



Technology Newsletter

Issue 1/2015

The CJEU Rules on Jurisdiction in Online Copyright Infringement Cases

Territoriality, being one of the main principles of copyright law, seems to conflict with claims concerning copyright infringements on the internet, at least at first glance. At the end of January, the Court of Justice of the European Union (the “**CJEU**”) gave its views on the jurisdiction questions relating to online copyright infringement (C-441/13, *Pez Hejduk v EnergieAgentur.NRV GmbH*).

The case itself was about a professional photographer Hejduk living in Austria who sued the German based EnergieAgentur for copyright infringement. Hejduk’s pictures were published on EnergieAgentur’s website (using a .de top-level domain), from where the pictures could also be downloaded, without Hejduk’s consent and without giving her any credit. The claim was initiated in Hejduk’s home state before the Handelsgericht Wien and consisted of claims for damages of some 4,000 euros. According to the defendant, the Viennese court lacked jurisdiction since the website as such was not directed at Austria.

The Viennese court turned to the CJEU in order to get clearance in the question regarding the jurisdiction of the court. The CJEU interpreted the Brussels I Regulation and came to the conclusion that in addition to the competent German court, the Viennese court has jurisdiction in the case since (i) the copyrights to the pictures were recognised in Austria, (ii) the damage in question had occurred in Austria, and (iii) the website was accessible from Austria.

Hence, what can be learned from this case is that the localisation of damage determines the questions relating to the jurisdiction of the court as regards online copyright infringement. In order for the damage to be located in a Member State, it does not require that the website on which the infringement occurs is directed at that Member State, as mere accessibility to the website is sufficient. What remains to be seen is whether this case will open up for more forum shopping in online copyright infringement cases and, furthermore, whether the courts of different Member States will be handling the same cases, but only in terms of the part specific to their country. This will certainly lead to interesting arguments regarding the measurement of the amount of damages taking place within a specific territory.

Ilona Tulokas, Senior Associate, Helsinki

Finnish Online Retailer Verkkokauppa.com and Its Subsidiary Jointly Liable for Unpaid Private Copying Levies – Landmark Case on Piercing the Corporate Veil

The Finnish Supreme Court ruled in its landmark decision KKO 2015:17 published on 9 March 2015 that the Finnish company Verkkokauppa.com Oy (“**Verkkokauppa**”, nowadays a publicly listed company Verkkokauppa.com Oyj) was jointly liable

with its Estonian subsidiary Arctecho OÜ (“**Arctecho**”) for unpaid private copying levies and legal interest totaling to some EUR 4,400,000.

The Estonian subsidiary Arctecho offered Finnish customers blank CDs and other devices which were subject to private copying levies set in the then-current Finnish copyright legislation (the legislation regarding the private copying levies has changed materially as of 1 January 2015). Arctecho operated its sales through a Finnish-language web store, accessible from www.verkkokauppa.com or www.verkkokauppa.ee. Arctecho did not pay the levies for the devices ordered by the Finnish customers, and Teosto – the Finnish copyright organization for composers, lyricists, arrangers, and music publishers – claimed compensation for the unpaid levies for the period of 2006 – 2010 from both Arctecho and Verkkokauppa.

Teosto claimed, among others, that Arctecho was established only to avoid the Finnish private copying levies and that Verkkokauppa was in fact conducting Arctecho’s business and hence also liable for the unpaid levies. Prior to June 2009, Arctecho’s shares were owned as follows: Verkkokauppa 29%, Verkkokauppa’s (then) sole shareholder 51%, and two Verkkokauppa’s board members 20%. As of June 2009, Verkkokauppa was the sole shareholder in Arctecho.

In its ruling, the Supreme Court firstly cited the clear starting point of the Finnish Companies Act, which is that a limited liability company shall be a legal person distinct from its shareholders and that the shareholders shall have no personal liability for the obligations of the company. Then, by referring to earlier case law of the Supreme Court and to legal literature, the Court noted that the piercing of the corporate veil – expansion of e.g. a company’s obligations to a shareholder – can be generally seen as exceptional outside the scope of certain special enactments. According to the Court, the piercing of veil may come into question if the group structure, relationship between companies, or controlling power of a shareholder is clearly used in an artificial and reprehensible manner resulting in e.g. damage to creditors or avoidance of liabilities set in law.

The Supreme Court stated that the key reason for establishing Arctecho as an Estonian limited liability company was to avoid the obligation to pay private copying levies for products sold to Finland and that Arctecho’s operations fully lacked independence from Verkkokauppa. According to the Court, Verkkokauppa had de facto conducted some of its regular business through Arctecho to avoid the levies and, noting the ownership and controlling power relating to the companies, the Court stated that the main purpose and goal of the corporate structure was to avoid the obligation set in law. Hence, Verkkokauppa had acted in a reprehensible manner in order to have Arctecho’s distinct liability set aside. The Supreme Court found Verkkokauppa to be jointly liable with its subsidiary Arctecho for the unpaid private copying levies.

Janne Joukas, Senior Associate, Helsinki

The CJEU Ruling on Exhaustion of Distribution and Its Impact on Digital Copies

The Court of Justice of the European Union (the “**CJEU**”) has found in its recent ruling that Article 4(2) of the Directive on Copyright in the Information Society (2001/29/EC, the “**Directive**”) must be interpreted as meaning that the rule of exhaustion of the distribution right set out in Article 4(2) of the Directive does not apply in a situation where “*a reproduction of a protected work, after having been marketed in the European Union with the copyright holder’s consent, has undergone an alteration of its medium*”. The Case *Allposters v. Stichting Pictoright* (C-419/13) addressed the reproduction of an artistic work and placing it on the market in its new form. The alteration carried out consisted of a transfer of the image from a paper poster onto a painter’s canvas by means of a chemical process where the image of the work disappears from the paper backing, but the image of the painting itself was not altered. The alteration of the medium was interpreted as having resulted in a new object and, therefore, a reproduction of the protected work. According to the CJEU, the resale of such object would require prior authorisation from the holder of the reproduction right.

With regard to digital copies, it is noteworthy that the CJEU expressly stated the exhaustion of the distribution right to be applicable to (the tangible object) into which a protected work or its copy is incorporated. This means that e.g. the resale of a book which includes protected content is allowed without the consent of the copyright’s holder as long as the medium is not altered. Because the distribution right upon first sale under the Directive applies to the tangible object, the first sale of intangible digital copies of works will hardly exhaust the distribution right to such copies. Hence, without the copyright holder’s additional consent, the resale of digital copies of e.g. e-books, music, and films duly purchased by way of download from the internet will likely be considered a copyright infringement.

With regard to intangible copies, the CJEU has previously allowed the resale of downloaded software without the copyright holder’s re-approval. In the *UsedSoft* ruling, the CJEU ruled that the first sale of an intangible copy of a computer program by way of download from the internet onto a buyer’s device with the copyright holder’s consent causes exhaustion of the distribution right to such copy. However, this judgment was based on the interpretation of a different EU Directive, namely the Directive on the Protection of Computer Programs (2009/24/EC, “**Software Directive**”) and not on the Directive. The Software Directive thus provides less protection to right holders than the Directive and is thus interpreted differently as

regards the exhaustion rule.

The relation between these two rulings is interesting because in the *Allposters v. Pictoright* case, the CJEU applied precisely the same arguments that it had previously rejected as not being applicable in the *UsedSoft* case, regarding e.g. the wording of recital 28 of the Directive, according to which copyright “*protection under this Directive includes the exclusive right to control distribution of the work incorporated in a tangible article*”. Considering the argumentation of the latter case, it would appear to be difficult for the CJEU to turn around in the future and decide that exhaustion of the distribution right under the Directive also applies to the first sale of intangible digital copies.

Erkko Korhonen, Senior Associate, Helsinki

Update on the Ratification of the Unified Patent Court Agreement - Six Down, Seven to Go

Since our HS Technology Newsletter 3/2014 published last autumn, one more Member State has ratified the Agreement on a Unified Patent Court (the “**Agreement**”). At the very end of 2014, Malta ratified the Agreement and joined the company of Denmark, Belgium, Sweden, Austria, and France, which had already ratified the Agreement earlier.

In order to become effective, the Agreement must be ratified by at least 13 Member States including France, Germany, and the United Kingdom, in which countries the majority of European patents are registered. As mentioned above, France has already ratified the Agreement, and hence, in addition to the United Kingdom and Germany, the Agreement has to be ratified by five other Member States before it may become effective.

The preparatory work for the ratification of the Agreement has been initiated in Finland and we will follow the progress closely and shall provide an update in our next newsletter.

Panu Siitonen, Partner, Helsinki

New Liability for Breaches of Russian Personal Data Law

In addition to new data localisation requirements which will enter into effect on 1 September 2015 and will require personal data concerning Russian citizens to be stored locally in Russia, on 24 February 2015 the Russian State Duma (the lower house of the Federal Assembly) passed a bill in its first reading which, if made into law, will establish new liability for breaches of Russian personal data law.

Currently, the maximum administrative fine for a breach of the personal data processing procedure established by law is a fine of up to RUB 10,000 (about EUR 150) for legal entities. The authors of the bill have proposed increasing the administrative fine to RUB 300,000 (about EUR 4,500) and differentiating liability for each violation of personal data processing. The most significant fines will be imposed for violations concerning the processing of special categories of personal data, which include personal information in relation to race, nationality, political and religious views, as well as health, intimate relations, and previous criminal convictions.

The authors of the bill believe that increasing liability will bring the Russian personal data legislation closer to European standards.

At this moment, only the prosecuting authorities are authorised to initiate administrative investigations with regard to a breach of personal data legislation, and it usually takes a significant amount of time to hold the wrongdoer administratively liable. In order to accelerate the consideration of such types of administrative cases, the new bill will also authorise Russia’s Federal Service for Supervision of Communications, Information Technology, and Mass Media (*Roskomnadzor*) to independently initiate administrative investigations as regards breaches of personal data legislation.

If the new bill is passed and signed into law, it will enter into legal force 10 days after its official publication.

Pavel Falileev, Associate, Moscow

Ruling on the Exemption for Processing of Personal Data in Unstructured Material

The Swedish Supreme Administrative Court recently ruled (in cases 642-14 and 571-14) on the exemption for processing of personal data in unstructured material. According to said exception, the majority of the provisions of the Personal Data Act (the “**PDA**”) need not be applied when processing personal data in unstructured material, such as running text. Thus, the exemption is applicable if the relevant data is not included or intended to be included in a collection of personal data (e.g. a document, case management system or any other database) which has been structured in order to significantly facilitate the search for or compilation of personal data. However, such processing of personal data must not entail a violation of the integrity of the registered person.

In November 2011, the Swedish Data Protection Authority (the “**DPA**”) issued orders against two companies, both providing services to employers which included background checks on applicants for work. The DPA ordered the companies to either stop providing the relevant services or take specific measures in accordance with the PDA. According to the DPA, the exemption for processing of personal data in unstructured material was not applicable.

The Supreme Administrative Court stated that the personal data in question was structured in such a way that it was listed in simple digital documents in spreadsheet or word processing programs. Certainly, the companies had taken advantage of computer technology, but not in terms of structuring in relation to manual handling. In this context, the Supreme Administrative Court found that the relevant data had not been structured in order to significantly facilitate the search for or compilation of personal data and ruled – contrary to the lower courts – that the exception for processing of personal data in unstructured material was applicable.

Petra Lennhede, Associate, Stockholm

Is the Safe Harbour Program in Jeopardy?

The Safe Harbour Program, under which the personal data of EU citizens is transferred to thousands of U.S. companies, has led to some doubts as to its security. The German Data Protection Commissioners (the “**Commissioners**”) claimed in the Data Protection Conference of Berlin that the data protection level of U.S. Companies does reach to the same level as in the EU despite the fact that U.S. companies have certified adhering to the Safe Harbour Rules. The German Data Protection Authorities (the “**DPA**”) have expressed their concern of inadequate enforcement of the Program by the U.S. Federal Trade Commission (the “**FTC**”). Most recently, some of the DPAs have initiated administrative proceedings against two U.S. companies whose data transfers are based on the Safe Harbour Program with the intention of putting a stop to the transfers. It is speculated that such suspension of data transfer may lead to a court decision denying the supervisory authorities’ competence to suspend data transfers. The actions of the German DPAs are based on an earlier conference where the Commissioners stated that surveillance activities by foreign intelligence and security agencies threaten international data traffic. The Commissioners’ concerns regarded reports about comprehensive surveillance activities by foreign agencies, in particular by the U.S. National Security Agency (the “**NSA**”). In 2013, the German Commissioners decided to stop the issuing of approvals for international data transfers. According to the Commissioners, there is a high probability that the principles of necessity, proportionality, and purpose limitation are being violated because personal data transferred by domestic companies to foreign countries may be accessed by foreign intelligence services without compliance to the principles.

In addition, EU officials have also criticised the FTC for failing to provide adequate protection to EU citizens while enforcing the Safe Harbour Program. Partly as a result of the disclosures by Edward Snowden, the European Commission released a list of 13 recommendations to address the deficiencies in the Safe Harbour Program in November 2013. The recommendations focused on transparency, redress, enforcement and audits and access by U.S. authorities. All except the latter have been addressed by the FTC. In February 2014, the European Data Protection Supervisor welcomed the measures considered by the Commission, but encouraged the Commission to be more ambitious when defining the next steps to be taken. Furthermore, the Article 29 Working Party has taken a stand on some of the issues in its opinion concerning cloud computing which gives a negative evaluation of the ability of the Safe Harbour self-certification to meet the requirements of national laws implementing the EU Data Protection Directive.

The FTC has followed the situation in Europe and, especially after the revelations of the NSA intelligence gathering, taken measures to bring back the trust in the functionality of the Safe Harbour Program. For instance, in 2013 the FCT promised more enforcement actions, and in 2014 it entered into settlement agreements with twelve companies that had allegedly falsely represented that they were current certified members of the Safe Harbour. Despite the repair attempts, there is strong support for the view that if an agreement with the U.S. government cannot be reached, suspension of the Safe Harbour Program should not be ruled out.

The Safe Harbour is quite a hot potato, as the system is critical for many U.S. based businesses (particularly for big tech companies) transferring data from the EU to the U.S. Even a short suspension could mean a serious disruption to the

business operations of these companies. In addition, most customers of these companies rely on the Safe Harbour Program as a basis for complying with the transfer restrictions set forth in the EU Data Protection Directive and the corresponding national legislation. Because there is such an economic incentive for making the Safe Harbour work, it is an interesting question whether the EU is all set to jeopardise this delicate structure. Global organisations may wish to consider alternative approaches to Safe Harbour, such as standard clauses, binding corporate rules (BCR), and increasing the self-assessment of entities.

Erkko Korhonen, Senior Associate, Helsinki

Protection of Consumers in Online and Mobile Games Addressed by European Authorities

Last year, the European Commission and the consumer authorities of the member states (i.e. the Consumer Protection Cooperation) negotiated with the gaming industry with regard to problems relating to online games. The authorities have paid special attention to areas that have been found problematic from the viewpoint of consumer protection, such as the advertising of online games, billing issues, and payments relating to games that have been advertised as free.

The negotiations between the authorities, Apple, Google, and the Interactive Software Federation of Europe were successful with regard to the above-mentioned questions, and both Apple and Google have bound themselves to communicate the actual costs of games more clearly and, furthermore, to also make sure that consumer protection questions relating to minors are identified. The authorities will continue to monitor the issue and, in particular, the extent to which the engagements made by the online game industry and platforms will actually address the concerns raised by the authorities.

For further details, please see the Commission's website.

Ilona Tulokas, Senior Associate, Helsinki

The CJEU on Liability for Potential Defects in Medical Products

The Court of Justice of the European Union (the “**CJEU**”) gave its views on liability for potentially defective products and the costs related thereto in its judgement of 5 March 2015 (C-503/13 and C-504/13, *Boston Scientific Medixinetchnik GmbH v AOK Sachsen-Anhalt – Die Gesundheitskasse and others*).

In short, the case was about a company selling pacemakers that, after carrying out quality controls, found that its pacemakers might be defective and constitute a danger to patients' health. The pacemaker producer recommended that the implanted pacemakers be replaced free of charge. In the proceedings between the insurers and the company selling the pacemakers, the German Federal Court turned to the CJEU asking whether the replaced pacemakers are to be classified as defective solely on the basis of the fact that defects had been found in other pacemakers of the same model. Furthermore, the German court asked the CJEU whether the pacemaker producer could be held liable for costs associated with replacing the devices.

According to the Court, a potential defect in a medical device renders it possible for all products of the same model to be classified as faulty without any need to show that each replaced product is defective. The Court also declared that costs related to the replacements are “damage” for which the company selling the pacemakers should be held liable.

The outcome of the case is, at least from a Finnish consumer protection perspective, quite expected. Furthermore, it is worth noting that in its judgment, the CJEU emphasised the special nature of the medical devices at hand, as the devices are subject to particularly high safety requirements and the vulnerability of the patients must also be considered. Hence, it remains to be seen whether the Product Liability Directive will be as broadly interpreted by the Court in future cases that concern products with lower safety requirements than those of pacemakers.

Ilona Tulokas, Senior Associate, Helsinki

The CJEU's Ruling on Parthenogenic Stem Cells – Striking a Balance between Human Dignity and Patentability

In its landmark decision of 18 December 2014 (C-364/13 *International Stem Cell Corporation v Comptroller General of Patents, Designs and Trade Marks*), the Court of Justice of the European Union (the “**CJEU**”) took on the task of redefining the balance between protecting human dignity, on the one hand, and providing patenting incentives for stem cell researchers in Europe, on the other hand. The CJEU reinterpreted the definition of a ‘human embryo’ in Article 6(2)(c) of the Biotech Patent

Directive 98/44/EC and now found that it “*must be interpreted as meaning that an unfertilised human ovum whose division and further development have been stimulated by parthenogenesis does not constitute a ‘human embryo’, within the meaning of that provision, if, in the light of current scientific knowledge, it does not, in itself, have the inherent capacity of developing into a human being*”. The ruling is significant as it opens up new possibilities for patenting stem cell research results in Europe after the CJEU’s previous judgement on the issue (C-34/10 Oliver Brüstle v Greenpeace eV.) had introduced very broad exclusions on the patentability of human embryonic stem cell inventions in order to ensure respect for human dignity. The CJEU’s new ruling strikes that balance anew, referring to current scientific knowledge presented to the Court according to which “*a human parthenote, due to the effect of the technique used to obtain it, is not as such capable of commencing the process of development which leads to a human being*”.

Tom Jansson, Associate, Helsinki

HANNES SNELLMAN

Disclaimer: Hannes Snellman Technology Newsletter is intended for information purposes only. It should not be relied upon as legal advice nor should it be used as a basis for any action or final decision without specifically verifying the applicability and relevant issues on their merits in each individual case.