out' by GO4YU d.o.o Beograd. However, the public can bypass this by connecting to the platform's service via Virtual Private Network (VPN), tricking the platform into believing that the device is located in Serbia or Montenegro. This is because the operator of the streaming platform would only see the IP address of the VPN server, not that of the client. Simultaneously, the streaming platform is advertised in Austria by two Austrian companies owned by GO4YU d.o.o Beograd (also defendants), offering subscriptions and customer service. The applicant believes that the acts of GO4YU d.o.o Beograd and of its related companies infringe its right of communication to the public, since the streaming platform is aware of the unauthorised public connections to its service via VPN address.

In this context, Austria's Supreme Court requested a preliminary ruling from the Court of Justice of the European Union (CJEU). The main question from the perspective of the right of communication to the public is whether the operator of a streaming platform which has implemented geoblocking is liable for copyright infringement if the users of its services use a VPN to access content that should not be accessible from a certain territory. The CJEU is also asked whether the two other companies owned by the platform could also be found liable for the communication to the public of the programs in Austria.

The third question seeks clarification on the jurisdiction of national courts regarding injunctions for copyright infringement. Specifically, can an Austrian court prohibit the communication to the public in territories outside Austria? For the AG this question on the interpretation of Article 7(2) of the Brussels I bis Regulation might not be admissible since the defendant is not located in the EU and, therefore, the question is not relevant to the outcome of the dispute in the present case. This post will therefore focus on the first two questions and will not analyse the jurisdiction issue.

From hyperlinking to geoblocking: towards a holistic conception of the notion of the "public"

First, the AG confirms some classic findings of the CJEU regarding the scope of the right of communication to the public, such as that the rebroadcast of a television broadcast on the Internet is a distinct and independent act of communication. Additionally, it is noted that it does not matter whether the rebroadcast on the Internet is simultaneous and unchanged from the original broadcast or not. It is also recalled that the "new public" criterion is not relevant where the Internet retransmission was made by different technical means from the original television broadcast (paras. 23-25).

However, the interest of the Opinion regarding the EU construction of the right of communication to the public is primarily methodological and lies in the expansive and consolidating application of the CJEU's principles in the hyperlinking cases in the completely different context of geoblocking. Such a method has also been used elsewhere, such as in *Soulier*, where *Svensson*'s findings regarding the determination of a 'new public' on the basis of the technically unreserved publication of works in the Internet by the right holder have been applied by the CJEU in a diverse context too (*Soulier*, par. 36). This approach appears in contrast with an assumed *lex specialis* character of the CJEU's hyperlinking principles (for instance, see par. 45 of *GS Media*). It is, nonetheless, more than welcome since it provides a more advanced consolidation of core concepts of the CJEU's communication to the public theoretical model. A model that has proved to provide mostly reasonable outcomes, but at the same time appears as complex, labyrinthine and technical.

Accordingly, the AG recalls, on the basis of the line of reasoning of the CJEU in the hyperlinking cases, that the circle of persons to whom a communication to the public is addressed is determined by the intent of the person making the communication. This intent should be deduced objectively by the applicable technical guarantees. A freely accessible website is addressed to all Internet users, while a website secured by access restrictions is addressed exclusively to persons who have gained lawful access to it (paras 32, 33 of the Opinion).

Therefore, if the operator of a streaming platform established a geoblocking mechanism which aims to secure the copyright holder's territorial segmentation of markets, the platform does not perform acts of communication outside the licensed territories. The platform is not liable even if its

users finally bypass the geoblocking via the use of VPN.

The "bad faith" of the platform

Another thought-provoking conceptual contribution of the Opinion is that the AG builds on the CJEU's findings in *Stichting Brein* (par. 44) in order to propose a consolidated criterion for the determination of copyright infringement by an intermediary on the basis of their "bad faith". This assessment focuses on whether the intermediary intentionally bypassed/contributes to the intentional bypassing of the right holder's target audience, as initially determined by the rights holder through technical means. In the present case, the bypassing takes place by the users themselves; only if the operator of the streaming platform had intentionally established an ineffective geographical blocking could it be held liable, which is a matter of fact to be resolved by the national court.

The question of the intention to establish an ineffective geoblocking mechanism would in practice prove to be a tricky one, since it should be analysed on the basis of objective evidence regarding (i) the platform's intention and (ii) the ineffectiveness of the geoblocking mechanism.

It is not clear whether the employment of geoblocking or another technical restriction mechanism which would be ineffective, not deliberately but due to gross negligence, could also result in the professional operator's liability. Following the hyperlinking saga, such an approach could be justified on the basis of *GS Media's* line of reasoning which established a heavier duty of care for professionals. It should, however, be recalled that the question of an absolute effectivenesss of digital rights management tools of other technical restrictions means is a chimera, as the AG points out (paras. 38, 39) and the CJEU confirmed in *UPC Telekabel* (paras. 62, 63). Furthermore, elaborating more on this issue would probably have gone too far, since the central question is about the liability of the platform for its users' acts.

Nevertheless, in small countries such as those in the case, the number of VPN services should be relatively small and the detection of their IP addresses easy. Therefore, it could be held by the national court that the operator is contractually bound by an implicit obligation of ensuring the effectiveness of the geoblocking measure by filtering VPN requests for access. Here, the limits of EU copyright law harmonization can be seen, in the sense that on this point the liability relies on civil law principles that should also be harmonized.

Direct and indirect interventions, a question of distance and substance

The second question tackles whether the related companies could be directly liable for the communication to the public. The AG supports the view that these companies do not have any influence on the programs, the content of the broadcasts and the geoblocking measures. Therefore, they cannot be liable for infringement of the right of communication to the public. The AG recalls on this point that a direct relationship is required between the user's intervention and the communication to the public.

More generally, the question of the liability of promoters and of persons facilitating, contributing or aiding copyright infringement has not been harmonized and is a matter of national law (par. 52

of the Opinion).

VPN, the elephant in the room

The case is stimulating also for another reason. It sheds light on the thorny issue of the use of VPN and its consequences on the efficacy of online copyright law enforcement. In this context, it is related to the landmark case *UPC Telekabel*, which dealt with the fundamental rights compliance of injunctions against Internet service providers.

First, the question of VPN is implicitly considered in *Telekabel* since the Court accepted that for an injunction to be considered as effective, it is not necessary for it to be absolutely effective. VPN is able to circumvent the blocking order against an Internet service provider, which means that any blocking order by nature is in part ineffective. Nevertheless, the effectiveness of an order should not be measured in terms of completely eradicating any forms of illegal access, but in terms of dissuation. The more users are discouraged from using VPN to circumvene geoblocking measures, the more the order is effective. This dissuasion is based on some deterring factors related to the use of VPN: the technical effort in finding and installing a VPN that would allow access to the protected content, the additional cost since fast VPNs ask for remuneration, and the potential harm to privacy, as the VPN has access to online communications taking place through its portal. Nevertheless, as the new generation becomes more and more familiar with the technology, these deterrent effects weaken.

Second, *Telekabel*'s logic is based on the idea that massive enforcement of copyright law would be counterproductive and that intermediaries, even if they are protected by a safe harbour, should participate in the efforts in fighting piracy. In this context, it should be accepted that the VPN provider is itself an intermediary (see footnote 20 of the Opinion where the AG confirms that Article 12 of the E-commerce Directive is applicable to VPN providers) that has gradually gained a significant role in the era of geoblocking.

The question is raised, then, (and unfortunately could not be answered by the AG here, as off-topic) whether VPN providers could be asked through blocking orders not to provide access to copyright infringing – such as geoblocked – content. At first glance an application by analogy of the jurisprudence on blocking orders could appear a solution to this thorny issue. However, it is necessary to keep in mind a further requirement posed by *Telekabel*: a blocking order should not have the consequence of interfering with freedom of expression by limiting access to lawful content. The VPN technology ensures cryptography and anonymity and if it is often used for illegally circumvening geoblocking measures, this is far from being its only usage. A blocking order against VPN providers would have the consequence of prohibiting some users from having access to content to which they are entitled.

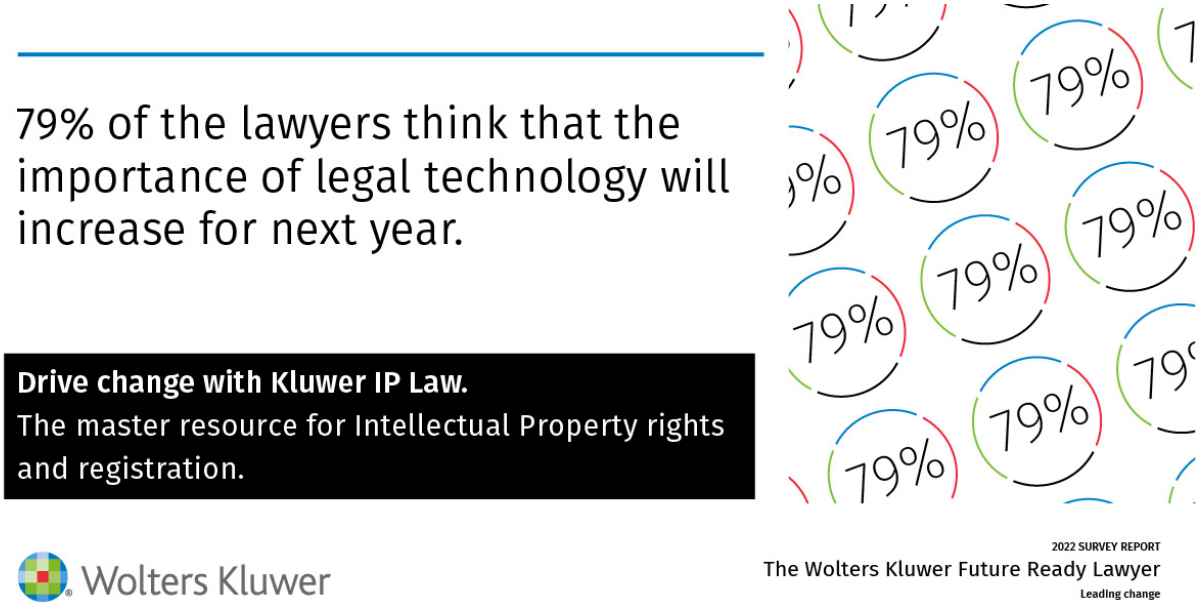
In conclusion, it is almost certain that the CJEU's decision, whether it follows the Advocate General's opinion or not, will mark the first step on a long and difficult road concerning the use of VPN to circumvene legal protections. Such a process needs audacity and, in this context the AG has, in his own brilliant manner, shown the way.

To make sure you do not miss out on regular updates from the Kluwer Copyright Blog, please subscribe here.

Kluwer IP Law

The **2022 Future Ready Lawyer survey** showed that 79% of lawyers think that the importance of legal technology will increase for next year. With Kluwer IP Law you can navigate the increasingly global practice of IP law with specialized, local and cross-border information and tools from every preferred location. Are you, as an IP professional, ready for the future?

Learn how **Kluwer IP Law** can support you.



This entry was posted on Tuesday, February 28th, 2023 at 11:51 am and is filed under Case Law, inter alia, for ensuring that EU law is interpreted and applied in a consistent way in all EU countries. If a national court is in doubt about the interpretation or validity of an EU law, it can ask the Court for clarification. The same mechanism can be used to determine whether a national law or practice is compatible with EU law. The CJEU also resolves legal disputes between national governments and EU institutions, and can take action against EU institutions on behalf of individuals, companies or organisations.">CJEU, Communication (right of), Enforcement, European Union, Infringement
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.