

C L I F F O R D
C H A N C E

17TH EDITION



GLOBAL INTELLECTUAL PROPERTY NEWSLETTER
BLOCKCHAIN, AI AND OTHER IP TOPICS
ISSUE 03/18

CONTENTS

Paris: French Supreme Court rules on patentability and validity of dosage regime claims	5
In a recent judgment dated 6 December 2017, the French Supreme Court set out the conditions under which a dosage regime may be patented.	
Paris: French Supreme Court rules on trade mark infringement with respect to goods intended for export only	7
In its decision of 17 January 2018, the French Supreme Court clarified that the unauthorised use of a registered trade mark in France amounts to trade mark infringement even though the products are intended for export to a country where the use of the same sign is lawful.	
Hong Kong: Driving success: Well-known trade mark status in China	9
This article considers a recent win by Clifford Chance for its client Aston Martin Lagonda Limited in successfully obtaining “well-known trade mark recognition” in China for the “ASTON MARTIN” mark. The article summarises the factors that helped secure the win and outlines the protection and benefits offered by the status.	
Hong Kong: China’s new Anti-Unfair Competition Law	12
China's main legislation on unfair competition practices has received a long-awaited update. Rules on unauthorised use of brands, packaging, corporate and domain names, commercial bribery and disclosure of trade secrets have all been strengthened in the new law which came into effect on 1 January 2018.	
London: Update on TV Format Protection	16
Protecting TV formats has been notoriously difficult both in the UK and worldwide. A recent decision by the High Court of England and Wales sheds new light on how TV formats may be protected under UK copyright law.	
Düsseldorf: Blockchain and its application in the field of IP: Smart Contracts and IPR management	18
While the bandwidth of use cases is still subject to ongoing research, one of the fields that will profit from the possibilities of blockchain is “smart contracts”, i.e. legal contracts built and executed (entirely or in parts) by means of software. This article will provide a first glimpse at what role intellectual property rights might take in this “new world” of blockchain and smart contracts.	
Düsseldorf: Securing IP rights in Blockchain-Technology from a German law perspective	21
In a fast-growing market, securing IPR over newly-developed Blockchain-technologies is crucial for stakeholders in order to maintain their competitive edge with respect to future commercialization. The article discusses how such protection could be achieved under German law.	

Prague: Blockchain technology and the GDPR	24
Blockchain technology is currently a hotly debated topic. Although mostly associated with Bitcoin and other cryptocurrencies, the scope of blockchain is much broader. Blockchain can be used in various fields, including banking & finance, healthcare, real estate, and energy management. It is a promising technology capable of bringing many benefits to entrepreneurs and society. However, it also carries certain risks, in particular when it comes to compliance with data protection laws.	
Milan: Trade Secret's protection and big data: an Italian view	27
Access to big data is currently regulated through rights <i>in rem</i>, by granting license rights. However, rights <i>in rem</i> are not enforceable against third parties. The upcoming national implementations of the EU Trade Secret Directive will provide an opportunity to Member States to facilitate suitable protection to investments made in big data and data science.	
London: Copyright in AI-Generated Works	29
This article considers whether copyright can subsist in an AI-generated work and whether AI systems can infringe third party copyright.	
Düsseldorf: Update on the UPC and the Unitary Patent: UK in a position to ratify the UPC Agreement, Germany blocked by constitutional complaint	32
After more than three decades of negotiations, the European Union has entered the final straight towards establishing a unified patent system. However, challenges in the UK and Germany will need to be overcome before the new system can finally be put into place.	
Barcelona: The CJEU Sheds Light on the Interpretation of the “Repair Clause” Established by Article 110(1) of EU Regulation 6/2002 of 12 December 2001, on Community Designs	36
In its Judgment of 20 December 2017 (cases C-397/16 and C-435/16), the Court of Justice of the European Union analysed the scope and requirements for applying the so-called “repair clause” (set out in Article 110(1) of EU Regulation 6/2002, on Community design rights), which excludes protection as a Community design for component parts of complex products if certain conditions are met.	
Acknowledgement	39
Contacts	40
Our International Network	43

17TH EDITION

Introduction

Welcome to the **17th Edition** of the **Clifford Chance Global IP Newsletter**. In this first issue of 2018, we will pick up where we left off last December and update you on recent trends and developments in IP law.

In a highly anticipated patent case in France, the French Supreme Court ruled on the **patentability and validity of dosage regime claims**. Further, in a separate case, the French Supreme Court decided on whether the unauthorised use of a trade mark in France can amount to trade mark infringement in cases where the use is of products intended for export to countries where there would otherwise be no infringement. Keeping the focus on trade mark law, we will also highlight a recent case won by Clifford Chance for its client *Aston Martin Lagonda Limited*. Our client successfully obtained well-known trade mark recognition for the mark “**ASTON MARTIN**” in China. In addition, we will take a look at the new **Chinese anti-unfair competition law** (enforceable since 1 January 2018) which governs the unauthorized use of brands, packaging, corporate and domain names, commercial bribery and disclosure of trade secrets.

The focus of this edition will then turn to **blockchain, smart contracts and the Internet-of-Things**, in particular with regard to questions of protection and application in the field of IP, a topic increasingly gaining attention throughout all industries.

We start with a comprehensive overview of various aspects to be taken into consideration when dealing with blockchain from an IP perspective, including the **protection of the underlying technology** as well as **IP being subject to and managed by blockchain** applications. Further, we will discuss to what extent the upcoming **General Data Protection Regulation** may be applicable to blockchain and what major risks may arise from the use of this new technology to process personal data. We will also analyse whether **Big Data** can be protected as trade secret in Italy.

Speaking of digitization, our London team will provide further insight into the copyright of **artificial intelligence** and discuss issues arising from the increasing prevalence, and increasing capability of **AI software**. We will then discuss *Banner Universal Motion Pictures Ltd v Endemol Shine Group* regarding TV format protection in the UK.

We will also provide a brief update on the current state of the **ratification process of the Unitary Patent system** in France, the UK and in particular in Germany where the required ratification has been blocked by a **constitutional complaint** filed at the German Constitutional Court – with a final judgment to be expected in 2018.

Finally, this Edition highlights the recent decision by the Court of Justice of the EU on the interpretation of the so-called “**repair-clause**” set out in Article 110(1) of EU Regulation 6/2002 on Community design rights.

We hope to provide you with some insight into developments in the world of IP and look forward to your feedback.

Your Global CC IP Team

PARIS: FRENCH SUPREME COURT RULES ON PATENTABILITY AND VALIDITY OF DOSAGE REGIME CLAIMS

On 6 December 2017, the French Supreme Court ("**Cour de cassation**") put an end to the very long saga involving Merck Sharp & Dohme Corp.'s ("**MSD**") "*Finasteride*" molecule used to cure male pattern baldness.

The long awaited judgment of the *Cour de cassation*, rendered in the *MSD v Téva Santé* case, is remarkable for two main reasons. First, it admits – though implicitly – the patentability of dosage regime claims. Second, it provides the tools to understand in which circumstances a second therapeutic application based on such new dosage regime can be protected by a patent.

Patentability of dosage regime claims

On the basis of the provisions of Articles 53 c) and 54(4) of the European Patent Convention ("**EPC**"), pursuant to which a second therapeutic application can be patented if it is new to the state of the art, the European Patent Office ("**EPO**") had admitted in 2010 the patentability of a second therapeutic application based on a dosage regime change¹.

However, until now, the position of French judges in this respect remained unclear. The Paris *Tribunal de Grande Instance* – having exclusive jurisdiction in patent cases as a first instance court – was more than reluctant to follow the patentability trend. Indeed, it considered that a dosage regime did not constitute a first or second therapeutic application but was rather the mere indication of the range in which the substance is efficient to actually cure the disease in respect of the tests described in the patent. In a highly debated judgment dated 28 September 2010², concerning *Finasteride* in the *MSD v Actavis* case, the *Tribunal de Grande Instance* ruled that "*Article 54(4) EPC (...) is completely silent on the allowability of patenting a particular posology. Accordingly, the answer of the Enlarged Board according to which 'such patenting is also not excluded where a dosage regime is the only feature claimed which is not comprised in the state of the art' does not arise from the Convention but from an interpretation of what is a posology, i.e. a further medical use, which it is obviously not.*"

The Paris Court of Appeal made a definitive first step towards the admission of dosage regime patents by ruling in the same *MSD v. Actavis* case that "*the patentability of a further medical use claim relying only on a posology feature may be allowed*"³. Still, by eventually declaring the patent invalid on the ground of insufficient disclosure in the *MSD v. Téva Santé* matter – and thus moving the debate from unpatentability to invalidity – the French Supreme Court definitively paved the way towards full recognition of dosage regime claims patentability.

Key Issues:

- There was some uncertainty in France regarding whether or not a substance or composition known as a "medicament" for treating a certain illness could be patented for use in treating the same disease, where the second or further medical use is based on a novel dosage regime.
- For the first time, the French Supreme Court has admitted, though implicitly, the patentability of dosage regime claims.
- Claims should still meet the validity requirements of novelty, inventive step and sufficiency of disclosure.
- The standard for a dosage regime claim to be considered sufficiently disclosed is quite strict. Although it is not necessary to clinically demonstrate the therapeutic effects of the dosage regime, the patent must reflect directly and unambiguously the claimed therapeutic application.

¹ EPO, enlarged board of appeal, February 19, 2010, G 2/08, *Abbott Respiratory LLC*.

² TGI Paris, September 28, 2010, No.07/16296, *Merck Sharp & Dohme v. Actavis*.

³ Cour d'appel de Paris, Pôle 5 Chambre 2, January 30, 2015, No. 10/19659, *Merck Sharp & Dohme v. Téva*.

Standard for sufficiency of disclosure

Though dosage regime claims appear to no longer be excluded from patentability *per se*, said claims must nevertheless meet the usual validity requirements of novelty, inventive step and sufficiency of disclosure.

In this respect, the second interesting point of the *Cour de cassation* judgment is that it lays down the principles on the sufficiency standard to be applied to second medical use inventions.

The court ruled that “*when a claim relates to a second therapeutic application of a substance, obtaining this therapeutic effect is a functional technical feature of the claim. [Thus], in order to meet the requirement of sufficiency of disclosure, it is not necessary to clinically demonstrate this technical effect [As MSD did], but **the patent application must directly and unambiguously reflect the claimed therapeutic application, so that the skilled person can understand, based on commonly accepted models, that the results reflect this therapeutic application***”. In the case at hand, the Court ruled that, since the patent description mentioned a “*surprising and unexpected discovery*” – without describing precisely the particular pharmacological action of the regime – the skilled person was not in a position to reproduce the invention without making further research on his own. In other words, for the dosage regime claim to be considered as sufficiently disclosed, it must be described precisely enough to allow the skilled person to manufacture the drug himself with the right dosage to obtain the very same therapeutic effect.

This rather strict standard – which subtly distinguishes “*clinical demonstration of technical effect*” from “*direct and unambiguous reflection of the claimed therapeutic application*” and is directly inspired by the case-law of the European Patent Office in this respect⁴, might often lead to invalidity decisions when it comes to dosage regime claims. Only time will tell what awaits.

Diego de Lammerville is “*very creative and commercial and has an in-depth technical knowledge of the law.*” He specialises in contentious commercial matters.

Chambers Europe 2018: France,
Dispute Resolution: Litigation



⁴ EPO, Boards of Appeal, January 22, 2015, T 0338/10.

PARIS: FRENCH SUPREME COURT RULES ON TRADE MARK INFRINGEMENT WITH RESPECT TO GOODS INTENDED FOR EXPORT ONLY

On 17 January 2018, the French Supreme Court (“**Cour de cassation**”) issued a landmark decision on trade mark infringement. The Cour de cassation ruled that holding products bearing a French trade mark in France, without the authorization of its owner, can amount to trade mark infringement, even though (i) the products are intended for export in a country where the use of such trade mark is not prohibited, and (ii) there is no risk for the products to be commercialized in the French territory.

This judgment marks a notable turnaround in the *Cour de cassation* case-law.

The *Cour de cassation*’s previous position

In a very controversial judgment of 10 July 2007¹, the *Cour de cassation* held that holding products bearing a French trade mark in France without the authorization of the trade mark owner did not amount to trade mark infringement under the same circumstances as described above.

The Paris Court of Appeal previously ruled that the mere storage of marked products to be exported to a country where the use of the trade mark was not prohibited did not constitute “*use in the course of trade*” pursuant to Article 5§2 of Directive 2008/95/EC to approximate the laws of the Member States relating to trade marks (the “**2008 Directive**”) and hence did not constitute a trade mark infringement².

This analysis was arguable in the light of the Court of Justice of the European Union (“**CJEU**”) case law and in particular the CJEU’s interpretation of the notion of “*use in the course of trade*” as meaning use of the sign “*in the context of commercial activity with a view to economic advantage and not as a private matter*”³. The Court of Appeal position was also arguable in view of the wording of Article 5§3 of the 2008 Directive which prohibited *inter alia* “*affixing the sign to the goods or to the packaging thereof*” and “*exporting the goods under the sign*”.

The *Cour de cassation* decided not to follow the rationale of the Court of Appeal regarding “*use in the course of trade*” and ruled that the holding of marked products in order to export them, constitutes use of the sign in the course of trade. However, controversially, the *Cour de cassation* found that the defendant’s use of the trade mark did not amount to trade mark infringement as it was “*legitimate*” as long as the products at stake were intended for export only and not intended for the French market.

Key Issues:

- In a 2007 judgment, the French Supreme Court provided for an exception to trade mark infringement in cases where the trade mark was affixed on products intended for export to a country where the use of the trade mark was lawful.
- This position had been criticized for being incompatible with EU law.
- In a recent judgment of 17 January 2018, the Court reversed its previous position and expressly stated that its previous ruling in this respect was incorrect.
- The owner of a French trade mark is now entitled to prevent a third party from affixing its sign on products and holding those products in France even though the products are not intended for the French market.

¹ Cour de cassation, July 10, 2007, No. 05/18571

² Cour d’Appel de Paris, June 1st, 2005, No. 04/09317,

³ Court of Justice of the European Union, November 12, 2002, C-206/01, *Arsenal Football Club v. Reed*.

In order to reach this judgment, the *Cour de cassation* relied on Article L. 716-10 of the French Intellectual Property Code providing criminal sanctions for trade mark infringement when, *inter alia*, products bearing a trade mark are being held with no “*legitimate reason*”. The decision led to heavy criticism in particular because it did not seem to comply with the 2008 Directive which did not provide for any equivalent exception.

The turnaround in the *Cour de cassation* case-law

In the case which resulted in the *Cour de cassation*’s ruling of 17 January 2018, the world leading Bordeaux wine company Castel Frères – owner of the trade mark “*Ka Si Te*” in France – had initiated a trade mark infringement action against a Chinese citizen who had affixed the sign “*Ka Si Te*” on wine bottles in France in order to export them to China, where he was fully entitled to use the sign.

Castel Frères argued that such unauthorized use of the “*Ka Si Te*” trade mark in France amounted to trade mark infringement even though the goods were destined to China.

The *Cour de cassation* followed the claimant’s arguments and reversed its case-law, highlighting that its 2007 ruling was in breach of the principle of full harmonisation of national laws intended by the 2008 Directive, since the 2008 Directive did not provide for any “*legitimate reason*” exception.



HONG KONG: DRIVING SUCCESS: WELL-KNOWN TRADE MARK STATUS IN CHINA

Clifford Chance recently assisted Aston Martin Lagonda Limited (“**Aston Martin**”) in successfully obtaining “well-known trade mark recognition” in China for the “ASTON MARTIN” mark. The recognition, issued by the PRC Trademark Review and Adjudication Board (“**TRAB**”), was part of a decision for a successful invalidation action brought by Aston Martin against a Chinese trade mark squatter.

The recognition was a well-deserved win, particularly in view of the established fame of “ASTON MARTIN” in both China and around the world. Other important factors contributing to the successful outcome were the inclusion of tailored submissions and the comprehensive presentation of evidence highlighting the “fame” of the mark.

Well-known status for foreign brand owners

Well-known trade mark recognition is a very powerful tool for combating infringers and trade mark hijackers as it offers a much broader scope of protection than offered to normal registered trade marks.

The evidentiary burden to obtain well-known trade mark recognition in China is high. Historically, it has always been difficult to obtain well-known trade mark status, especially for foreign brand owners who will have more difficulty in collecting evidence of use and promotion in China. According to statistics from the Chinese Trade Mark Office (“**CTMO**”), between 2012 and 2013 only around 20 out of 1,300 trade marks recognised as well-known under the old trade mark law originate from foreign brands. Even after the new PRC Trade Mark Law (“**TML**”) came into effect in 2014, foreign brands have continued to experience difficulty in obtaining recognition especially when compared to domestic Chinese brands which naturally have more local presence.

Protection and benefits of well-known trade marks

Under Article 13 of the TML, the degree of protection afforded to well-known trade marks depends on whether the mark is registered in China or not. Both registered and unregistered marks are protected against the use and/or registration of third party marks which are *reproductions, imitations or translations* of the well-known trade mark. This wording is slightly wider than the usual protection given to prior marks on the register which would be protected against other marks which are “*identical or similar*”.

Well-known trade mark protection is an exception to the “first-to-file” rule and sub-classification system in China. Well-known trade marks registered in China are given cross-class protection: third party marks covering *non-identical or dissimilar* goods or services will not be allowed to be registered (as long as the use of such marks would confuse the public and prejudice the interests of the registrant of the

Key Issues:

- Clifford Chance recently assisted Aston Martin Lagonda Limited in successfully obtaining well-known trade mark recognition in China for the “ASTON MARTIN” mark.
- Well-known trade mark recognition is a powerful tool for combating infringers and trade mark hijackers as it offers a much broader scope of protection than offered to normal registered trade marks.
- Brand owners looking to obtain well-known status protection for their marks need to document and collate evidence of use and promotion in China in a careful and considered manner.

well-known mark). Protection for unregistered well-known marks extends to identical or similar goods or services.

This proves to be especially helpful in infringement cases. Infringers nowadays have become more sophisticated than ever. Very often infringers do not merely copy famous brands entirely. Instead, they may imitate famous brands by copying some parts of the design with other elements added in; or they may use a pirated (or imitated) mark that is not registered in relation to precisely the same goods/services. When faced with such infringing activities the potential enforcement actions will not be so straight-forward for normal trade marks.

However, owners of well-known trade marks are able to assert their rights against such infringing use with increased chances of success, so long as the infringing use is after the date for which the trade mark has been officially recognised as well-known.

Recognition process and supporting evidence

Well-known trade mark status is determined on a case-by-case basis by the Court or trade mark authorities when considering the merits of infringement cases or oppositions or invalidations in China. A request for the recognition of a well-known trade mark can be made to (i) the CTMO in trade mark opposition cases, (ii) the Administration for Industry & Commerce (“**AIC**”) when trade mark infringement is being investigated, and (iii) the TRAB in trade mark refusal and invalidation cases. Courts may also recognise the well-known status of a trade mark in civil and administrative trade mark cases.

A request for well-known recognition must be supported by ample factual evidence of reputation. Under the “*Provisions on the Determination and Protection of Well-Known Trademarks*” (which became effective in August 2014), a mark must be shown to be “widely known by the relevant public in China” before well-known recognition is granted. This burden is higher than the standard under previous trade mark laws, which merely required the mark to be “generally known by the relevant public in China and to enjoy a relatively higher reputation”.

The following evidence is taken into account:

- materials showing the relevant public’s knowledge of a mark;
- materials showing the period of use of a mark, such as materials on historical use, scope of use and registration of the mark;
- materials evidencing the duration, intensity and geographical reach of any promotion of the mark, such as materials showing the manner, geographic scope, type of media and the quantity of advertisements in the three years prior to the filing of the mark which is the subject of the case;
- materials showing that the mark has been protected as a well-known trade mark in China, or in any other country or region; and
- other materials showing that the mark is well-known, such as the revenue, market share, net profit, taxes on and sales territories of key products bearing the mark in the three years prior to the filing of the mark which is the subject of the case.

The Aston Martin case

In July 2015, a Shanghai company obtained a registration for “AstonMartin” in Class 10 (the “**hijacked mark**”) covering the goods “*medical apparatuses and instruments*”. Subsequently, in 2016, Clifford Chance on behalf of Aston Martin filed an invalidation application against the hijacked mark with the TRAB.

Amongst other arguments in the invalidation action, Clifford Chance requested that Aston Martin’s PRC reg. no. 767245 for “ASTON MARTIN” in Class 12 be recognised as well-known in China. To support this request, various media coverage was produced as evidence, including Chinese materials on the history and background of Aston Martin, marketing brochures and photos of the mark’s participation in exhibitions, and registration certificates of ASTON MARTIN marks.

The TRAB accepted the evidence as sufficient to show that the “ASTON MARTIN” mark had achieved well-known status in China in relation to automobile and related accessories prior to the filing date of the hijacked mark. By extension, the mark “ASTON MARTIN” was afforded cross-class protection under the PRC Trademark Law and the hijacked mark was declared invalid.

Enforcement efforts and how you should prepare

Decisions acknowledging the well-known status of trade marks are followed by government departments such as the CTMO, the TRAB and the AIC (unless the opposing party produces sufficient evidence to dispute this finding). These decisions will be useful as evidence in both applications and enforcement cases.

Brand owners who are looking to obtain well-known status protection for their marks in China will need to document and collate evidence of use and promotion in China in a careful and considered manner. In addition, since the recognition is issued as part of the overall decision on the merits of a particular case, it is important to strategically select an appropriate case to enhance the chances of obtaining such recognition. The filing date of the other party’s mark will be an important consideration since it will be the reference date used by the Court and the authorities in their assessment as to whether the brand owner has produced evidence of having attained a well-known status.

Despite the need to devote substantial time and effort in collecting evidence and preparing appropriate submissions, obtaining a well-known status mark would greatly facilitate future enforcement actions in China. It should therefore be considered by all brand owners who have substantial presence or fame in China as part of their brand/enforcement strategy in the country.

HONG KONG: CHINA'S NEW ANTI-UNFAIR COMPETITION LAW

China revises its Anti-Unfair Competition Law

China's main legislation on unfair competition practices has received a long-awaited overhaul with the revised Anti-Unfair Competition Law (the "**New Law**") having come into force on 1 January 2018.

The New Law is the first update to the Anti-Unfair Competition Law originally promulgated in 1993 (the "**Old Law**").

The Old Law was formulated according to market practices current back in 1993. There is hence a need for many of the principles and definitions to be updated. The New Law has expanded the scope of commercial bribery offences and introduced additional offences for IP, commercial secrets and other market-conduct related violations. It has also eliminated many overlaps with the Old Law with other related laws/regulations and adjusted penalty amounts.

Compared with the Old Law, the New Law has brought in several significant amendments as follows:

Revising the definitions of unfair competition activities – Article 6 (and Article 18(2))

The categories of prohibited acts which cause market confusion (such as misuse of trade marks, name or packaging) have been expanded under Article 6 of the New Law and the criteria for obtaining protection have also been relaxed.

Article 6 provides that any of the following actions, which lead to confusion as to the origin or association of a product, will be prohibited:

- unauthorised use of the name, packaging or decoration, etc., or marks similar to the name, packaging or decoration of products of a certain level of influence;
- unauthorised use of another's corporate name (including short forms), personal name (including pen, stage and translated names), domain name or website name which are of a certain level of influence; and
- other confusing acts which would mislead people into believing that a product originates from a third party or has a particular association with a third party.

These changes are in contrast to the Old Law which only offered protection to "*unique names, package or decoration*" of "*famous commodity*". Although there is no clarity as to how to demonstrate "*a certain level of influence*" under the New Law, it is hoped that this will be clarified in subsequent implementing regulations. Drawing an analogy from the same standard used in the PRC Trade Mark Law, "*a certain level of influence*" should be a lower threshold than "*famous*". In addition, the New Law has also clarified that "short forms" of corporate names, domain names and website names are also protected.

Key Issues:

- China's new Anti-Unfair Competition Law came into effect on 1 January 2018.
- There are expanded prohibitions against the unauthorised use of third party marks, names and brands.
- Protection of trade secrets and prohibition against commercial bribery are both broadened in scope.
- Prohibitions on unfair trade practices, including online trade practices, have also been updated.

On the other hand, the prohibitions relating to the counterfeiting of “*registered trade marks*” have now been removed to reduce overlaps with the PRC Trade Mark Law.

If it is a company's name which contravenes the provisions of Article 6 above, Article 18 of the New Law empowers the company registration authority to replace the company name with the company's unified social credit code pending the change of name procedures to be carried out by the business operator. This is a practical and welcome improvement for brand owners so that any infringing company names can be quickly removed with the aid of the relevant registration authority.

Trade secrets – Article 9

The New Law prohibits a business operator from:

- obtaining another's commercial secrets by theft, bribery, intimidation or other improper means;
- disclosing, using, or allowing third parties to use another's commercial secrets obtained by the means mentioned in the preceding paragraph; or
- disclosing, using or allowing third parties to use another's commercial secrets in violation of an agreement or another's requirements on keeping such commercial secrets confidential.

The New Law has not made substantial changes in respect of trade secrets infringement. The major changes are: (i) updating the definition of “trade secrets”; and (2) extending protection against third parties who do not misappropriate the trade secrets by themselves but who use/publish trade secrets with knowledge (or constructive knowledge) that the trade secret has been misappropriated. In this regard:

- the New Law defines “trade secrets” as technical information and operational information not known to the public that has “commercial value” (and for which measures have been taken to maintain confidentiality). This is in contrast with the old definition which required “economic benefits and practical value”. The new definition, which has removed the requirement for “practical value”, offers a broader protection to cover trade secrets which may not have practical use; and
- it is also provided that, where a third party knows or ought to be aware that an employee or former employee of the owner of commercial secrets (or any other entity or individual) has committed any of the illegal acts listed above – but nonetheless accepts, publishes, uses or allows any others to use such secrets – the third party will itself be deemed to have infringed the trade secrets. Therefore, even though the third party may not have obtained the trade secrets directly from an employee, the third party could still be liable if the employee or former employee disclosed the trade secrets unlawfully in the first place.

Redefining commercial bribery – Article 7

The Old Law prohibits commercial bribery aimed at the sale or purchase of products. The New Law expands this prohibition to include commercial bribery aimed at securing a transaction *opportunity* or *competitive edge*. Furthermore, the prohibition is no longer limited to bribery of those directly involved in a transaction but now includes those who may use their powers to influence to affect a transaction.

New Rules against internet-related unfair competition by technical means – Article 12

The New Law also introduces new regulations against unfair competition acts in the online space. Persons are prohibited from:

- inserting a link into a network product or service legally provided by another operator to compel a destination jump without the approval of such operator;
- misleading, deceiving or compelling users into modifying, closing, or uninstalling a network product or service legally provided by another business operator;
- implementing in bad faith an incompatibility with a network product or service legally provided by another business operator; or
- any other act that impedes or disrupts the normal operation of network products or services legally provided by another business operator.

The key idea behind the conducts listed above is that an Internet company is prohibited from obstructing legitimate activities of competitors. The last prohibition appears to be a “*catch-all*” provision which can be used to enforce against a wide variety of objectionable acts in the online space.

Increasing the Penalties of Prohibited Activities

Very often, it is difficult to determine the actual loss suffered by the rights holder or the illegal gains obtained by the infringer, which are used as the basis for determining damages. Thus, the enhanced amount of penalties becomes very helpful as rights holders will often seek statutory compensation instead of trying to establish the damage caused by the wrongdoing or having to calculate any illegal gains made by the infringer, which are often intangible and difficult to estimate. See below some examples of the tougher penalties:

- *Unfair Competition Activities – Article 6*: Fines for contravention of Article 6 are increased to up to 5 times the illegal gains (an increase from up to 3 times the illegal gains). Where the illegal gains cannot be determined, a fine of up to RMB 250,000 may also be imposed.
- *Commercial bribery – Article 7*: The limit on fines for commercial bribery is increased from RMB 200,000 to RMB 3 million.
- *Trade secrets – Article 9*: The limit on fines for contravening the prohibitions on trade secrets has been increased more than tenfold from RMB 200,000 to RMB 3 million.
- *Online trade practices – Article 12*: Contraventions of the new regulations against unfair competition acts in the online space will also attract fines of up to RMB 3 million.

Cases of serious contraventions of Article 6 (unfair competition activities) and Article 7 (commercial bribery) may now result in the revocation of the business licence of the infringer as well.

Reinforcing Supervision and Inspection – Articles 13 and 28

The investigative powers of authorities to investigate acts of unfair competition have also been expanded under the New Law. For example, authorities are granted powers to (i) access the business premises involved in a suspected act of unfair competition for inspection; (ii) question the business operator under investigation; and (iii) inquire into the bank account of a business operator suspected of an unfair competition act.

A fine of up to RMB 5,000 (for individuals) and RMB 50,000 (for corporates) may be imposed for any obstructions to the supervision or investigation by authorities under the New Law.

Conclusion

In summary, the New Law has brought the Old Law up-to-date in many areas. In particular, it addresses some of the issues raised by advances in technology by setting out new objectionable online trading practices as unfair competition acts enabling enterprises/business operators to better safeguard their legitimate rights and interests when faced with unfair competition online. In addition, the New Law has also removed many ambiguities and overlaps under the Old Law to provide a much broader protection for rights holders which is to be welcomed.



LONDON: UPDATE ON TV FORMAT PROTECTION

The global television formats business is a multi billion pound industry based on lucrative licensing deals in multiple territories. However, legal protection varies significantly between jurisdictions. In the UK, claims have been made that TV formats should be protected as “dramatic works” under the Copyright, Designs and Patents Act 1988. In the CDPA, a ‘dramatic work’ is a work of action, with or without words or music, which is capable of being performed before an audience. In *Green v Broadcasting Corporation of New Zealand* [1989] UKPC 26, a claim that the format of the TV talent show ‘Opportunity Knocks’ could be protected as a dramatic work failed. It was held that there was not sufficient certainty or unity in the show’s format to make it capable of being performed. This has left TV format creators with little guidance on how their formats could be capable of protection in copyright. However, the recent case of *Banner Universal Motion Pictures Ltd v Endemol Shine Group Ltd & Anor* [2017] EWHC 2600 (Ch) has shed some new light on the potential for TV formats to be protected as dramatic works. The new developments, while as of yet untested in English courts, should come as positive news to TV format creators who have previously struggled to obtain protection for their creations.

Changes to the protection TV formats in the UK

Recently, the High Court of England and Wales ruled in *Banner Universal Motion Pictures Ltd v Endemol Shine Group Ltd & Anor* that a particular TV format document did not qualify for copyright protection as a dramatic work as its contents were unclear and lacking in specifics. However, the judge provided helpful guidance on the way TV formats should be recorded or expressed in order for there to be a prospect of success for it to be protectable as a dramatic work.

The Claimant (“Banner”) alleged that, after pitching the concept of its TV game show for ‘Minute Winner’ to one of the Defendants (the Swedish TV production company, Friday TV) in 2005, Friday TV went on to copy the format, by developing a similar game show format called ‘Minute to Win It’. ‘Minute to Win It’ first aired in the US in 2010 and was subsequently aired in the UK on ITV2 in 2011. It has since been sold in over 70 countries worldwide.

The concept for the Minute Winner game show involved members of the public being given exactly one minute to try and win a prize. The show format was set out in a short document (‘the Minute Winner Document’) which described such features of the show

Key Issues:

- TV format creators have struggled to find appropriate protection for their works in IP law both in the UK and worldwide.
- The new Banner case sheds new light on whether a TV format can be protected under copyright law in the UK.
- It is important for TV format creators to document as much information as possible in respect of the format of their show to demonstrate that the work should be protected under copyright law.

as a brief synopsis; where the program was to be filmed; and the prizes that could be won. Banner claimed that copyright subsisted in the Minute Winner Document as a dramatic work and that the Defendants had infringed this copyright by producing 'Minute to Win It'. Banner also was unsuccessful in bringing a claim for Breach of Confidence and Passing Off.

Snowden J held that the Minute Winner format could not be afforded copyright protection. He explained that copyright protection will not subsist unless, as a minimum; (i) there are a number of clearly identified features which, taken together, distinguish the show in question from others of a similar type; and (ii) that those distinguishing features are connected with each other in a coherent framework which can be repeatedly applied so as to enable the show to be reproduced in recognisable form. Snowden J also acknowledged the possibility for TV formats (even if not fully developed) to be protected by the law of confidential information, while noting that information which is too vague, insufficiently developed and of a very general nature is unlikely to qualify for protection under the common law of confidential information.

In practice, this means that production companies should document as much information as possible about the format of their show in order to demonstrate that it has a coherent framework. The bible of documents should contain comprehensive details of all aspects of the show's concept including: any scripts, catch-phrases, set designs, floor plans, costumes, logos, theme tunes and other relevant aspects relating to the "look and feel" of the show. Although it should be noted that whilst Snowden J has set out the minimum requirements, we would probably still need further judicial analysis in order to properly formulate a test to determine when TV formats qualify for protection. It will now be interesting to see if the courts of other jurisdictions adopt a similar approach.



DÜSSELDORF: BLOCKCHAIN AND ITS APPLICATION IN THE FIELD OF IP: SMART CONTRACTS AND IPR MANAGEMENT

The enormous potential of blockchain and its real-world application has increasingly gained traction throughout all industries. In 2017 the dreamlike growth in value of the blockchain-based cryptocurrency “Bitcoin”¹ brought the concept of blockchain to the attention of the general public. However, the ongoing debate about Bitcoin’s suitability as a financial investment should not detract from the fact that the underlying technology of the blockchain-protocol and similar technologies based on the idea of a decentralized register are going to have tremendous impact on how we – and machines² – do business in the future. This is especially due to the fast-growing digitization and automation of our world in general. While the bandwidth of real-world use cases is still subject to ongoing research, one of the fields that will profit from the possibilities of blockchain are “smart contracts”, i.e. legal contracts built and executed (entirely or in parts) by means of software. The present article aims to provide a first glimpse on how Intellectual Property Rights (“IPR”) might play a role in this “new world” of blockchain and smart contracts.³

Blockchain and Smart Contracts – an overview

The blockchain-protocol was first introduced in a whitepaper published under the pseudonym *Satoshi Nakamoto* in November 2008.⁴ The whitepaper describes a concept where bundles of transactions (*blocks*) between users (*nodes*) are cryptographically linked in chronological order, creating a continuous, tamper-proof register (*chain*) that is stored and managed by all users simultaneously (*distributed ledger*). Intermediaries such as centralized service providers are not required. Each user disposes of a *private key* (to initiate a transaction) as well as a *public key* (to receive funds). Dedicated participants of the network (*miner*) provide the necessary computing power to validate transactions (*Proof-of-Work*) while creating (*mining*)

Key Issues:

- In general, first use cases of blockchain and smart contracts appear to be promising, but further research will be required to assess the full potential and possible legal challenges in the future.
- Copyright and patent law provide the required legal means to protect any new development in this field.
- IP could be subject to and managed by smart contracts. However, certain limits are reached where human judgment is required (e.g., construction of legal concepts such as “reasonable” or “necessary”).



¹ As well as other cryptocurrencies such as Litecoin, Ethereum, Ripple or IOTA.

² Machine-to-machine (“M2M”) business means the automated exchange of data between machines in order to fulfil certain tasks as important part of the Internet-of-Things (“IoT”). Bosch Software Innovation estimates the number of such “Connected Devices” to be around 14 billion in 2022, see <https://www.bosch-si.com/de/iot-plattform/aktuelles/downloads/whitepaper-iot-big-data.html>.

³ The question whether and to what extent Blockchain-technology may enjoy IP protection will be subject to the article “Securing IPR on Blockchain-Technology from a German law perspective” in this Newsletter.

⁴ The whitepaper “Bitcoin: A Peer-to-Peer Electronic Cash System” can be downloaded from <https://bitcoin.org/bitcoin.pdf>. To this date, its true identity of the creator(s) of the blockchain-protocol remains unknown.

Bitcoin as reward for their expenses (e.g., hardware, energy costs). However, Bitcoin is only one application of distributed ledger technology, which is expected to be useful in a broad variety of other cases across almost all industries in the future.⁵

Smart contracts, a concept first postulated by the computer scientist Nick Szabo in 1994⁶, are intended to execute contractual obligations through software code. For example, if a certain pre-defined condition is met (e.g., confirmation of a payment), the code triggers the respective legal consequence(s) (e.g., dispatch of delivery good; grant of access to know-how). In this context, a blockchain linked to a smart contract could provide the parties with a transparent, verifiable, tamper-proof register to record the contract's execution. But not all types of contractual obligations can be described by a (rather simple) digital *true/false*- or *if/then*-scheme which is more applicable to standardized procedures.⁷ More complex tasks on the other hand, such as:

- the compilation/execution of contractual obligations;
- the weighting of the parties' interests; and
- the construction of undefined legal concepts like "reasonable" or "necessary",

may not be mastered by software alone, but will likely require human intellect in order to resolve any disputes in a fair and well-balanced way – at least with current technical means.

IPR managed by Blockchain-applications

Any type of IP (e.g., patents, utility models, trade marks, know-how etc.) could be subject to a blockchain-application as the object of the transactions can be freely defined dependent on the purpose of the respective use case. One field of application may be (public) IP registers such as the German or European patent and trade mark registers. For example, assignments of IP rights, licenses or pledges on patents could be entered into a **blockchain-based IP register** directly by the parties (respective software API provided), reducing time and costs of Office proceedings. In addition, it could render the register more reliable regarding the substantive legal situation, ensuring the register is kept more up-to-date.⁸

In the context of any development agreement, any work results (e.g., contributions of collaboration partners, freelancers) – or rather the IP's corresponding "digital fingerprint" (*hash value*) can be stored in the blockchain, enabling the contracting parties (as well as any other third parties) to verify the IPR's coming into existence at a certain point in time (*Proof-of-Existence*). Such proof can be of particular importance if

Blockchain: A decentralized "account book", reporting a chronological database of transactions and organized into blocks of data.

Block: A bundle of transactions, referring to the preceding block in the blockchain.

Distributed ledger: A database held and updated independently by each participant in a large network.

Proof-of-Work: Highly complex computational results to ensure that only legitimate transactions are included into a blockchain in order to prevent duplicate transactions (*"double spending"*).

Miner: Dedicated participants of the network who may add blocks to the blockchain by solving cryptographic "puzzles".

Smart Contracts: A computerized transaction protocol that executes the terms of a contract.

⁵ For an overview of potential use cases of blockchain technology, please see for example <https://gomedici.com/45-plus-use-cases-for-blockchain-technology/>.

⁶ According to Szabo, a smart contract is „a computerized transaction protocol that execute[s] the terms of a contract“.

⁷ For this reason, smart contracts are often compared to vending machines where inserting a coin and selecting the desired leads to the releasing of the good to the client.

⁸ For example, the German patent and trade mark register is many cases outdated as the parties may transfer the respective IPR without informing the Office as the change of the respective register entry is no requirement for the transfer to become legally effective. Especially in case of large portfolios, the parties tend to refrain from filing such update for time/cost reasons.

the applicable legal regime does not provide for a registration mechanism (conveying absolute rights to a person on a given subject matter) such as (German) Copyright law.

With respect to smart contracts, blockchain may further be suitable for the management of access authorization and the grant of licenses. For example, **access to digital online content**⁹ (e.g., music, videos, photos, other documents) would only be provided if the respective payment made by the user was validated in the blockchain. Similarly, in case of **licensing relationships**, the smart contract/blockchain could track the grant of licenses and/or sublicenses and the orderly payment of royalties (which could be calculated based on the number of acquired licenses or other data).

Another use case may be **“Smart” Research and Development (“R&D”) Agreements** where the collaborating parties license their existing IP to each other in order to create new IPR. The regime of allocating ownership of (new) IPR and (unilateral/mutual) licensing of project IPR might be handled via a blockchain solution. Moreover, confirmation that certain project milestones are reached (e.g., successful development of a first-stage prototype) could unlock further funds.

However, so far blockchains have their limits where more complex issues such as legal assessments become necessary. That could include the evaluation of whether the developed subject matter actually complies with the desired research results envisaged under such “Smart” R&D Agreement or any construction of a term which needs interpretation.

Conclusion

Industry 4.0 and the technologies that come with it are still in their early stages. However, it is clear that digitization and automation of entire industries are progressing at a fast pace and will shape our lives over the next few decades. With respect to blockchain and the **design, supervision and enforcement of smart contracts**, it is clear that IP lawyers will need to accumulate the necessary IT know-how to render effective legal advice. While it might not yet be entirely clear to what extent these new technologies will be implemented or when the necessary software standards will be available, first use cases appear to be promising and should be closely monitored from the start.¹⁰

Examples of further potential use cases:

- Geneva has implemented a commercial register based on blockchain technology.
- Blockchain-based decentralized organizations (“DAOs”) that can operate autonomously (e.g., managing funds).
- In Estonia public notary services are provided via the platform “Bitnation” enabling registered residents to notarize business contracts, birth certificates and even marriages.¹¹
- A number of countries such as Canada run research projects to establish blockchain-based identity management systems.¹²
- Local energy trading focused on building blockchain-backed smart grids.¹³

9 For a music distribution service, see for example UJO (www.ujomusic.com) und PeerTracks (www.peertracks.com).

10 <https://www.cliffordchance.com/news/news/2018/01/digitale-transformation--clifford-chance-buendelt-globale-tech-e.html>.

11 <https://bravenewcoin.com/news/e-estonia-initiative-progresses-with-blockchain-partnerships/>.

12 <https://www.ethnews.com/blockchain-based-id-management-systems-being-developed-for-canada>.

13 <http://fortune.com/2017/12/24/siemens-blockchain-lo3/>.

DÜSSELDORF: SECURING IP RIGHTS IN BLOCKCHAIN-TECHNOLOGY FROM A GERMAN LAW PERSPECTIVE

It is of utmost importance to secure intellectual property rights over new developments in the field of blockchain/smart contracts at an early stage in order to stay competitive in the market. Under German law, blockchain-applications, including smart contracts consisting of computer software/algorithms, can enjoy protection under the German Patent Act ("**GPA**") as well as the German Copyright Act ("**GCA**"). The legal issues that arise in this context are not entirely new, but certain aspects will present new questions when seeking protection for new technologies.

Patent protection

It can be assumed that the "basic" blockchain-protocol is not patentable as it likely became prior art following its publication in 2008. However, any subsequent developments encompassing the blockchain-protocol – or aspects thereof – could potentially enjoy patent protection if the legal prerequisites of Section 3 GPA (novelty and inventive step) are met. In particular, the software patent needs to provide for a technical solution of a technical problem, causing an effect in the outside world. This could be, as an example, software controlling anti-lock braking systems which reduce the risk of blocks in wheels.¹ The fact that a software runs virtual commands, triggering electric signals on a computer system which lead to certain computation results is generally not sufficient to consider a software patentable.

The significant number of blockchain-related patent applications at the German and the European patent offices in recent years (relating to, e.g., the management of digital wallets, smart contracts or identity management) show that stakeholders are confident that they can obtain the absolute (exclusive) right to commercialize the subject matter.²

However, these patent applications are clearly only part of a much larger trend with over 48,000 European patent applications related to Industry 4.0, as recently determined by the first European Patent Office landscaping study on "Patents and the Fourth Industrial Revolution (4IR)" in co-operation with the German Handelsblatt Research Institute.³ Finally, as the market for blockchain- and smart contract-solutions grows larger, stakeholders should consider commissioning Freedom-to-Operate searches before filing any patent and/or launching a product to ensure that they do not infringe any third-party IPR.

Key Issues:

- Developers of blockchain-technology should be eager to seek IP protection at an early stage of the development process.
- Patent and Copyright law provide for the necessary legal means to protect blockchain-technology.
- In addition, although certain aspects might still be unclear, blockchain may also enjoy protection as data base *sui generis* (Section 87a GCA), protecting the substantial investment made by the producer of the blockchain.

¹ German Federal Court, decision from 13 May 1980, X ZB 19/78.

² E.g., a cursory search for the keyword "Blockchain" (conducted on 6 March 2018) at the European patent register yielded 93 search results.

³ <https://www.epo.org/news-issues/news/2017/20171211.html>.

Copyright/database protection

Blockchain-applications and smart contract software may be protectable under Section 2(1) and Section 69a(1) GCA with regard to source and object code, draft material, the application programming interface (API) as well the graphic user interface (GUI) without any registration needed.

In addition, the blockchain itself could be protectable as a *sui generis* data base (Section 87a GCA), protecting in particular the financial investment made by the producer of the database. A blockchain can generally be considered a “data base” in terms of Section 87a GCA as it represent “a collection of works, data or other independent elements arranged in a systematic or methodical way and individually accessible by electronic or other means”.⁴ The producer of a database within the meaning of GCA is the person who has made the “substantial qualitative or quantitative investment”.

Further, the producer of the database “has the exclusive right to reproduce and distribute the database as a whole or a qualitatively or quantitatively substantial part of the database and to make this available to the public” (Section 87b GCA). Therefore, the regime of *sui generis* protection might not be useful with regard to the concept of a public (*permission-less*) blockchain (like Bitcoin) requiring the blockchain to be duplicated, stored and constantly updated among an unlimited number of anonymous users. Thus, the producer of the data base, i.e. the public blockchain – assuming that the producer can be determined⁵ – could not prevent third parties from copying the entire database as envisaged by Sections 87a et seq. GCA and therefore not exercise his rights of protection.

This might be different in case of private (*permissioned*) blockchains where the owner/investor or a designated administrator can restrict access to the network to a specific circle of users. In these cases, the blockchain does not necessarily have to be anonymous and the need for complex security mechanisms might be lower as the users’ identities are disclosed to the participants. The scope of the authorized use of the blockchain infrastructure by the participating users will then likely be covered by a respective agreement governing the terms of conditions. Private blockchains could be used, for example, for the purpose of monitoring/recording the execution of smart contracts under which IP is created, allocated and licensed via blockchain.⁶

20-21 March 2018, Amsterdam IPBC Europe 2018 – Harnessing IP value in European companies

Theme:
Inside IP transactions
(Claudia Milbradt)

Owning intellectual property gives you the ability to monetise assets through sale or licence – the challenge is to do it right.

- When to license, when to sell
- Top transaction tips
- Key issues in FRAND and licensing standard-essential patents

Interested? Find out more and register: <http://events.ipbc.com/events/ipbc-europe-2017/event-summary-988323652a0e4165b6412392e754d950.aspx>

Recent event
Ladies only – Zukunft im Blick
Cooperation Event with HSBC
13 March 2018
Digitalization – Chances and Challenges (Claudia Milbradt)

Claudia Milbradt – “She is very well prepared in court, defends cases well and tells you realistically what she thinks will and will not work.”
Chambers Europe 2018 - Germany, Intellectual Property: Patent Litigation

⁴ See Willecke, DSRITB 2017, 833, 837 et seq.

⁵ The question, who the “producer” of the data base is, needs to be assessed on a case-to-case-basis. The collection but not the generation” of the data is protected under Section 87 et seq. GCA.

⁶ For further examples in regard to smart contracts and IP, please refer to “Blockchain and its application in the field of IP: Smart Contracts and IPR management” in this Newsletter.

Conclusion

In a competitive, rapidly growing market, blockchain stakeholders such as software developers **should seek IP protection for any new developments early on**. German and European patent law as well as German copyright law provide for the necessary legal means to protect the right holders' interest in the future commercialization of blockchain. However, as the underlying technology is subject to ongoing intensive research, with many real-world use cases still to be developed in the coming years, **legal practitioners** will need to keep an eye on the most important trends and **will have adapt to the legal challenges**. Ultimately, it may also become an exercise for legislators to make the required adjustments for an efficient and fair legal framework in case the current law cannot keep up with the technological progress.



PRAGUE: BLOCKCHAIN TECHNOLOGY AND THE GDPR

Introduction:

Blockchain is one of the key technological inventions of recent times. Its importance has even been recognised by the European Commission, which recently launched the EU Blockchain Observatory and Forum to explore blockchain's potential. However, like other technologies, blockchain does not only open up new possibilities for business, but also gives rise to several legal issues. In this article, we briefly describe why the General Data Protection Regulation (the “**GDPR**”) may be applicable to blockchain technology and suggest what major risks may arise from using blockchain to process personal data.

Technology

Blockchain is a distributed ledger technology that records all digital transactions that have taken place across a peer-to-peer network. Each block in a blockchain consists of a list of records of executed transactions. The blocks are chained to each other sequentially using cryptographic pointers, which help maintain the security of records. Once a record has been entered on a block, it cannot be altered without leaving a trace. Thus, in principle, transaction data on the blockchain are immutable. The data is shared across the network and reconciled, with all participants in the network (nodes) having a copy of the chain. The decentralized and distributed nature of the blockchain thus removes the need for a centralised administrator. Blockchain is further characterized by the transparency of all executed transactions, which is ensured by records being made visible to other participants in the network. Finally, it should be noted that there are several kinds of blockchains, all of which have different features or architectures.

Personal data in blockchain

The GDPR only applies to the processing of personal data and defines personal data as all information relating to an identified or identifiable natural person, such as a name or national identification number.

On a blockchain, a participant initiates a transaction by signing it with his/her private key and broadcasting the transaction to all other network participants. The other participants only see the public key representing the participant making the transaction, which they are unable to read without having the private key. However, if the participant uses the same public key for several transactions, the participant can become identifiable. Therefore, the public key is regarded as personal data.

In addition, it is conceivable that the transactions on a blockchain will include personal data such as an ID number. The hashing used by blockchain assigns data with a code known as a hash. In a nutshell, the hash function takes input data, which may include personal data, and converts it into output data of a fixed length. A cryptographic hash

Key Issues:

- Data recorded on blockchain may qualify as personal data.
- Decentralized and distributed blockchain technologies may be subject to the regulations of various jurisdictions, including the GDPR.
- Data controllers and data processors on blockchain may be difficult to identify.
- The key features of blockchain may clash with the data protection principles and rights under the GDPR, in particular the storage limitation principle and right to be forgotten.

function only works one way, meaning that the output cannot be reversed later on. The Article 29 Working Party, an EU advisory body, considers such personal data to be pseudonymised in this way rather than anonymised. Accordingly, this type of data should remain subject to the GDPR.

Applicable law

As a cyberspace phenomenon, blockchain does not recognize national borders. Network participants, their computers, and persons whose data are being processed can be located anywhere in the world. Thus, it is highly probable that data processing will be subject to the regulations of various jurisdictions. This is particularly the case for public blockchains, where the applicable data protection law should be determined on a transaction-by-transaction basis. With private blockchains, the probability of a conflict of laws is somewhat lower, as it is more likely that participants will be located in one territory only. However, unlike in contractual law, parties cannot choose the data protection law that will apply to them and thus it cannot be ruled out that other data protection laws may apply.

Considering the broad territorial scope of the GDPR, which covers (i) data processing carried out by non-EU data controllers and processors processing the personal data of data subjects from the EU where the offering of goods or services is concerned, and (ii) how these non-EU data controllers and processors monitor the behaviour of EU data subjects, blockchain is likely to have an EU-related element that will trigger the application of the GDPR.

Identification of data controllers and data processors

To comply with the GDPR, it is crucial for the data controller and data processor in each blockchain to be correctly identified. In general, the data controller is the person that determines the purposes and means of processing personal data, whereas the data processor processes the personal data on behalf of the controller.

Given the decentralized nature of blockchain, where all network participants share their resources on a peer-to-peer basis and can add information to the ledger without requiring any authorization from a central administrator, identifying these persons can be a very challenging task. In general, any participant entering personal data in blocks of the chain can qualify as a data controller of the data it has provided. At the same time, any participant can be regarded as a data processor in respect of the personal data of which it has a copy.

Consequently, under the GDPR, if there are two or more controllers that jointly determine the purposes and means of processing personal data, they, as joint controllers, must conclude governance arrangements on their respective responsibilities. However, it is questionable how feasible this actually is, particularly in relation to public blockchains with thousands of nodes. The situation appears to be more straightforward with private and permissioned blockchains, as these networks are not accessible to everyone and only certain participants have permission to add information to the blocks.

Although the fact that only network participants are subject to GDPR obligations may appear to let companies providing blockchain solutions off the hook, the reality is somewhat different, in particular for blockchains that involve an administrator. Each

blockchain must therefore be assessed separately to enable the roles of each party and their obligations to be identified.

Possible conflicts between blockchain technology and GDPR

We are of the opinion that the greatest challenges for blockchain in respect of the GDPR (besides determining the applicable law and correctly identifying the roles in a network) are compliance with the right to be forgotten and the principle of storage limitation.

Since being recognised by the CJEU in the *Google Spain* case, the right to be forgotten has been explicitly inserted into the GDPR. Essentially, this right allows data subjects to request the erasure of their personal data and obliges data controllers to do so and to notify other controllers of any such request where there are grounds for their erasure. Grounds for erasure include personal data no longer being necessary for the purposes for which they were collected or processed, and personal data being unlawfully processed.

According to the principle of storage limitation, data must be kept in such a way that enables data subjects to be identified for no longer than is necessary for the purposes for which their data are being processed.

Immutability, one of the key features of blockchain technology, seems to conflict with both the principle of storage limitation and the right to be forgotten. As mentioned above, the immutable nature of blockchain means that data added to blocks cannot generally be removed. Thus, the data controller may not be able to erase data even where grounds for their erasure exist. The deletion of data requires the cooperation of at least 51% of nodes. Not only is this threshold difficult to reach, but it may also trigger the Streisand effect, where the data subject's attempts to have his or her personal data forgotten could conversely attract more attention. Where the motive for erasure concerns data no longer being necessary for the original purpose, it could be argued that this data must be perpetually retained on the blockchain, the purpose of which is to achieve transparency by evidencing all transactions made at any time in the past and preventing them from being altered. Nonetheless, this argument remains to be assessed by data protection authorities. It is important to note that this would only resolve the issue surrounding one motive for erasure, rather than providing a comprehensive solution.

Conclusion

As demonstrated above, processing personal data using blockchain technology can prove problematic. However, this does not mean that blockchain technology cannot be compliant with the GDPR. Indeed, there are already blockchains that, for instance, store personal data off chain in order to make information editable and thus enable compliance with data protection laws. Nevertheless, before launching any blockchain technology that may process personal data, it is worth considering the legal implications in order to avoid placing oneself at risk of facing fines under the GDPR, which might amount up to 20 million euros or 4% of a company's total worldwide annual turnover.

MILAN: TRADE SECRET'S PROTECTION AND BIG DATA: AN ITALIAN VIEW

The aim of intellectual property law is to reward investments made towards innovation. Nowadays, one of the most relevant drivers of innovation is data science, *i.e.* the techniques of analytics (models and algorithms) applied to 'big data' which is mined from several data lakes and collected from a number of sources (e.g. social networks, apps, web traffic, Internet-of-Things, etc).

However, the very concept of big data does not easily lend itself to 'classic' intellectual property protection. As such, enforcing rights in big data may prove to be a difficult task.

Enforcing rights in big data through 'classic' intellectual property rights

As far as **patent law** is concerned, courts subject patentability to the narrow condition that software solves a technical issue or improves a process (e.g. by reconfiguring data into different display sets, or by reformatting data from disparate sources), and not just executes routine operations (e.g. collecting or listing data) which an individual may do by hand.

The **copyright protection to databases** also only offers a limited scope of protection, since copyright covers the way data is compiled and not the content of the compilation (data) or the algorithm used. As recently confirmed in the EU Commission's report following the consultation on the Database Directive, the ***sui generis* right in a database** also provides limited protection. According to CJEU case-law on the matter, the creation of a database must be excluded from the relevant investment. Furthermore, the territorial limitation imposed on *sui generis* rights in databases (only enforceable within the European Union and few additional countries) clashes with the global nature of big data operations.

From a civil law standpoint, data *per se* cannot be owned as clarified by a number of case precedents all around Europe. That being said, access to data can be regulated: when granting access to a third party pursuant to a **license agreement** – in order to maximise the value of big data – **contract law** may provide legal basis for the data right holder to both seek reward for its investment in and to maintain control over data. However, competitors who are not party to the license agreement may still aim at taking a free ride off the back of the right holder who may then not be in a position to rapidly enforce its rights against these free riders.

Trade Secrets: can secrecy protect investment in big data?

Some Italian jurists are debating whether **trade secrets** could ensure confidentiality over algorithms and processes.

Key Issues:

- National implementation of Directive (EU) 2016/943 (Trade Secret Directive)
- Public Consultation on Directive (CE) 1996/9 (Database Directive)
- Articles 98-99 of Italian Legislative Decree no. 30/2005 (Italian Code of Industrial Property)

Monica Riva – “Monica has a strong ability to consider all the different parameters, and to expose facts and considerations in a clear and simple manner.”

Chambers Global & Europe 2018 – Intellectual Property

Monica Riva – ranked in Band #4

Chambers Global 2018 and Chambers Europe 2018 – Intellectual Property

The issue is of particular interest in the EU, since Member States are about to implement the **Trade Secret Directive**. Implementing this directive may change the way trade secrets have previously been dealt with by affording a greater level of protection to big data processes and data science techniques.

The current Italian approach to trade secrets already considers these issues and could therefore be seen as an appropriate model for national implementation of the Trade Secret Directive. In particular, data mining and data analytics processes can meet the ordinary requirements imposed by articles 98-99 of Italian Code of Industrial Property which cover both 'commercial' (e.g., customer lists and mailing lists) and 'technical' know-how (e.g., data mining and data analytics, formulae, procedures, and techniques).

Data mining and data analytics processes will likely fall under 'technical know-how'. These processes are **secrets**, *i.e.* they are not, as a body or in the precise configuration and assembly of the components, generally known among or readily accessible to persons within the circles. Data mining often entails a high degree of subjective judgment. These processes also have **commercial value**, in that the very goal of big data is to give the data holder a competitive advantage lying in the insights that can be inferred from data. Lastly, the data holder can easily adopt **reasonable steps to keep the data secret**, by employing technical measures of protection and/or legal measures, such as confidentiality and non-disclosure agreements, which, in any event, allow additional protection and easy-to-enforce contractual remedies against breaches of confidential processes.

Conclusions

In addition to license agreements, which can help the right holder regulate rights in and access to data, protection under trade secrets rules seems to be the best *candidate* to afford legal protection against third-parties' unauthorised use of big data and data science. The upcoming national implementation of the Trade Secret Directive into the EU Member States' regulations could be the first opportunity to expressly confirm this expectation.

LINK DIRECTORY

Directive (EU) 2016/943 (Trade Secret Directive):

<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0943>

Report on public consultation on Directive (CE) 1996/9 (Database Directive):

<https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-legal-protection-databases>

Andrea Ottolia, *Big Data e innovazione computazionale*:

<http://www.giappichelli.it/big-data-e-innovazione-computazionale,9211234>

Andrea Tuninetti Ferrari, *Big Data: Balancing the Web User's and the Service Provider's Rights in the Big Data Era*:

<http://dspace-unipr.cineca.it/bitstream/1889/3333/1/Andrea%20Tuninetti%20Ferrari%20-%20Tesi%20dottorato%20-%20Big%20Data.pdf>

LONDON: COPYRIGHT IN AI-GENERATED WORKS

AI and IP: copyright in AI-generated works (UK law)

Artificial intelligence (“AI”) is a broad term used to describe a range of software functionality. At present, it is used almost synonymously with ‘machine-based learning’. In this article we consider some of the intellectual property law issues arising from the increasing prevalence, and increasing capability, of AI software. In particular, we will consider from an English law perspective, whether copyright can subsist in an AI-generated work and whether AI systems can infringe third party copyright.

Does copyright law recognise AI-generated works?

Traditional copyright law protects the original creations of authors (which include artists, composers and other creators). An author of a work is defined as the person who creates it, with additional clarification for particular types of work, e.g. the producer of a sound recording is deemed to be its author. For a literary, artistic, dramatic or musical work, which includes software, to qualify for copyright protection the work must be “original”. Case law provides that for a work to be original it must be its “author’s own intellectual creation”.

The above is the threshold for originality; crucially it requires the exertions of a human author. Without a human author, the work cannot be original. If a literary, artistic, dramatic or musical work is not original, then no copyright subsists in the work (Section (1)(a) Copyright Designs and Patents Act 1988 (“CDPA”).

We already accept that authors may use tools, including computer software, to assist in the creation of their works. An example is a photographer using automatic settings and timers on a camera. The fact that the photographer used automatic settings and did not press the shutter button at the moment the photo was taken does not preclude him or her from being an author of an original photograph.

UK copyright law goes further and acknowledges the possibility that works could be ‘computer-generated’ defined as a “*generated by computer in circumstances such that there is no human author of the work*” (Section 178 CDPA). Section 9(3) CDPA provides that the author of a computer-generated work is deemed to be the person “*by whom the arrangements necessary for the creation of the work are undertaken*”. Continuing the photography analogy, if it were debatable whether merely rigging up a motion sensitive camera was enough to make someone an author of photographs it takes, Section 9(3) might clarify the position.

Who, if anyone, is the author?

If we assume that an AI tool has acted sufficiently independently of any human that the identity of the author in a normal sense is unclear, and Section 9(3) may therefore apply, the answer to the question whether copyright can subsist in an AI-generated work depends on whether it is obvious who is the human “*by whom the arrangements necessary for the creation of the work*” In the short term this is likely to mean whether a human user of the AI tool is the author of works created, or whether it is the original programmer of the AI tool.

Key Issues:

- For the time being, the author of an AI-generated work is likely to be a human user of AI or the original programmer. However, as AI becomes more autonomous, it may become increasingly difficult to say with certainty who made the arrangements necessary for the creation of a given work.
- The CDPA provides that the making of temporary copies by electronic means is a restricted act, which may amount to copyright infringement. Nevertheless, copyright can only be infringed by a person and does not extend to AI itself.
- The courts will likely look at the person most closely connected with the infringing act, including the degree of control the user has over the actions of the AI.
- Where the copying of third party works is inevitable, there is a strong case for infringement by an operator of AI. However, as AI advances, it is unclear whether an operator will be responsible for third party infringement, or whether other persons involved with the design of AI may be held accountable.

As AI becomes more advanced, and the tasks allocated to AI allow the AI system more freedom to make its own decisions, it may become increasingly difficult to say with certainty who created or made the arrangements necessary for the creation of a given work – or indeed whether anyone made the necessary arrangements at all. In the scenario where the AI is fully autonomous, if no person made the arrangements necessary for the creation of a work which requires originality for copyright to subsist, then no copyright could exist in the work as there would be no author.

Would high-level instructions of the operator suffice for authorship, would the role of the programmer of the AI system need to be factored in, or would we have to concede the work was created without any human intervention at all with the consequence that the work is not protected by copyright? This could have dramatic consequences for a party seeking to monetise works generated using AI tools.

Can AI infringe copyright?

Section 16(1) of the CDPA sets out the acts restricted by copyright in a work. These acts include reproducing a copyright work, which – crucially for AI – includes the making of temporary copies by electronic means. Whilst there are some permitted uses of copyright works, if AI is used in a commercial context these are unlikely to apply. Section 16(2) CDPA suggests that AI cannot of its own volition infringe the copyright in a work, as copyright can only be infringed by a “*person*” who does, or authorises another to do, one of the acts restricted by copyright.

Section 16(2) CDPA does not however provide carte blanche to developers and operators of AI software to allow the AI to use third party works with impunity. In case law where similar issues under Section 16(2) CDPA have been raised, the court has looked for the person most closely connected with the infringing act. If the creator of the AI and the user of the AI are separate, the degree of control the user has over the actions of the AI is likely to dictate whether a court would find that it is the operator of the AI which is the closest person, or the developer having provided the AI in the first place. The outcome will be highly fact-dependent.

Who is responsible for the AI's actions?

If an operator used AI software in such a way that the copying of third party works was inevitable then there would be a strong argument that the operator had caused the infringement. As AI advances, the question of whether an operator is responsible for the third party infringement will become much more opaque, particularly if the AI decides to copy or adapt a particular work absent any specific instructions to do – or not to do – so from the operator. There is a risk for developers that a court would look behind the operator to the design of the system. If, for example, the design of the AI system made the unauthorised use of third party copyright inevitable, developers may find it difficult to argue successfully that they do not have legal responsibility.

In the short term, serious consideration needs to be given to the appropriate allocation of risk in a licence of AI software (if applicable). In doing so this will require an understanding of how the AI operates and how it is intended to be used. Particular care should be taken if the AI will have access to public sources, such as the internet.

CC London:

Clifford Chance LLP has increased its ‘presence’ in this space, following the recent arrival of the ‘charming but tough’ **Stephen Reese** from Olswang LLP; he has considerable expertise in the life sciences sector and the ‘confidence to listen to views from the whole team’. Reese recently acted for Astex in a dispute with AstraZeneca regarding an Alzheimer’s drug’s clinical development. Brands specialist Vanessa Marsland, who focuses on the technology, media and consumer goods sectors, recently advised Mondeléz on the sale of various Australian brands, including Vegemite. Leigh Smith is experienced in handling soft IP, and fellow senior associate Anna Blest advises on transactional and contentious IP.

Legal 500, UK, 2017

In the long term, developers should look to control the risk by embedding the recognition of intellectual property rights within the AI's code itself. Developers of AI will need to teach their software to respect the rights of third parties, particularly if the AI is so advanced that the process by which tasks are completed is out of the control of the operator. A failure to do so could lead to a future finding that the developer, rather than the user, is the person *"most closely connected"* to the infringing act.



DÜSSELDORF: UPDATE ON THE UPC AND THE UNITARY PATENT: UK IN A POSITION TO RATIFY THE UPC AGREEMENT, GERMANY BLOCKED BY CONSTITUTIONAL COMPLAINT

After more than three decades of negotiations, the European Union has entered the final straight towards establishing a unified patent system. As a single patent right, the new Unitary Patent (“UP”) will provide protection for inventions in all EU Member States. Furthermore, the pursuit of infringements will be centralised at the Unified Patent Court (“UPC”) with jurisdiction across all participating countries.

One of the main reasons for the delay in establishing the new system were differences regarding language. In particular, Italy and Spain were reluctant to abandon their desire for European patent specifications being completely translated into Italian and Spanish. It was not until December 2010 that 25 Member States participated in the enhanced cooperation in accordance with Article 20 Treaty on the Functioning of the European Union (TFEU), leading to both EU regulations (Regulation No 1257/2012 and Regulation 1260/2012) and the UPC Agreement, which was signed on 19 February 2013.

The final hurdle to overcome before the UPC Agreement can enter into force, is the completion of the ratification process in the UK, Germany and France as they are the EU Member States with the highest number of patent filings. Furthermore, all three countries as well as the State of Luxembourg (which will host the appeal court) have to ratify the UPC’s Protocol on Privileges and Immunities (“PPI”).

France

France ratified the UPC Agreement on 14 March 2014.

UK

It came as a surprise, when the UK announced in November 2017 that it would ratify the UPC Agreement despite Brexit. In December 2017, the Houses of Parliament approved the draft followed by the UK’s Privy Council approval of the PPI in February 2018. Except for certain aspects devolved to Scotland, this completes the necessary legislative steps for the UK to be in a position to ratify the UPC Agreement.

However, when announcing the plan to ratify, the UK Minister responsible signalled that the UK will need to “negotiate a new relationship with the UPC” post Brexit and that this should be done as “seamlessly as possible so that businesses can continue to take advantage of the provisions that the UPC makes possible.”

Key Issues:

- The UK stands on the threshold of ratification. All relevant legislation is in place. However, after Brexit the situation may change again.
- In Germany the ratification was blocked by a constitutional complaint. Criticism surrounds the incompatibility of the UPC Agreement with European Union law, the missing qualified majority in the German Parliament, the lack of independence of the boards of appeal and the arbitrary determination of legal fees.
- However, German associations give new hope that the Unitary Patent project will still succeed. All organisations agree that the constitutional complaint is inadmissible and/or unfounded. There is hope that the Federal Constitutional Court will keep these opinions in mind when drafting its final decision.
- A decision on the constitutional complaint is expected later in 2018.

Even though it remains unclear what this will mean in practice, the legislative steps seem to prove that the UK indeed has the political will to ratify the UPC Agreement before it leaves the EU in March 2019 and – according to the statement of the UK Minister – wants to stick with the UPC system even when Brexit is triggered. However, withdrawal negotiations will determine to what extent the UK will stay part of the UPC system after Brexit.

Germany

In Germany the Federal Council (*Bundesrat*) approved the UPC Agreement and the implementation law in March 2017. Following the approval of the German Parliament (*Bundestag*) only ratification by the Federal President (*Bundespräsident*), the publication and the entry into force of the law were still necessary.

I. Ratification in Germany blocked by constitutional complaint

The ratification process came to an unexpected halt, when a constitutional complaint against the ratification of the UPC Agreement combined with an injunction to prohibit all involved parties to take further steps was filed on 31 March 2017. Remaining anonymous at first, the national journal GRUR explicitly confirmed that patent lawyer Dr. Stjerna filed the constitutional complaint.

The legal consequences were severe: the Federal President Frank-Walter Steinmeier followed the request of the Federal Constitutional Court (*Bundesverfassungsgericht*) on 3 April 2017 and ultimately did not sign the law in order to allow the court the necessary time to engage with the constitutional concerns. Therefore, the unified patent system will not come into force before the court reaches a decision which is expected to be rendered in 2018 as indicated by the Federal Constitutional Court in its “yearly preview list” on its website.

II. Constitutional concerns

The constitutional complaint questions the compatibility of the UPC Agreement with European Union law. It is feared that the Federal Republic of Germany gives away its sovereign rights, which is incompatible with the principle of democracy pursuant to Article 38(1)1 GG (*Grundgesetz*, the Constitution).

If the Federal Constitutional Court confirms a breach of constitutional law with EU law, it might submit the question to the European Court of Justice. Again, this would mean another delay.

Furthermore, the constitutional complaint rebuts that German Parliament acted by simple majority and not, as necessary, by qualified majority according to Article 23(1)(3) and Article 79(2) GG. The accusation was that instead of 630 parliamentarians being present, only 35 parliamentarians were.

However, the unanimous opinion is that this is less critical in comparison to the other points. In case of doubt, the voting needs to be repeated, whereby the result is likely to be the same due to a uniform political will.

Moreover, Mr. Stjerna criticises the lack of independence of the boards of appeal leading to a breach of the principle of separation of powers.

The UPC Agreement implements a new court. However, the boards of appeal are still responsible for decisions in patent prosecution procedures and opposition procedures.

Locally, the court and the boards of appeal are housed in the same building and are integrated into the same organisation and personnel management. However, this should not have a major impact on the court's decision anymore since the criticism was widely heard and a reaction followed immediately. The boards of appeal were therefore moved to another building, creating more organisational independence.

However, besides the close organisational structures, the UPC faces additional criticism due to fact that the UPC-president Benoît Battistelli is chairman of both boards of appeal and the court which might lead to a critical concentration of power. For example, as chairman or president he has a right to nominate the new president of the boards of appeal, who is therefore dependent on the goodwill of Benoît Battistelli.

Furthermore, Mr. Stjerna complains about the level of costs in respect of the service provided by a lawyer, assessing them as arbitrary. The legal fees would exceed the fees under the German Law on the Remuneration of Lawyers (*Rechtsanwaltsvergütungsgesetz, RVG*) many times over.

III. Opinion of 27 German organisations

In advance of the German Constitutional Court making a final decision, it has invited 27 organisations to comment on the matter by December 2017. Seven institutions and associations responded, including the German government, the EPO, the EPLAW (European Patent Lawyers Association), the DAV (*DeutscherAnwaltVerein*, German Bar Association), BRAK (*Bundesrechtsanwaltskammer*, Federal Bar Association), GRUR (*Deutsche Vereinigung für gewerblichen Rechtsschutz und Urheberrecht*, German Association for the Protection of Intellectual Property) and EPLIT (European Patent Litigators Association). Some of the opinions are publicly available and all of these conclude, in essence, that the complaint should be rejected as inadmissible and/or unfounded.

The BRAK and GRUR opinions go into considerably more detail than those of the DAV, with BRAK concluding the complaint is both inadmissible and unfounded while GRUR does not take a clear line on admissibility but does conclude that the complaint is unfounded (see the statement of Alexander Robinson, at Dehns). The other submissions came from the EPO, EPLAW (European Patent Lawyers Association) and the German Government. The EPO and German Government will not make their views public, while EPLAW has not yet.

However, German associations give new hope that the unitary patent project will still succeed. In particular, for patent owners the unsecure legal situation both in the UK and in Germany leads to more and more frustration.

For IP owners the current legal situation, according to which they need to take legal action in each individual Member State, is both a time and financial burden. In addition, the same case often leads to different court decisions in each Member State. The

implementation of an UPC would lead to relief of court and legal fees and moreover would reduce the work load of the judiciary. With a view to successful systems like the Union Trademark Courts or the Design Rights Courts a similar system for patents would be welcomed.

Conclusion

Although the German Constitutional Court plans to decide the constitutional complaint in 2018, it still remains unclear whether it will follow the recommendation of several German associations to put the UPC system finally into force or if constitutional concerns will prevail. Through the eyes of a constitutionalist, the lack of independence of the boards of appeals might be considered unconstitutional. Furthermore, another delay can occur if the Federal Constitutional Court calls the CJEU for a preliminary ruling. Whatever happens, we will keep you updated.



BARCELONA THE CJEU SHEDS LIGHT ON THE INTERPRETATION OF THE “REPAIR CLAUSE” ESTABLISHED BY ARTICLE 110(1) OF EU REGULATION 6/2002 OF 12 DECEMBER 2001, ON COMMUNITY DESIGNS

On 20 December 2017, the Court of Justice of the European Union (“**CJEU**”) issued a Judgment in cases C-397/16 and C-435/16 regarding the interpretation of Article 110(1) of EU Regulation 6/2002 of 12 December 2001, on Community Designs (“**Regulation 6/2002**”), which establishes the so-called “**repair clause**”: *“Until such time as amendments to this Regulation enter into force on a proposal from the Commission on this subject, **protection as a Community design shall not exist for a design which constitutes a component part of a complex product used within the meaning of Article 19(1) for the purpose of the repair of that complex product so as to restore its original appearance.**”*

Article 19(1) of Regulation 6/2002 identifies the exclusive rights conferred by the Community design, namely to use the design and to prevent third parties from using it without the design holder’s consent. Such “*use*” includes “*in particular, the making, offering, putting on the market, importing, exporting or using of a product in which the design is incorporated or to which it is applied, or stocking such a product for those purposes.*” The repair clause establishes, as an exception, that the protection conferred by a design does not extend to the use of a component part protected by the design merely for repairing a complex product to restore its original appearance. The exception’s purpose, as the CJEU highlights in paragraph 50 of its Judgment of 20 December 2017 (“**Judgment**”), is to avoid creating captive markets for spare parts. If acts covered by the repair clause were to fall within the design holder’s *ius prohibendi*, consumers would be “*indefinitely tied, for the purchase of external parts, to the manufacturer of the complex product*” and competition would be adversely affected.

The issues referred to the CJEU were raised in the context of infringement complaints filed by Pneusgarda Srl and Audi AG (“**Audi**”) in Italy and by Dr. Ing. h.c. F. Porsche AG (“**Porsche**”) in Germany against Acacia Srl (“**Acacia**”). In the second case complaints were also filed against Acacia’s Managing Director. Audi and Porsche alleged that Acacia had infringed their Community design rights by manufacturing and marketing alloy car wheel rims identical to those protected by such designs. Acacia relied on the repair clause to defend itself against the complaints. The complaints were initially upheld in both cases, but the Italian Appellate Court and the German Federal Court of Justice referred the issues regarding the interpretation of the repair clause to the CJEU for a preliminary ruling.

Key Issues:

- According to the CJEU, the repair clause is not restricted to components whose shape is fixed by the shape of the complex product.
- Among the conditions for applying the repair clause set out by the CJEU is the requirement that the replacement part have a visual appearance identical to that of the part originally incorporated into the complex product when it was placed on the market.
- The CJEU concluded that uses of the component part for reasons of “*preference or purely of convenience*” (for example, replacing a part for aesthetic purposes, or customisation of a complex product) are not covered by the repair clause.
- According to the CJEU, manufacturers or sellers of component parts are under a duty of diligence as regards compliance by downstream users with the conditions set out in Article 110(1) of Regulation 6/2002.

The CJEU first analysed whether the repair clause excludes Community design protection for designs constituting a component part of a complex product which is used for the repair of that complex product, so as to restore its original appearance, **subject to the condition that the protected design is dependent upon the appearance of the complex product.** In other words, whether the repair clause only applies to parts whose shape is fixed (parts whose shape is *“immutably determined by the appearance of the complex product and cannot therefore be freely selected by the customer”*, paragraph 30 of the Judgment), as alleged by Audi and Porsche to defend that alloy car wheel rims are not covered by the repair clause.

The CJEU concluded that dependence of the protected design on the appearance of the complex product is not required to apply the repair clause, as supported by (i) a literal interpretation of Article 110(1) of Regulation 6/2002, (ii) the legislative work preceding the adoption of the repair clause (since this condition was omitted from the final version of Article 110(1)), and (iii) the repair clause’s purpose.

Secondly, the CJEU identified the repair clause’s requirements:

- (1) The existence of design rights over a component part (fulfilled in this case);
- (2) The component must be part of a *“complex product”* (fulfilled in this case, insofar as a wheel rim is part of a car, a complex product, and without it such complex product could not be subject to normal use);
- (3) The component must be *“used”* within the meaning of Article 19(1) to *“repair”* the complex product. According to the CJEU, *“use”* covers *“any use of a component part for the purposes of repair”*, and it must be *“necessary for the repair of a complex product that has become **defective**”*. Thus, the use of a component part for reasons of *“preference or purely of convenience”* (such as the customisation of a complex product) is not covered by the repair clause (paragraphs 68 to 70 of the Judgment);
- (4) Repairs must be carried out to restore the complex product’s original appearance. Only components benefitting from protection as a design (and which, according to Article 4(2) a) of Regulation 6/2002, remain visible during normal use of the complex product) are covered by the repair clause.

Furthermore, the component must be used to restore the complex product to its appearance when it was placed on the market. In this regard, the CJEU concluded that the repair clause only applies if the replacement part is **“visually identical”** to the part originally incorporated into the complex product when it was placed on the market, rejecting Acacia’s argument that the repair clause covers all standard variants of original wheel rims (paragraphs 74 to 77 of the Judgment).

Lastly, the CJEU analysed whether, to benefit from the repair clause, manufacturers or sellers of component parts must ensure (and if so, how) that the part *“can be purchased exclusively for repair purposes”* (paragraph 79 of the Judgment).

The Court concluded that manufacturers or sellers of components are not required to guarantee, *“objectively and in all circumstances”*, that the parts they make or sell are,

Notable practitioners

Described as the *best expert in Spain for patent litigation*, **Miquel Montaña** is highly regarded by clients and peers alike for his contentious IP practice. He has long-standing experience of representing clients in the life sciences industry. One client enthuses: *“Miquel is one of a kind: a unique individual with charisma and legal knowledge that always stand out.”*

Newly appointed partner **Josep Montefusco** has a broad-ranging IP practice. He acted for Samsung on trademark protection strategy and copyright work involving the development and launch of several mobile apps. One source says: *“He is really very strong – a great lawyer.”*

ultimately, used by end users in compliance with the repair clause's conditions. However, in order to rely on the clause, manufacturers and sellers must comply with a **"duty of diligence"** as regards compliance by downstream users with the clause's conditions (paragraphs 85 to 88 of the Judgment), particularly by:

- (1) Informing the downstream user that the component part incorporates a design of which they are not the holder, and that the part is intended exclusively for repairing the complex product to restore its original appearance;
- (2) Ensuring through *"appropriate means, in particular contractual means"* that downstream users do not intend to use the components beyond the conditions required to apply the repair clause; and
- (3) Refraining from selling a component part when *"they know or, in the light of all the relevant circumstances, ought reasonably to know"* that the part will not be used in compliance with the repair clause conditions.

In conclusion, in its Judgment of 20 December 2017, the CJEU has provided some necessary clarity on the scope of the repair clause (which has been subject to differing interpretations in the past). The CJEU attempted to strike a balance between broad and strict interpretations. While the Judgment will undoubtedly have a significant impact on manufacturers and sellers of spare parts and complex products, the practical implementation of the criteria it establishes is yet to be seen; for example, as regards the duty of diligence imposed on manufacturers and sellers of component parts.



ACKNOWLEDGEMENT OF CONTRIBUTORS TO THE CURRENT EDITION

We would like to thank the following people for their contributions to this publication:

Ana Benetó	Frédérique Fontaine	Monica Riva
Alice Tang	James Jeffries-Chung	Nicolas Hohn-Hein
Andrea Andolina	Josep Montefusco	Sharman Nigel
Andrea Tuninetti Ferrari	Judith Dany	Sunny Kumar
Anja Schwarz	Laura Rayak	
Daniela Benčová	Ludvík Růžička	

CONTACTS

Australia



Tim Grave
Partner
Sydney
T: +61 28922 8028
E: tim.grave@cliffordchance.com



Sam Luttrell
Partner
Perth
T: +61 892625 564
E: sam.luttrell@cliffordchance.com



Thomas Vinje
Partner
Brussels
T: +32 2 533 5929
E: thomas.vinje@cliffordchance.com



Dieter Paemen
Partner
Brussels
T: +32 2533 5012
E: dieter.paemen@cliffordchance.com

China



Ling Ho
Partner
Hong Kong
T: +852 2826 3479
E: ling.ho@cliffordchance.com



Diego de Lammerville
Partner
Paris
T: +31 1 4405 2448
E: diego.delammerville@cliffordchance.com



Frederique Fontaine
Avocat
Paris
T: +33 1 4405 5490
E: frederique.fontaine@cliffordchance.com



Claudia Milbradt
Partner
Düsseldorf
T: +49 211 4355 5962
E: claudia.milbradt@cliffordchance.com

Italy



Luciano Di Via
Partner
Rome
T: +39 064229 1265
E: luciano.divia@cliffordchance.com



Monica Riva
Counsel
Milan
T: +39 02 8063 4383
E: monica.riva@cliffordchance.com



Krzysztof Hajdamowicz
Counsel
Warsaw
T: +48 22 429 9620
E: krzysztof.hajdamowicz@cliffordchance.com



Torsten Syrbe
Partner
Moscow
T: +7 49 5725 6400
E: torsten.syrbe@cliffordchance.com

Poland

Russia

CONTACTS CONTINUED

Spain



Miquel Montaña
Partner
Barcelona
T: +34 93 344 2223
E: miquel.montana@cliffordchance.com



Josep Montefusco
Partner
Barcelona
T: +34 93 344 2225
E: josep.montefusco@cliffordchance.com



Montserrat López-Bellosta
Of Counsel
Barcelona
T: +34 93 344 2255
E: montserrat.lopez-bellosta@cliffordchance.com



Alvin Khodabaks
Partner
Amsterdam
T: +31 20 711 9374
E: alvin.khodabaks@cliffordchance.com

The Netherlands

United Kingdom



Vanessa Marsland
Partner
London
T: +44 20 7006 4503
E: vanessa.marsland@cliffordchance.com



Stephen Reese
Partner
London
T: +44 20 7006 2810
E: stephen.reese@cliffordchance.com

United States



Daryl Fairbairn
Counsel
New York
T: +1 212 878 4960
E: daryl.fairbairn@cliffordchance.com



Stephen Nickelsburg
Partner
Washington
T: +1 202 912 5108
E: steve.nickelsburg@cliffordchance.com

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

A world map with a light gray background and darker gray landmasses. Thirty black dots are placed on the map to indicate study sites. The dots are distributed across North America (USA and Canada), South America (Brazil), Europe (Western and Central), Africa (North and West), the Middle East, Asia (East and Southeast), and Australia.

São Paulo
Seoul
Shanghai
Singapore
Sydney
Tokyo
Warsaw
Washington, D.C.
Riyadh**

****Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh. Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.**

CLIFFORD CHANCE

This publication does not necessarily deal with every important topic nor cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, Königsallee 59,
40215 Düsseldorf, Germany

© Clifford Chance 2018

Clifford Chance Deutschland LLP is a limited liability partnership with registered office at 10 Upper Bank Street, London E14 5JJ, registered in England and Wales under OC393460. A branch office of the firm is registered in the Partnership Register at Frankfurt am Main Local Court under PR 2189.

Regulatory information pursuant to Sec. 5 TMG and 2, 3 DL-InfoV:
www.cliffordchance.com/deuregulatory

Abu Dhabi • Amsterdam • Bangkok
Barcelona • Beijing • Brussels
Bucharest • Casablanca • Dubai
Düsseldorf • Frankfurt • Hong Kong
Istanbul • London • Luxembourg
Madrid • Milan • Moscow • Munich
New York • Paris • Perth • Prague
Rome • São Paulo • Seoul • Shanghai
Singapore • Sydney • Tokyo • Warsaw
Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.