scripted

Volume 10, Issue 2, August 2013

FOOTBALL DATACO V SPORTRADAR: SECOND HALF AND HOME FIELD FOR DATABASE MAKERS

Perttu Virtanen [*]

Abstract

The Court of Justice of the European Union gave a preliminary ruling in Football Dataco Ltd v Sportradar GmbH and Others on the jurisdiction of the Courts on matters concerning the sui generis database protection. The previous Dataco case concerning copyright protection of databases, had been decided by the Court of Justice in the same year, however in this instance the solution focused essentially on the Court's jurisdiction in the online environment which pivoted on the question of where the claimed extraction or re-utilization was deemed to occur.

DOI: 10.2966/scrip.100213.278

[*] Post-doctoral Research Scientist, Helsinki Institute for Information Technology (HIIT), Aalto University. The hyperlinks were last accessed on 26 April 2013 unless otherwise indicated. Many tanks to Dr. Olli Pitkänen for his valuable comments.

1. The procedure in national courts and before the CJEU.

This is the second case, brought by the same applicant, concerning the legal protection of databases, before the Court of Justice of the European Union (CJEU) in the same year. The difference being that the first judgment concerned databases protected by copyright[1], whereas the second case touched more on the *sui generis* legal protection of databases. The claimants, Football Dataco Ltd and its partners, are responsible for the English and Scottish football leagues' annual organization and also maintain a Football live database, which contains information about the currently played matches. The goals and scorers, yellow and red cards, penalty kicks, substitutions and similar elements of a match comprise the data fed into the database. The data was collected mainly by freelancers contracted by Dataco who attended the matches for that purpose.

Football Dataco Ltd.'s claims were pursuant upon their substantial investment, as a result of the activities mentioned above, qualifying for *sui generis* protection conferred by the Database Directive[2] as implemented by the UK Database Regulations[3] . They alleged that the respondents had violated this protection by copying the data from their Football live database.

The respondents, a German company and its Swiss holding company, provide football and other sports statistics and run a website betradar.com outside UK. The site offers, in addition to other services, a live football score allegedly using information copied from Football live. Furthermore, a British betting company and another offshore (Gibraltarian) company, both contractually customers to the respondents, targeted the UK audience to offer sports betting to their customers through their own web-sites providing a link to betradar therein.

The claimants argued that the respondents had violated the claimants' database right and that, therefore, action may be brought in the UK. However, the respondents claimed they did not copy the claimant's data, but rather accumulated it independently and therefore did not need a licence from the claimants. Furthermore, the respondents took the view that the matter was not within the jurisdiction of the UK court because none of the company servers were located in the UK and their office was also situated abroad, therefore the alleged infringing actions did not take place in the UK.[4] Accordingly, the respondents commenced proceedings against the claimants of this case in a German court seeking negative declaratory judgment of non-infringement.

---

[1] P Virtanen: *Football Dataco v YAHOO!* – The ECJ Interprets the Database Directive, [2012] 9 *SCRIPTed* 2, 258-267, at: http://script-ed.org/wp-content/uploads/2012/08/virtanen.pdf

[2] *Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases*, [1996] OJ L77, at 20-28.

[3] *The Copyright and Rights in Databases Regulations* 1997 No. 3032, as subsequently amended.

[4] According to the High Court judgment the respondents had servers located in Germany and Austria. Pursuant to the Appeal Court judgment, the respondents' server was located in Austria, with a back-up server in Holland and the livescore service on which the betradar is based mainly operated by the subsidiary office in Germany. As for the servers, it was decisive perhaps that all were situated outside the UK, thus also the generic denomination "A" while generic "B" can in this case refer to UK.

The High Court, Chancery Division of England and Wales decided that the British court had jurisdiction, reasoning that the decisive criterion was where the alleged infringing actions were deemed to occur. In terms of the relevant legal background in this context, in addition to the Database Directive, Article 5(3) of Regulation No 44/2001 on jurisdiction *etc* in commercial and civil matters, establishes that, in cases which concern tortuous liability, special jurisdiction exists on the part of the courts for the place where the harmful event occurred or may occur.[5] Further, in accordance with the Regulation on the law applicable to non-contractual obligations, in the case of an infringement of an intellectual property right which is not a 'unitary Community' right, the law applicable to a non-contractual obligation arising from such an infringement is, under Article 8(1), 'the law of the country for which protection is claimed'.[6] While these grant jurisdiction to the court where the harmful act occurred and establishes the relevant applicable law, the question as to *where* the harmful act occurred remains.

While none of the servers were located in the UK, both the extraction and re-utilization of data was held to have occurred in the UK. This was because they provided the service to customer betting companies which then provided the hyperlink to the betradar database to end-users in the UK. These acts made a good arguable case of joint liability against the respondents together with the customer betting companies. On appeal, the Court of Appeal decided that a reference to the CJEU concerning the interpretation of acts of extraction and re-utilisation on the one hand, and the localisation of the extraction and re-utilisation on the other, was necessary. [7]

The CJEU opined that the referring court essentially asked (a) whether Article 7 of Directive 96/9 must be interpreted as meaning, that the sending by one person, by means of a web server located in Member State A, of data previously uploaded by that person from a database protected by the *sui generis* right under that directive to the computer of another person located in Member State B, at that person's request, for the purpose of storage in that computer's memory and display on its screen, constitutes an act of 'extraction' or 're-utilisation' of the data by the person sending it. If so, it asked, by part (b) of its question, whether that act must be regarded as taking place in Member State A, in Member State B, or in both those States. Thus, the first question concerns whether Sportradar's activities constitute an activity covered by the exclusive rights of the database maker, Dataco, and if so, where the location of those acts of extraction and/or re-utilisation are taken to occur when completed via the

---

[5] *Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters*.

[6] *Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations* (Rome II).

[7] The Court of Appeal presented the following questions as interpreted by the Court of Justice of the European Union: "*Where a party uploads data from a database protected by sui generis right under Directive 96/9/EC ("the Database Directive") onto that party's web server located in member state A and in response to requests from a user in another member state B the web server sends such data to the user's computer so that the data is stored in the memory of that computer and displayed on its screen: (a) is the act of sending the data an act of "extraction" or "re-utilisation" by that party? (b) does any act of extraction and/or re-utilisation by that party occur (i) in A only (ii) in B only; or (iii) in both A and B?"*

Internet. The answers to these questions are crucial to resolving whether a UK court has jurisdiction or not.

In reference to question (a), focusing on re-utilisation, the court held that an act, such as that at issue in the main proceedings, in which a person sends data previously extracted from the content of a database protected by the sui generis right, to another person's computer, at that person's request, by means of his web server, this constitutes an act of re-utilisation by the person sending it.[8] Concerning question (b) and the localisation of an act of 're-utilisation', within the meaning of Article 7 of Directive 96/9 it must, like the definition of that concept, correspond to "independent criteria" of European Union law, according to the CJEU.[9] In developing and pronouncing these criteria, which are not dependent on Member State law, the Court made numerous references to its earlier case-law highlighted below.

In terms of the meaning of an act of re-utilisation, this consists of a series of successive operations, ranging at least from placing data online by means of a web server, onto a website to be consulted by the public, to the transmission of that data to the interested members of the public, which may take place in the territory of several different Member States. The mere fact that the website, which contains the data in question, is accessible in a particular national territory is not a sufficient basis for concluding that the operator of the website is performing an act of re-utilisation caught by the national law applicable in that territory concerning protection by the *sui generis* right.[10] This arises from the fact that the consultation of a publically available website can take place irrespective of any intention on the part of the operator of the website in regard to its consultation beyond that person's Member State of establishment and outside of that person's control. Localisation of an act of re-utilisation in the territory of the Member State to which the data in question is sent depends on there being evidence that the act discloses an intention of the performer of the act to target persons in that territory. [11]

First, because data on Sportradar's server includes data relating to English football league matches, which suggests that the acts at issue in the main proceedings follow from an intention on the part of Sportradar to attract the interest of the public in the United Kingdom which may constitute such evidence. Second, since Sportradar granted, by contract, the right of access to its server to companies offering betting services to that public may also be evidence of its intention to target them, if Sportradar was aware of that specific destination or if the remuneration set by Sportradar as consideration for the grant of that right of access took account of the extent of the activities of those companies in the United Kingdom market and the prospects of its website betradar.com subsequently being consulted by Internet users in the United Kingdom.

Finally, the data placed online by Sportradar was accessible, in their native language, to United Kingdom internet users who are customers of those companies which is not

---

[8] *Football Dataco v Sportradar, paras 20-21 and 47.*

[9] *Ibid*, para 33, referring to *Donner* , [2012] C-5/11, para 25.

[10] *Ibid,* paras 34-6, the last point referring to *Pammer and Hotel Alpenhof*, [2010] C-144/09, para 69, and *L'Oréal and Others* ,[2011] C-324/09, para 64.

[11] *Ibid,* para 39, making a reference by analogy again to *Pammer and Hotel Alpenhof*, paragraphs 75-6, 80 and 92; *L'Oréal and Others*, para 65; and *Donner*, paragraphs 27 to 29.

the same as the languages commonly used in the Member States from which Sportradar pursues its activities. This also provided supporting evidence for the existence of an approach targeting in particular the public in the United Kingdom.[12] Consequently, the referring court will be entitled to consider that acts of re-utilisation such as those at issue in the main proceedings are located in the territory of the Member State of the location of the user to whose computer the data in question is transmitted, at his request, for the purposes of storage and display on screen (Member State B), where there is evidence from which it may be concluded that the act discloses an intention on the part of the person performing the act to target members of the public in Member State B, which is for the national court to assess.[13]

2. Analysis

This case essentially involved a non-contractual commercial dispute between two business entities providing separate online database information services. Both were willing to litigate on the alleged database right infringement, with the ascertainment of the appropriate jurisdictional forum being the other key question.

The starting-point, for this analysis, is to note that the Database directive did not aim to introduce a uniform *sui generis* right in European Union law. Instead, it aimed to achieve the harmonization of domestic Member States' laws concerning database intellectual property protection both in regard to the copyright protection attaching to databases and the *sui generis* right, to the degree the Directive provided. Accordingly, the protection by a *sui generis* right provided for in the legislation of a Member State is limited in principle to the territory of that Member State, so the person enjoying the protection can rely on it only against unauthorised acts of extraction or re-utilisation which take place in that territory.

As for part (a) of the question outlined above concerning re-utilisation, The ECJ held that the concept of re-utilisation covers an act in which a person sends, by means of his web server, to another person's computer, at his request, data previously extracted from the content of a database protected by the *sui generis* right. In doing so, that data is made available to a member of the public and accordingly falls within the exclusive right granted to the database maker. This decision appears to be based on the precedent set in *The British Horseracing Board Ltd & Others v William Hill Organisation Ltd*[14] and arguably adopts a technologically neutral and markedly broad interpretation of the exclusive right in question.[15] Consequently, in answering part (b) of the question on the location of the re-utilisation, the nub of the matter is whether the acts of "sending data", which are at issue in the main proceedings, fall to be considered as acts taking place within the United Kingdom, and accordingly within the territorial scope of the protection enshrined by the *sui generis* right afforded by the law of that Member State.[16]

---

[12] *Football Dataco v Sportradar,* para 42.

[13] *Football Dataco v Sportradar,* para 47.

[14] *The British Horseracing Board Ltd and Others v William Hill Organization Ltd* , [2004] C-203/02

[15] *The British Horseracing Board Ltd and Others v William Hill Organization Ltd* , [2004] C-203/02, paras 51 and 67; *Football Dataco v Sportradar*, para 20.

[16] *Football Dataco v Sportradar*. para 28.

It is perhaps important to note that the Court did not set the site operator a duty to demonstrate that the provision of the content is limited to a particular region or a particular language user group. The assumption of liability is formulated *e contrario:* the starting point is that the mere fact that the website containing the relevant data is accessible in a particular national territory is not a sufficient basis for concluding that the site operator is performing an act of re-utilisation caught by the national law applicable in that territory concerning the *sui generis* right.[17] Instead, the localisation of the relevant act depends on the evidence disclosing *an intention on the part of its performer to target persons in that territory*.[18] Thus, the assumption appears to be non-universal in application and is determined on the basis of the assessment of the region where a particular service has been allocated. The criteria for such an assessment are listed in the judgment.

The list appears to be based in part on the Court's own precedent where the locality of certain acts, some of which were performed online, were analysed and the development of "independent criteria" was found necessary.[19] Four such criteria disclosing the requisite intention to target persons in the UK are mentioned in the judgment, and each of them deserves a brief analysis. After that, it is useful to consider their interrelationship.

The Court held that since the data on Sportradar's server includes data relating to English football league matches, proceeding from an intention on the part of Sportradar to attract the interest of the public in the United Kingdom, it may constitute evidence indicating the intention to target persons therein. However, this is unconvincing for anyone familiar with the international football scene. English and also Scottish league events draw widespread interest outside the UK within a broad community of football enthusiasts and those interested in betting. Thus audiences overlap to a degree for such events, with a substantial portion of the audience coming from outside the borders of the UK.

The same applies *a fortiori* to the last criterion mentioned, the use of the English language, "which is not the same as those commonly used in Member States from which Sportradar pursues its activities" pursuant to the judgment. Sportradar runs an Internet-based business for the provision of information services. This business is international, transcending purposely the national boundaries of both its own places of establishment; Germany and Switzerland. According to the company's own information, as listed on its website, currently more than 300 businesses in over 60 countries use Sportradar's data services for betradar.[20] Currently, the English language is the *lingua franca* both in Europe and globally and this applies particularly in the online context, although not everyone appears to be ready to acknowledge the fact. The chosen *modus operandi* for running the information service through an Internet website suggests the same international or, rather, global tenet. Consequently, the choice of English language for an international audience is understandable and its inherent value in showing intent to target UK audience is less convincing. There is

---

[17] *Ibid,* paras 36-38.

[18] *Ibid,* para 39.

[19] In this respect, the current judgment refers to *Pammer and Hotel Alpenhof, Donner,* and *L'Oréal and Others,* the cases already mentioned *supra*, in paras 40-42.

[20] https://www.betradar.com/dp/

arguably nothing wrong with using the language or the characteristics of the relevant activity as markers to indicate the intention to target a certain geographical area in general. However, the case clearly highlights how the strength of such criteria is dependent on the particulars of a given case.

The two remaining factors are more intriguing in the current case and may well have a bearing on showing the intent of targeting audiences in a certain country or countries. The CJEU opined that as Sportradar's customer companies offered betting services to the UK public, this could constitute evidence of Sportradar's intention to target the UK market, if the latter was aware, or must have been aware, of that specific end user. Further, it could be relevant in this respect if the remuneration fixed by Sportradar, as consideration for the grant of access, took into account the extent of the activities which those companies had in the UK market and the prospects of its website betradar.com subsequently being consulted by Internet users in the United Kingdom.

The first criterion is again problematic in many aspects. As said therein, it was the betting companies that were Sportradar's actual customers, and not the users accessing the database through a hyperlink. Accordingly, was it not the companies that were the actual *potential* target of Sportradar and not the UK end users of the information? Did the betting companies provide betting services exclusively or predominantly to the UK audience? The intentions to target a specific audience by the betting companies may differ from the intentions of Sportradar. Sportradar's intention thus may become equalled to its acquiescence. This may have been recognised in the latter criterion of the Court, the possible fixing of consideration based on UK end users, if the sum charged from betting offices is based on their customer base. What if these betting offices also have non-UK customers who are charged on the same basis? Further, does this criterion not still potentially confound the initial targeting of "persons" in the relevant territory with the clients of Sportradar and their eventual success, depending on how and when the fixing of rates is carried out?

Of course, these are all matters of adducing the relevant evidence to the relevant circumstances. To turn the tables for a while, it may well serve the interests of the respondents to show that instead of intending to target persons in the UK, they were rather seeking to attract a global customer base, which may consist of betting companies *et cetera* having their own international audience. Further, as a consequence of this, Sportradar may have chosen to use English exactly to *not* target any individual country like the UK alone, and the choice for the provision of UK football abreast with possible other non-UK football information data stemmed from its intent to reach a wider, even global audience. *E contrario,* the absence of such circumstances may well allude to targeting, but it is suggested that it is requisite to put even that in a reasonable context.

The criteria pronounced by the CJEU would also arguably benefit from clarification as to how they should operate together in practice. For instance, is the existence of one of the criteria mentioned in the list sufficient to prove that there was an intention to target persons in the UK? If not, how about if some points provide evidence on behalf of the targeting while others militate against it? It remains to be seen how the internal logic of the list of criteria given is to be properly applied. Not surprisingly, the Court sagely inserted the standard clause to the ruling that it is for the national court to assess whether there is evidence disclosing an intention to target the members of the public in the UK (Member State B).

Two final points deserve attention. First, as the numerous references to parallel case-law of the CJEU indicate[21], the problem of determining jurisdiction for matters involving acts performed on the Internet is a recurring problem in several branches of law, not only those relating to intellectual property issues. The earlier CJEU cases referred to in this case cover matters such as; trade mark issues related to use of keywords on websites; "independent interpretation of the EU law" in respect of non-Internet copyright infringement; consumer protection on website hotel bookings; alleged infringements of personality rights by publishing photographs on Internet websites and the liability of an online operator on claimed trade mark infringement. One of the reasons for numerous references is the fact that formerly e.g. the strategic positioning of a web server in another country may have contributed to changing the court having jurisdiction, and depending on the possible divergences in the relevant branch of law, having more favourable rules for the setting up the web-based operations or providing the possibility of escape from liability in some occasions.

Second, it is yet slightly embarrassing to read in a ruling that a person sends information by means of a web server to another person's computer upon his request. Rather, these operations are as a rule automated and the relevant server does this, the natural or juristic person offering the service merely arranges or outsources the provision of such a technological system which is then in charge of these tasks. These systems have already evolved past the stage that the location of servers or "sending" can alone be seen as relevant for the determination of location of relevant acts on the Internet, it is argued here *de lege ferenda*.

Thanks to the introduction and wide adoption of cloud computing and cloud services,[22] where computing resources are delivered as a service over a network like the Internet, it is difficult or virtually impossible to establish the physical location of the hardware configuration owing to the fact that it changes, if necessary, at short notice, without even an information service provider, in charge of the technical implementation, being all the time aware of the changes or the actual location of the servers. In short, this shows that, due to the development in underlying technology, the location of the hardware and software is often not a reliable criterion for determining the location of an act even partly dependent on uploading or keeping the server downloaded with relevant data available. In respect of making data available to the public, or the concomitant reutilisation in the database context, to rely on acts of downloading by the users, makes little sense either. They can be scattered around the globe in a manner inconsistent with the initial plans or intentions of the information provided to target a specific audience and rather, may be a consequence of circumstances not necessarily in their control. As a consequence, the motivation to move away from determinations based solely on the placement of hardware on one hand, or information's universal availability via Internet on the other, is welcome *per se.*

---

[21] *Wintersteiger*, [2012] C-523/10, *eDate Advertising and Martinez,* [2011] joined cases C-509/09 and C-161/10, *Pammer and Hotel Alpenhof*, *L'Oréal and Others*, and *Donner.*

[22] See e.g. L Wang – G Laszewski: Scientific Cloud Computing; Early Definition and Experience, 26 October 2008, at 2-5, available at: http://cyberaide.googlecode.com/svn/trunk/papers/08-cloud/vonLaszewski-08-cloud.pdf ; H Motahari *et al:* Outsourcing Business to Cloud Computing Services: Opportunities and Challenges, HP laboratories external publication, 2009:23, available at: http://www.hpl.hp.com/techreports/2009/HPL-2009-23.html

The *judicium* employed by the CJEU then resembles, remotely, that of determining the *locus* of a criminal act, and, as is the case for criminal law, the alleged infringer's intentions can be difficult to determine in retrospect with regard to their acts, let alone eventual consequences. The evaluation of someone's intended purposes is consequently often open to interpretation, in which case flexible criteria set out by the CJEU potentially give rise to more complexity and unpredictability which may become legal and business obstacles, or interfere with other rights such as freedom of expression. These issues can be exacerbated when the service provider's original intention was international business, and the Internet was availed of to open up new opportunities globally. Yet, some potential audiences could have received particular attention to lure customers from that group. While the CJEU's initial stance was exactly that of not invoking an unlimited responsibility in each country having Internet access, it does not lead to a consistent solution if the criteria provided then advance potentially an opposite interpretation that deliberately invokes such responsibility .

It is useful to bear in mind that the German company actually running the information service never sought to avoid the litigation and perhaps the resultant liability. Instead, it instituted proceedings in its own *forum domicilii* after learning about the UK proceedings. Consequently, the choice of appropriate forum on Internet related cases has consistently been one pregnant with different policy considerations and related issues, both in domestic and international disputes.[23] At the same time, the Directive was the instrument deliberately chosen by the then EC to address the problem of patchy legal status for the intellectual property protection of databases, and to provide the increased and harmonised level of protection across the Member States, including both the UK and Germany. However, the Directive did not introduce any rules to establish the location of possible infringement. In other words, it neither harmonised nor introduced new rules in this respect. While the history of judicial activism[24] and the arguments thereof have been a perennial bone of contention concerning different levels of Community legislation, the holding that the localisation of re-utilisation *must* correspond to independent criteria of EU law á la *Donner* arguably amounts to filling a Community level lacuna in the Database Directive by judicial means.[25] One can question whether such a mandate exists. In addition, concerning the *modus* of the reasoning, Hume's Guillotine is also effective in this context.

---

[23] The difficulties were recognized readily in the 1990s with the rapidly spreading Internet adoption, see e.g. G Kalow, "From the Internet to Court: Exercising Jurisdiction over World Wide Web Communications" [1997] 65 *Fordham Law Review* 5, at 242-275; subsequently J. Reidenberg "Technology and Internet Jurisdiction" [2005] 153 *University of Pennsylvania Law Review*, at 1951-1974; In Europe and Particularly in the UK, R Lautman – K Curran "The Problems of Jurisdiction on the Internet" [2011] 3 *International Journal of Ambient Computing and Intelligence* 3, at 36-42.

[24] See e.g. the classic treatises: H Rasmussen: *On Law and Policy in the European Court of Justice: A Comparative Study in Judicial Policymaking,* (Dordrecht: Martinus Nijhoff, 1986); T. Hartley: *Constitutional Problems of the European Union* (Oxford: Hart, 1999); and recent: G Conway: *The Limits of Legal Reasoning and the European Court of Justice* (Cambridge: CUP, 2012).

[25] *Football Dataco v Sportradar*. para 33. Interestingly, the reference therein to *Donner* judgment reveals that the need for independent interpretation concerned the notion of distribution provided by the relevant directive, and not directly the localization thereof; The underlying EU international treaty obligations are also relevant in the context speaking on behalf of independent interpretation. See paras 25-30 therein.

Nevertheless, the current preliminary ruling opens the door for an interpretation granting jurisdiction to a UK Court where the rightsholder resides. The ruling is thus more favourable for the rightsholder than was the previous Dataco case concerning copyright protection of databases. It is open to the domestic courts in this particular case to apply the criteria to establish whether there were sufficient grounds to hold that the respondents had an intention to specifically target the UK audience, thus securing the home field for the claimants. However, it is still useful to bear in mind that the actual substantial issue between the parties, the establishment of an eventual database right infringement, only follows this determination of the relevant domestic court having jurisdiction. The transition to a network of computer based information services which presages the case is hardly likely to be the last of its kind.