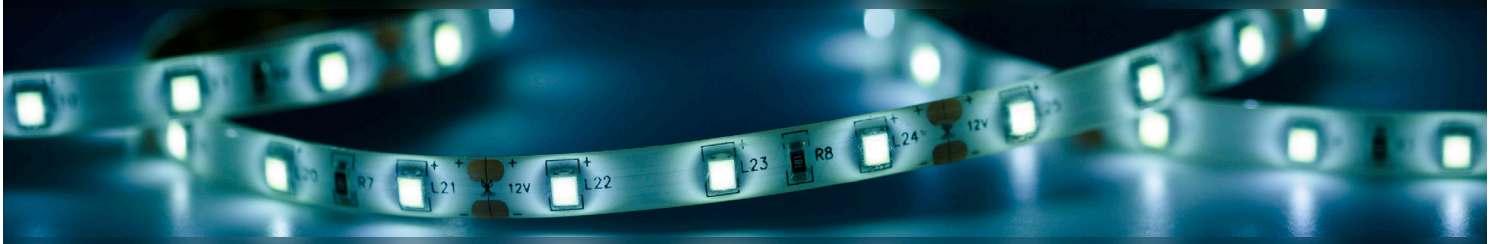
CLIFFORD
CHANCE

23RD EDITION



GLOBAL INTELLECTUAL PROPERTY NEWSLETTER

LEGAL ISSUES SURROUNDING THE PROTECTION OF 'DATA' AND OTHER IP TOPICS

ISSUE 09/19

23RD EDITION

Introduction

Welcome to the 23rd Edition of the Clifford Chance Global IP Newsletter. This newsletter has a focus on legal issues concerning the protection and use of 'Data'.

We start with the question of whether there is a need for an **ownership right to data** regarding its growing importance as an economic asset.

Colleagues from Hong Kong, the UK, Poland and Germany present the **current legal status in each country regarding data ownership**, the **protection of data** as a Trade Secret and the protection of data in individual cases.

The next article looks at **Australia's Notifiable Data Breach Scheme** and current developments in this context, in particular whether it should also be applied with respect to IP rights. The following article covers the guidelines issued by the Italian authorities for Competition, Data Protection and Communications in February 2019 that address certain competition and data protection concerns in relation to **Big Data**. Further, our Italian colleagues will look at the third version of the European Directive on Public Sector Information, which aims to promote the use of **Open Data**, its implementation in Italian law and the role Open Data can play in furthering digital economy. In another article, a new Italian law providing the first legal definitions for **Distributed Ledger Technology and Smart Contracts** is discussed.

Data is also of great relevance for **Smart Products**. In this context, special **liability issues** will be addressed. The same applies in the context of the **Internet of Things**, for which data is indispensable. Therefore, light will be shed on the challenges of developing smart devices for the Internet of Things against the restrictions set out by the **General Data Protection Regulation**.

Data can occur in various forms. In particular, it may also form or be part of trade secrets. For this reason, our German colleagues have dealt with the new **German Trade Secret Act** and the new features that go along with it.

Moreover, we have an article summarizing and examining a **Spanish Royal Decree** implementing an amended system of **fair compensation for copyright holders** with regards to **private copying**.

We hope you enjoy reading this latest issue of the Global IP Newsletter and look forward to receiving your feedback.

Your Global CC IP Team

CONTENTS

GERMANY

Florian Reiling / Fabian Pollex

DATA OWNERSHIP – FUTURE OR DELUSION?

The possible emergence of ownership rights to data is currently the focus of many discussions surrounding the digital economy. As digitalisation progresses, the question of who owns data is becoming more and more important. In this respect, it is worth considering the following questions:

- does ownership of data operate in the same way as ownership of physical objects or other intangible assets?
- is there a need for ownership of data?
- could the ownership of data produce any negative effects?

Key Issues

- Property rights to data do not exist in the current German and EU legal systems.
- Whether or not, in view of the growing economic importance of data, ownership rights should be recognised or should be created by new legal regulations, is currently the subject of intense debate.
- Irrespective of the legal policy concerns, the allocation of data ownership appears to be practically difficult to implement.
- Contractual agreements between parties regarding the rights to use data offer appropriate and practicable solutions.

Economic importance of data

As a result of increasing networking activities (caused, for instance, by the Internet of Things), the amount of data generated is constantly rising. According to a study of the International Data Corporation, the worldwide data volume is expected to grow exponentially from 33 zettabytes (one zettabyte being 10^{21} bytes or 1 trillion gigabytes) in 2018 to 175 zettabytes in 2025. Moreover, by 2025 the share of real-time data as a percentage of overall data volume is expected to rise to 30% from a current share of only 5%. On average, each person is expect to interact with data in some form, whether privately or professionally, every 18 seconds.[1]

Data has become a key asset and one of the top priorities of many companies. In online marketing, entire business models are based on data collection and analysis. It is not surprising then that German Chancellor Angela Merkel describes data as "*the raw material of the 21st century*" and the EU Commission has stated that data should be seen as a valuable production factor and as an economic good.

In view of the growing economic importance of data, whether or not ownership rights should be recognised or created by new legal regulations is currently the subject of intense debate.

Rights to data

The first ideas on the subject of data ownership were first raised decades ago.[2] However, there is still no consensus on how data ownership should operate or whether it should exist at all. Due to data's "intangibility", property rights to data do not exist in

1 See *Reinsel/Gantz/Rydning* (2018), 'Data Age 2025 – The Digitization of the World – From Edge to Core', available under https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf (accessed on 9 August 2019).

2 For example, in the USA, the debate goes back to the 1960s. See *Litman, J.* (2000), Information Privacy/ Information Property, Stanford Law Review, available under http://www-personal.umich.edu/~jdlitman/papers/infoprivacy.pdf (accessed on 9 August 2019).

the current German or EU legal systems. However, it is acknowledged that objects containing information, e.g. hard disks or computer chips, can be subject to ownership rights and their respective owners may assert their rights to these objects. They cannot, however, prevent others from reading, using, reproducing or publishing information on the basis of these property rights once such third parties have gained access to the data, i.e. once they have had a chance to decompile the information from the physical object (provided that the data is not protected by contractual confidentiality obligations or as a trade secret).

Further, among existing intellectual property rights, there is currently no other right which could be utilised to overcome the lack of a right to data. Copyright only protects the creation itself and not the underlying data or ideas. In its entirety, databases can at most be protected as an ancillary copyright in the form of a collection of data in accordance with Section 87a et seq. German Copyright Act ("**UrhG**"). Even the German Trade Secrets Act ("**GeschGehG**"), which came into force in April 2019, does not confer ownership rights to data as such and all such protection is lost if the data becomes publicly available. In the EU General Data Protection Regulation ("**GDPR**"), the legislator has taken comprehensive measures for the protection of *personal data* and has generally prohibited the processing of personal data, as far as no legal permission is available (Article 6 GDPR). However, the regulations of the GDPR do not provide any property rights to data.

Current proposals for data ownership rights

There are different proposals in German legal literature for regulating the ownership of data:

Data-specific approach

Such an approach would involve classifying the ownership of data in accordance with the category of data involved. According to this approach, the type of data would determine whether the data are owned by an individual or by a company. For instance, if data is companyrelated (e.g. machine data etc.) that data would be owned by the company rather than by the individual to which the data relates.

Property law approach

The ownership of data could be classified by how and where the data are stored. This approach provides an element of 'tangibility'. However, as data's main value is in its portability and companies are increasingly turn to cloud systems to store their data, this approach may fail to deal adequately with data as an asset class.

Action-related approach

An alternative approach is to grant data ownership in favour of the producer of the data. This model also produces uncertainty, for instance, would the "producer of the data" be: (i) individuals to which the data relates, (ii) the compiler of the data, or (iii) someone else?

Beneficial owner approach

A study commissioned by the German Federal Government suggests a different approach, which provides for the allocation of data to a "*beneficial owner*". According to this approach, the ownership of data would be determined by considering, among other things, the "*merit*" of data generation, production costs and further costs for the storage of data. However, given the exponential growth in the production or storage of data as detailed above, this approach would likely give rise to many disputes between different parties who have borne costs in relation to the data.

Even though the above-described approaches are being discussed among scholars, there are no concrete current legislative efforts in Germany to introduce a right to data ownership.

Legal-policy considerations

The question of data ownership touches on the relationship between the protection of privacy and informational self-determination on the one hand and freedom of thought, communication, science, economic competition and technological innovation on the other. In order to protect both types of interests, data has so far not been subject to any proprietary right.

Generally, governments grant exclusive property rights as an incentive to invest, and, in return, expect benefits for the general public that result from the resulting technological progress (e.g. fostering technical progress through patented inventions). In this respect, data ownership could create new investment incentives by encouraging the collection and use of data. Further advantages of data ownership could be the better economic allocation of data and a more convenient usability of the data.

However, the "owner" of data is usually not interested in protecting the data as such, but rather seeks for protection of the information which is represented by the data or the knowledge obtained from that information. Exclusivity rights to data could therefore, indirectly, create monopoly positions over information, and this lack of cooperation could intensify the growth and duplicate data collection as parties could not make use of each entities' data.

The collection and control of vast amounts of data is generally accompanied by a fear of the curtailing of freedom of opinion, information and the press. Given that new technologies require a free flow of information, it is arguable that the ownership of data could indirectly lead to a stagnation of technological development.

Irrespective of the legal policy concerns, some argue that the allocation of data ownership appears to be practically difficult to implement. For example, the question arises of how data ownership and the acquisition of data should be demonstrated to third parties and how a transfer of ownership of data affects ownership rights existing with respect to the media/object containing the respective data.

Conclusion

The current legal provisions relating to the trading and transmission of data demonstrate that an allocation of data or a data ownership right may not be required. In fact, for a large share of the problems surrounding the allocation of data, a solution is already available: contractual agreements.

Contractual agreements between parties regarding the rights to use data – in most cases – offer more practical and relevant solutions. They can be designed flexibly and are thus suitable for a wide range of commercial needs. Accordingly, and due to the fact that the legislative discussion regarding data ownership is currently on hold, the real challenge lies in creative contract drafting.

Therefore, when data is involved it is absolutely essential to enter into discussions and draft contracts covering: how data is made available, for what purpose the data may be used, how such use is remunerated, how accumulated data is to be treated and also when data must be deleted. All these aspects are key for successful data-related contract drafting and require communication to ensure contractual provisions work legally and commercially.

DÜSSELDORF, HONG KONG, LONDON, WARSAW

Florian Reiling / Julian Scheerbaum / Ling Ho / Nicola Kung / Jonathan Coote / Katarzyna Kuchta

PROTECTION OF DATA – AN OVERVIEW INCLUDING CHINA, GERMANY, UK AND POLAND

With the already enormous amounts of data growing every second across the globe, its unique character, its omnipresence in our everyday lives and increasing commercial value requires lawmakers to keep pace with technological development and provide appropriate legal frameworks. However, while data tend to be treated more and more like any other asset, they do not fit easily into the traditional legal notion of "*tangible goods*".

While the idea of (positive and negative) ownership in the sense of free and exclusive use is generally applicable to data, other traditional concepts such as physical transfer, assignment and permanent destruction are substantially different due to data's non-physical, sometimes transient, nature. Not only can data be easily stored, copied and reproduced without considerable costs, but they may also be used in many different ways by different people at the same time.

This article aims to compare different jurisdictional approaches to the protection of data across China and Europe, particularly focusing on:

- ownership of data;
- database protection;
- protection of data as trade secrets;
- protection of data in specific cases such as AI and blockchain; and
- related case law.

Key Issues

- The unique character of data requires the adjustment of legal frameworks.
- Despite the lack of statutory provisions on data ownership throughout the compared jurisdictions, initial progress has been made in the adjustment process. For example, EU law grants a *sui generis* right to authors of databases while protection in China can only be achieved by fulfilling specific Copyright / Cybersecurity Law provisions. Further, in the EU, the implementation of the Know-How-Directive gradually provides for a harmonised protection of data as trade secrets, whereas China is lacking independent trade secret legislation.
- However, it is still a long way to go until practicable solutions to all legal problems caused by the technological development will be found.

Local legal considerations

a) Germany

Data Ownership	Protection of Databases	Protection of Data as a Trade Secret	Protection of Data in individual cases (e.g. AI, blockchain etc.)
Neither data ownership nor any other absolute rights on data currently exist within the German legal system. The current legislation only contains criminal law provisions, property regulations in respect of the data carriers and copyright law concerning the content of data. The German Federal Government has advocated/ proposed an approach that provides for the allocation of data to its beneficial owner. Currently, legislative efforts are put on hold, but different approaches are being discussed, including: (i) a data-specific approach (classifying of ownership in accordance with the category of data involved), (ii) a property law approach (ownership right depending on who owns the data carrier, e.g. the hard disk), (iii) an action-related approach (granting ownership in favour of the data producer), and (iv) the aforementioned governmental approach providing for the allocation of data to its beneficial owner.	The EU directive on the Protection of Databases (96/9/EC) has been, *inter alia*, implemented into the German Copyright Law ("**UrhG**") in 1998. Section 87a et seq. UrhG grants an exclusive *sui generis* right to the authors of databases.	In April 2019, the German Law for the Protection of Trade Secrets ("**GeschGehG**") implementing the EU Know-How-Directive (2016/943) entered into force. Following EU law, information is subject to protection only when it is: (i) *"neither in its entirety nor in the exact arrangement and composition of its components generally known or readily accessible to persons in the circles that normally handle this type of information and therefore be of economic value";* and (ii) *"subject to appropriate secrecy measures by its lawful owner"*. Unlike Union law, the information must additionally be (iii) *"subject to a legitimate interest in secrecy"*.	Smart products such as autonomous cars can collect large amounts of data, e.g. machine data, user behavior and user interests. Since data, as such, are not protected under German Law, companies must seek other ways to gain control of data. This can be achieved by first securing access to data through detailed contractual agreements and then implementing effective access control through encryption and assignment of permission rights.

b) China (PRC)

Data Ownership	Protection of Databases	Protection of Data as a Trade Secret	Protection of Data in individual cases (e.g. AI, blockchain etc.)
PRC law does not explicitly recognise the concept of data ownership but recent case law indicates the courts' recognition of property rights in data. In the case of personal data, network operators (defined to include all owners and administrators of networks, as well as network providers) must obtain individuals' informed consent before collecting their data. Individuals may make correction requests when they are aware of any errors in their information held by a network operator. The Cybersecurity Law and its implementing regulations present a state-centric approach to data protection. All network operators are required to accept supervision by the government. The latest draft of the Measures for Security Assessment of Cross-border Transfer of Personal Data[1] includes a data localisation requirement applying to all network operators. If it comes into force, the approval of the Cyberspace Administration of China will be needed for any personal data transfer out of China.	While there is no *sui generis* protection of databases, electronically stored databases are protected under the Cybersecurity Law. The Cybersecurity Law places obligations on all network operators to protect network data. The term "network data" is defined to include "*all kinds of electronic data collected, stored, transmitted, processed and generated through the network*" and is broad enough to capture databases held electronically. Network operators are required to prevent unauthorised access, theft and damage to data (e.g. by implementing internal security management procedures).	Data may be protected as a trade secret under the Anti Unfair Competition Law if it is: (i) *unknown to the public*; (ii) *commercially valuable*; and (iii) *subject to confidentially measures* (e.g. confidentiality agreements, any internal/external confidentiality procedures). If the data qualifies as a trade secret, any recipient of the data will be under a statutory duty to keep the information confidential, whether or not they have entered into a confidentiality agreement. The Anti Unfair Competition Law prohibits the acquisition of trade secrets by theft or other improper means, as well as the disclosure of trade secrets in breach of obligations of confidentiality. Penalties for non-compliance include administrative orders to cease the infringing activity, confiscation of illegal gains, and fines of RMB 10,000 to 5 million.	Huge amounts of data are collected by China's internet giants through multi-purpose "super-apps" such as WeChat. WeChat has over a billion users and a wide range of functions including instant messaging, e-payment, flight booking, taxi hailing, and financial investment. Data from these apps feeds into social credit systems operated by the same companies which rate citizens based on their behavior and trustworthiness. These large volumes of data are much coveted by mobile device makers as well as social media companies. Data protection requirements are set out in the Cybersecurity Law and numerous subsidiary guidelines and measures. These include requirements to formulate internal security management systems, to adopt technical measures to prevent cyberattacks, and to back up and encrypt data. Companies can protect the data they hold by communicating clear privacy policies setting out how the data will be used and who it can be transferred to.

1 PRC Security Assessment Measures (Cross-Border Data Transfer) 个人信息出境安全评估办法 issued on 13 June 2019.

c) Hong Kong

Data Ownership	Protection of Databases	Protection of Data as a Trade Secret	Protection of Data in individual cases (e.g. AI, blockchain etc.)
There is no statutory concept of data ownership. Traditional concepts of IP rights are difficult to apply to ownership rights in data. As far as personal data is concerned, under the Personal Data Protection Ordinance (Cap 486), a data user must obtain an individual's consent to collect or process their personal data. Individuals also have a right to verify whether a data user holds any of their personal data, request access to that data and request corrections to be made. For the time being, the more realistic means of protection are contractually addressing issues of data ownership and concepts such as confidentiality.	Hong Kong law does not recognise a *sui generis* database right. If the database content meets the requirements for copyright protection, then it will be protected under the Copyright Ordinance (Cap 528). Copyright protection applies to the compilation, arrangement or selection of the content which is the result of a creative human effort; however, protection only applies to the database's structure, expression and not its content. The database must be sufficiently original for copyright to subsist. The manner of compilation and any original matter added as part of the compilation must be analysed in determining whether the standard of originality is met, but generally computer generated databases or simple databases do not qualify for copyright protection.	There is no statutory protection of trade secrets in Hong Kong, but it is possible for confidential data to be protected under the common law and equitable actions for breach of confidence. Three preconditions must be satisfied for an action in breach of confidence to succeed: (i) *the information itself must be confidential in nature*; (ii) *the information must have been imparted under circumstances importing an obligation of confidence*; and (iii) *there must have been an unauthorised use of that information to the detriment of the party communicating it*. A duty of confidence can also be imposed and regulated under contract.	In March 2019 the Privacy Commissioner issued specific guidance for data protection in fintech. It highlighted privacy risks such as the collection and use of large amounts of personal data without a user's notice, and the risks of data leakage or interception during transmission. It recommends taking both administrative measures (e.g. implementing policies and procedures) and technical security measures (e.g. encryption and safe erasure methods) to protect data. The recently published Guide to Data Protection by Design for ICT Systems promotes good practices such as data encryption, access control and conducting penetration testing.

d) Poland

Data Ownership	Protection of Databases	Protection of Data as a Trade Secret	Protection of Data in individual cases (e.g. AI, blockchain etc.)
In Poland there is no specific regulation on data ownership.	Databases are protected under the Databases Protection Act of 27 July 2001 implementing EU Directive 96/9/EC on the legal protection of databases. A database is a set of data or any other materials which: (i) *has been collected in accordance with a particular system or method*; (ii) *is individually available in any way, including electronic means*; (iii) *required an important (in quality or quantity) investment effort to prepare, verify or present its content*. Database producers have an exclusive and transferable right to download and re-utilise data in whole or in substantial part (qualitatively or quantitatively). Databases are protected for 15 years following the year of their creation. Additionally, databases can be protected under the Act on Copyright and Related Rights dated 4 February 1994 if they are of individual creative nature. In such case, the databases enjoy protection as a "work" which, in general, lasts for 70 years following the year of the author's death.	In Poland, there are no specific regulations regarding the protection of data as a trade secret and therefore the general rules on trade secrets (the Act on Combatting Unfair Competition dated 16 April 1993) apply. Data can constitute a trade secret if: (i) *it is technical, technological, organisational information of an enterprise or other information of economic value;* (ii) *it is confidential* (i.e. it cannot be commonly known to, or easily accessible by, those who usually deal with this type of information, unless a party authorised to use the information took actions to keep them confidential). Obtaining, use or disclosure of trade secrets in an unlawful way is an act of unfair competition. Nonetheless, violation of trade secret law which causes serious damage can be a criminal offence.	Currently, in Poland there is no specific regulation regarding protection of data (such as AI or blockchain).

e) UK

Data Ownership	Protection of Databases	Protection of Data as a Trade Secret	Protection of Data in individual cases (e.g. AI, blockchain etc.)
Under English law, there is no property right in data per se because it cannot be stolen (*Oxford v Moss [1978] 68 CR App Rep 183)*. As data are not tangible property, it cannot be the subject of a common law lien (*Your Response Ltd v Datateam Business Media Ltd [2014] EWCA Civ 281*).	The EU Directive on the Protection of Databases (96/9/EC) was implemented into the Copyright, Designs and Patents Act 1988 (the "**CDPA**") in 1998 by the Copyright and Rights in Databases Regulations 1997 (SI 1997/3032) (the "**Database Regulations**") which created the EU *sui generis* Database Right. Databases (and even individual datasets) may also be protected under copyright law as "*literary works*" if they are "*original*" (the "*author's own intellectual creation*" (*Infopaq International A/S v Danske Dagblades Forening C-5/08*)). **Post-Brexit** *Under the Withdrawal Agreement* holders of *sui generis* EU Database Rights before Exit Day will be granted an equivalent UK right, with the same level of protection as their existing EU right (Article 58 of the Withdrawal Agreement). **No-Deal** The UK would continue protection for the *sui generis* Database Rights of EU makers on Exit Day.	In June 2018, the Trade Secrets (Enforcement, etc.) Regulations 2018 (SI 2016/943) (the "**Trade Secrets Regulations**") implementing the EU Know-How Directive came into force. The EU Know-How Directive is similar to and may be used "*in addition to, or as an alternative, to*" the pre-existing Law of Confidence under English Common Law. Under Common Law, the three-stage test of confidentiality is: (i) *information must have the necessary quality of confidence* (i.e. it must involve some effort/human capital and must not be public property or knowledge); *(ii) information must be disclosed in circumstances importing an obligation of confidence (*e.g. through a Confidentiality Agreement, an employer-employee relationship, a notice of confidentiality, encryption, or, more broadly, a "*reasonable appreciation of confidentiality*"); and	There are no English laws that deal specifically with the ownership of data as an asset class generally or in individual applications such as AI, smart products or blockchain. *Rights in AI-Generated Databases/Datasets* This is a complex and largely untested area of law. Under copyright law, individual datasets or records, as well as a database as a whole, may be protected as a "literary work", provided that it meets the originality test (i.e. be the "*author's own intellectual creation*"). English copyright law also allows for the protection of works that are "*generated by a computer … such that there is no human author of the work*" (s. 178 CDPA). The compatibility of this section with European case law concerning authorship of copyright works has however been questioned by academics.

Data Ownership	Protection of Databases	Protection of Data as a Trade Secret	Protection of Data in individual cases (e.g. AI, blockchain etc.)
	However, UK legislation would be amended so that only UK makers in the UK will get future protection and UK makers will lose protection in the EU (Reg. 28 of the Intellectual Property (Copyright and Related Rights) (Amendment) (EU Exit) Regulations 2018 (SI 2019/605)).	*(iii) there must be unauthorised use.* The rights conveyed by the English Common law of confidentiality are similar to those introduced by the EU Know-How Directive, which was brought in to bring the whole of the EU in line with a standard level of protection. Differences from pre-existing Common Law under the Trade Secrets Regulations include: (a) the requirement for the owner to take "*reasonable steps*" to keep the information secret – arguably under English Common Law the focus is on the confidentiality of the information and how it is shared ("*disclosed in circumstances importing an obligation of confidence*") rather than how it is protected. The extent to which this constitutes a material difference remains to be seen; and (b) the requirement that the information "*has commercial value because it is secret*" – however, under English Common Law the "*commercial value*" of information has already been considered in case law (see *Douglas v Hello! Ltd [2007] UKHL 21* or, more recently, *Racing Partnership Ltd v Done Brothers (Cash Betting) Ltd [2019] EWHC 1156 (Ch)*).	

Data Ownership	Protection of Databases	Protection of Data as a Trade Secret	Protection of Data in individual cases (e.g. AI, blockchain etc.)
		Therefore, the extent to which these two coexistent rights diverge is subtle and over time will depend on the interpretation of these standards by the English courts, particularly in light of Brexit. **Post-Brexit** The Trade Secrets Regulations will be retained in UK law and so will be unaffected by Brexit. However, the English courts would be under no obligation to conform their interpretation (e.g. of "*reasonable steps*" and "*commercial value*") with the CJEU.	

Conclusion

Legislative efforts reflecting the unique character of data are underway.

However, the above comparison indicates that the current legal provisions do not grant sufficient protection of data, especially considering that legislative efforts concerning data ownership in Germany are currently put on hold.

Therefore, in light of the above-highlighted deficits in legislative protection, it is essential for companies to focus on contractual drafting to adequately protect their data. In particular, companies should carefully draft licence agreements and confidentiality clauses to ensure that they can protect their data using flexible and commercial solutions.

SYDNEY

Tim Grave / Jack Oakley / Joshua Malek

"BREACHER BEWARE": MANDATORY NOTIFICATION OF DATA BREACHES — A CAUTIONARY TALE FOR IP REPOSITORIES

In late 2018, the Australian National University ("**ANU**") fell victim to cyberattacks, which were only discovered in late May 2019 amidst fears that unpublished academic material was stolen and put up for sale on the dark web. This incident follows a similar cyberattack in 2018 by hackers tied to the Iranian government, who targeted over 76 universities across 14 countries with the aim of stealing intellectual property. Clearly, the valuable nature of intellectual property inherently increases its exposure to threats of cyber theft. Against this backdrop, this article will highlight the importance of securing intellectual property data in light of Australia's Notifiable Data Breaches Scheme ("**NDBS**").

With the evolving nature of data itself, the Australian Parliament has recognised the clear need for regulation and legislation to keep pace with technological advancements. Accordingly, this article posits that there could soon be an expansion of the NDBS beyond "personal information",[1] in order to ensure the protection of intellectual property held by third parties, non-compliance with which could have serious financial and reputational consequences for entities storing IP data on an owner's behalf.

Key Issues

- In May 2019, the Australian National University (**ANU**) notified students, staff and alumni of a cyberattack involving 19 years' worth of personal data, which included unpublished academic works feared to have been put up for sale on the dark web. This incident follows a similar cyberattack in 2018 by hackers tied to the Iranian government, who targeted over 76 universities across 14 other countries with the aim of stealing intellectual property.
- Australia's Notifiable Data Breach Scheme is evolving and may soon intersect with the field of intellectual property (or, in certain respects, may already).
- Corporates, government agencies and NGOs that hold sensitive intellectual property on online databases should be wary of the threat of cyberattacks (coupled with the consequent litigation risk) and take whatever steps necessary to limit their exposure.

The increasing prevalence of data breaches

The proliferation of data has increased exponentially, as has data's relevance to commercial transactions and the consequent potential for disputes to arise in the realm of trade and commerce.[2] Couple this with the fact that recent studies have suggested

1 Defined in sec. 6 of the Privacy Act 1988 (Cth) as "*information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not*", which is technologically neutral to ensure sufficient flexibility to encompass changes in information-handling practices over time, consistent with international standards and precedents (see also Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 at 53.

Comparatively, the definition of "personal data" EU's Global Data Protection Regulation of 2016 ("**GDPR**") has been interpreted broadly by the European Commission as extending to include anything from a name, home address or an email address.

2 See, e.g. *Shahin v BP Australia* [2019] SASC 12, where the Supreme Court of South Australia closely scrutinised a contractual provision concerning transfer of customer data, in light of the franchisor's reliance on its privacy law obligations to refuse to comply with the relevant clause.

breaches of data security have increased in frequency and scope,[3] and the associated risks for data repositories quickly begin to materialise. While these data breaches have primarily involved "personal information" (see, e.g. the case studies of Westpac, Telstra, and the Red Cross Blood Service),[4] the increased storage of intellectual property on online databases increases its exposure to cyber theft. Alarmingly, as hackers are becoming increasingly sophisticated, data repositories are reportedly finding it increasingly difficult to detect when they've been hacked.[5]

As a further recent example, consider the financial and reputational impact of the recent data breach at British Airways – which exposed 500,000 customers to the threat of financial fraud because credit card information had been stolen for illicit purposes – resulting in the company being fined £183 million (equating to approximately 1.5% of its annual turnover for FY2017).[6] Consider too the fact that Verizon Communications' purchase price of Yahoo! Inc. in 2016 was slashed during negotiations by US$350 million as a result of data breach liability being uncovered in the due diligence process (with Yahoo! Inc also agreeing to pay 50 per cent of costs in respect of related private litigation).[7]

As a corollary to the above matters, cyber security must similarly be 'ramped up' by corporates and data repositories to ensure protection of information stored online, lest they suffer the consequences of financial and reputational damage, particularly if data breach liability extends into the highly valuable IP space (discussed below).

3 Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) at 19 (referring to a 2014 report commissioned by Telstra and a 2016 report commissioned by PwC).

4 Westpac: Almost 100,000 customers exposed to cyberattacks from a PayID payment platform, whereby mobile numbers or email addresses could confirm the name of the corresponding account holder, potentially leading to commission of fraud on mass scale – see Ben Grubb and Clancy Yeates, 'Almost 100,000 Australians' private details exposed in attack on Westpac's PayID', *The Sydney Morning Herald* (online), 3 June 2019 <https://www.smh.com.au/business/banking-and-finance/australians-private-details-exposed-in-attack-on-westpac-s-payid-20190603-p51u2u.html>.

Telstra: 15,775 Telstra customers were affected by breaches that made names, telephone numbers and home and business addresses accessible through a global Google search—see Commonwealth, Parliamentary Debates, Senate, 13 February 2017, 595 (Lisa Singh).

Red Cross Blood Service: 550,000 donors' personal information registered between 2010 and 2016 was accessed by an unauthorised person, including names, addresses, dates of birth and personal details provided in response to a questionnaire – see Australian Red Cross Blood Service, *Blood Service Apologises for Donor Data Leak* (28 October 2016) <https://www.donateblood.com.au/media/news/blood-service-apologises-donor-data-leak>.

5 Sam Duncan, 'Australian National University hackers shine light on IP theft', *The Australian* (online), 11 June 2019 <https://www.theaustralian.com.au/business/technology/uni-hackers-shine-light-on-ip-theft/news-story/4117c5b4d02e4c75dfb4d99703c02741>.

6 Rory Cellan-Jones, 'British Airways faces record £183 million fine for data breach', *BBC News* (online), 8 July 2019 <https://www.bbc.com/news/business-48905907>.

7 Megan Gordon, Daniel Silver, Bernjamin Berringer and Brian Yin, 'Cyber and Data Privacy Due Diligence' in Benjamin A Powell, Leah Schloss, Maury Riggan and Jason C Chipman (eds) *Global Investigations Review: The Guide to Cyber Investigations* (2019).

IP and Australia's NDBS

Australia's NDBS was implemented in February 2018[8] and applies to all organisations which are required to comply with the *Privacy Act 1988* (Cth). It put in place a mandatory notification scheme vis-à-vis unauthorised access to "personal information" held by that organisation, to the extent that access results in serious harm to the individuals to whom the information relates. Since the NDBS was introduced, notification of data breaches in Australia has increased by 712%.[9] Given the effectiveness of the NDBS to date, coupled with the increased prevalence and scope of cyberattacks discussed above, it is foreseeable that mandatory reporting of data breaches could extend beyond "personal information" and into the realm of IP.

In this connection, the Australian Government has recently announced plans to reform Australia's privacy laws,[10] including increased penalties for privacy breaches, and additional enforcement powers for the Office of the Australian Information Commissioner ("**OAIC**"). Senator Penny Wong[11] has previously spoken of the Australian peoples' concerns about privacy in the digital age, and their placing of faith in the Australian Parliament to respond in the appropriate way to data breaches. Relatedly, Senator Catryna Bilyk[12] has credited the NDBS as being critical to understanding the gravity and magnitude of data breaches. It is therefore conceivable that the media scrutiny attending the ANU data breach might trigger public expectations vis-à-vis mandatory reporting of data breaches at large (i.e. not merely breaches specific to "personal information"). Indeed, widening of the existing scheme has already been contemplated in Australian public discourse.[13]

Whilst it is fair to say that theft of "personal information" still garners the most media and parliamentary attention, IP theft is emerging as a risk weighing on corporate decision makers' minds. A recent study commissioned by software developer Bromium revealed that theft of trade secrets and intellectual property accounted for $500 billion dollars globally – a third of the overall revenue generated by cybercrime.[14] Similarly, renowned security software developer McAfee released a report in April 2019 which expressed the view that cyberterrorists are as equally focused on intellectual property theft as they are on personal information.[15]

8 *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) s 2.

9 Angelene Falk, *Notifiable Data Breaches Scheme 12-month Insights Report*, Office of the Australian Information Commissioner <https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics/ndb-scheme-12%E2%80%91month-insights-report.pdf>.

10 Christian Porter (Attorney-General) and Mitch Fifield (Minister for Communications and Minister for the Arts), 'Tougher penalties to keep Australians safe online' (Joint Media Release, 25 March 2019) <https://www.minister.communications.gov.au/minister/mitch-fifield/news/tougher-penalties-keep-australians-safe-online>.

11 Commonwealth, *Parliamentary Debates*, Senate, 13 February 2017, 582-585 (Penny Wong).

12 Commonwealth, *Parliamentary Debates*, Senate, 13 February 2017, 588-592 (Catryna Bilyk).

13 For example, the Australian Information Security Association ("**AISA**") has recommended the current NDBS should be part of a broader and 'more responsive' regulatory approach to supporting information security, whilst the ACCC Digital Platforms Inquiry recommended (in a preliminary report dated December 2018) that a statutory cause of action for serious invasions of privacy should be introduced to increase the accountability of businesses over control of personal information.

14 Dr Michael McGuire, *Into the Web of Profit: Understanding the Growth of the Cybercrime Economy* (2018) <https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf>.

15 McAfee, Grand Theft Data II: The Drivers and Shifting State of Data Breaches <https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-data-exfiltration-2.pdf>.

Even ignoring the prospect of legislative reform, it is likely that, in many cases, intellectual property already incorporates a degree of "personal information". For example, a patent lawyer will often need to collect personal data of the inventors for the purposes of their patent application.[16] Accordingly, the current NDBS regime may already be triggered by IP cyber theft if it can be determined that personal data was obtained as a result. In support of this proposition, consider *Privacy Commissioner v Telstra Corporation Ltd [2017*] FCAFC 4, where Kenny and Edelman JJ reasoned that information "about an individual" merely requires that the individual be the subject matter of the information. Accordingly, data that includes information such as names of individuals, could fall within the operation of the *Privacy Act*,[17] with the consequence that intellectual property such as the stolen unpublished academic works held in the ANU case may well be subject to the existing NDBS if the works include the author's name(s). Having said that, academic commentary posits that Australian case law on this issue remains unclear (at least when compared to international counterparts),[18] with the consequence that legislative intervention may be required to fill any voids created by judicial interpretation.

Potential consequences and practical implications

Irrespective of whether the NDBS extends to the IP sphere or not, data repositories must take practical steps to minimise the threat of cyber theft. This includes a streamlined approach to handling all data (including intellectual property data) and the introduction of compliance programmes and employee training. Companies must also develop action plans to ensure an orderly and appropriate response to a breach, in order to minimise any damage that may result. Those responses (and the timeliness of them) will be scrutinised by regulatory bodies and will likely be wholly determinative of any decision to commence enforcement action. When combined with the significant and persistent threat of collateral or standalone class actions (as a means of private regulation), the risks for data repositories are too great to ignore.

Accordingly, irrespective of the onerousness of the applicable obligations, a stringent approach is recommended (including when considering appropriate levels of insurance coverage, given the valuable nature of most IP) to ensure compliance and transparency. At a minimum, data repositories should ensure they follow the OAIC's basic four-step guide to responding to data breaches:

(i) contain the data breach to prevent any further compromise of information.

(ii) assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.

(iii) notify the data breach to the individuals concerned and the OAIC.

(iv) review the incident and consider what actions can be taken to prevent future breaches.

16 Patrick Wheeler and Mette Marie Kennedy, 'Practical Tips on GDPR for Intellectual Property Attorneys' (2019) 11(3) Landslide 50.

17 Gabriella Shailer, 'Limitations of personal information in an online environment' (2018) 43(4) Alternative Law Journal 309 at 310.

18 Norman Witzleb, '"Personal Information" under the Privacy Act 1988 (Cth) – Privacy Commissioner v Telstra Corporation Ltd [2017] FCAFC 4' (2017) 45 Australian Business Law Review 188 at 188.

ITALY

Luciano Di Via / Francesca Zambuco

BIG DATA AND INSTITUTIONAL COOPERATION: ANTITRUST, CONSUMER PROTECTION AND PRIVACY ENFORCEMENT

On 10 July 2019, the Italian Competition Authority ("**ICA**"), the Italian Data Protection Authority ("**DPA**") and the Italian Authority for Communications ("**IAC**", jointly with the ICA and the DPA the "**Authorities**") adopted, following a fact-finding inquiry started in 2017, the '*Guidelines and Policy Recommendations on Big Data*' (the "**Guidelines**").

The Authorities' analysis starts from the premise that Big Data is increasingly important in the current economic and social context and its development has huge and undeniable advantages for both market players and consumers. However, in the view of the Authorities, when undertakings with such large quantities also enjoy significant market power, concerns may arise in the areas of fundamental rights, competition and pluralism.

Therefore, the Authorities implemented 11 **policy points and recommendations** analysing (i) data acquisition, (ii) data utilisation, and (iii) the Authorities' power and mutual cooperation.

Data acquisition

The Guidelines state that a fundamental goal of Big Data policies should be the **reduction of the information asymmetry between users and digital operators** both from a data protection and competition standpoint. The fact-finding inquiry has clearly demonstrated that there is an inverse relationship between the purchase price of an app and the consent required from the users (i.e. the lower the price the higher the consent required). In particular, at the time data are collected, users must be informed about the possibility of being recognised as individuals, including from anonymised data, and about the right to data portability among platforms (pursuant to Article 20 of the General Data Protection Regulation).

With regard to competition, undertakings holding large quantities of data may be obliged to give their competitors access to indispensable and non-replicable data. The Guidelines suggest reducing the information asymmetry **between large digital platforms and other operators that make use of them**, for instance by designing more transparent rankings for the positioning and the visibility on the platforms.

Key Issues

- The Guidelines identify a fundamental goal of Big Data policy: the reduction of the information asymmetry between users and digital operators and between large platforms and other operators using the platform.
- The Authorities suggest that merger rules can assume a pivotal role in catching so-called "*killer acquisitions*" (acquisitions by large tech companies of tech start-ups, which stifle growth and innovation) and thus represent a first method for tackling possible concerns, along with consumer protection provisions.
- The Guidelines provide a number of proposals for national and international cooperation to ensure the effective safeguarding of privacy, competition, consumer protection and pluralism regarding Big Data.

Data utilisation

From the **consumer's perspective**, the Authorities underscored that operators managing Big Data should ascertain if **data** are of a **personal nature** and, if so, they should use them according to **stricter standards**. The ultimate aim should be to safeguard consumers' welfare and their ability to have access to information, in particular online information, that is fair, complete, verifiable and non-discriminatory.

From the **undertakings' perspective**, the Authorities highlighted that the use made of Big Data by undertakings, and online operators, in particular, has crucial consequences on competition dynamics in online markets. Currently, antitrust and consumer protection provisions are limited in their ability to tackle issues connected to Big Data. However, they are still the first methods used to manage possible concerns. For instance, the Guidelines consider that algorithms may become a vehicle to implement collusion among undertakings, and that **merger rules** should assume a new **pivotal role in catching** transactions that may appear *prime facie* irrelevant (as the turnover thresholds are not met), but are in fact "**killer acquisitions**" by large tech companies of innovative start-up companies.

Powers of the authorities and cooperation

Finally, the Guidelines provide a number of proposals in relation to **international cooperation** between authorities, as well as specific considerations for **national cooperation**. At the European level, cooperation among competition authorities should be undertaken in the context of the European Competition Network. At a global level, the Organisation for Economic Co-operation and Development, the International Competition Network and the UN Conference on Trade and Development should be used. The Guidelines also highlight, from a consumer protection standpoint, the importance of strengthening the information exchange between the different Authorities within Italy, with a view to both protecting consumers' privacy and promoting competition. The Authorities should also implement effective advocacy activities aimed at preventing and resolving concerns relating to **privacy**, **competition**, **consumer protection** and **pluralism**.

Conclusions

The Guidelines confirm the attention that Italian national authorities are paying to Big Data from different perspectives. In this context, it will be important to analyse the final report of the fact-finding inquiry carried out by the Authorities and to monitor the enforcement trends not only in Italy, where effective implementation is expected, but also in other jurisdictions.

ITALY

Andrea Andolina / Andrea Tuninetti Ferrari

OPEN DATA GAINS MOMENTUM IN ITALY (AND THE EUROPEAN UNION)

Since the beginning of the millennium there has been great attention across Europe around data and information deriving from public bodies. When data serves as a *raw material* to be re-used by private (and commercial) players for the supply of new goods and the provision of new services, this is referred to as Public Sector Information ("**PSI**"). This is defined as "*information collected, produced, reproduced and disseminated within the exercise of a public task or a service of general interest*".

Efforts at the European level have been devoted primarily to making PSI accessible to everyone with a legitimate interest. (Notably, commercial use *does* qualify as a legitimate interest.) The goal initially was, and still is, to increase the amount of Open Data available to the public by (i) promoting "*data in an open format that can be freely used, re-used and shared by anyone for any purpose*" and (ii) adopting polices which "*encourage the wide availability and re-use of public sector information for private or commercial purposes, with minimal or no legal, technical or financial constraints and promote the circulation of information not only for economic operators but primarily for the public*".

All of the previous quotes are from the most recent PSI Directive (the Open Data Directive ((EU) 2019/1024), adopted on 20 June 2019 which recasts the previous directives on PSI. Member States have until 17 July 2021 to implement the directive.

The Public Sector Information Directives

Directive (EC) 2003/98 ("**Dir. PSI I**") was the first legislative instrument adopted at the European level to establish a set of minimum rules governing the re-use and the practical arrangements for facilitating re-use of existing documents held by public sector bodies. The Dir. PSI I harmonised some fundamental principles (such as "***re-use for commercial or non-commercial purposes***" and "***transparency***") and definitions (such as what constitutes a "*document*"). This has encouraged the adoption of **standard licenses** on non-discriminatory bases for everyone requesting access to PSI.

Dir. PSI I was then amended by the Directive (EU) 2013/37 ("**Dir. PSI II**"), which widened the existing scope by including data and information gathered from museums, libraries and archives. Dir. PSI II also encouraged translation, to the extent possible, of the information in machine-readable format. In addition, the directive stated that as a key principle: Access and re-use of PSI is to all effects a right and therefore is not something which should be left to the discretion of the public entities holding the requested PSI. While Member States were free to set the conditions to give access to PSI (provided that these were transparent), the ability to charge compensation for the access was limited to only covering **marginal costs**.

Key Issues

- On 20 June 2019 the European Union adopted Directive (EU) 2019/1024 on access and re-use of Public Sector Information (the Dir. PSI III).
- The Dir. PSI III recasts the Dir. (EC) 2003/98, already revised by the Dir. (EU) 2013/37.
- Member States have until 17 July 2021 to transpose the Dir. PSI III.
- Italy was noted by the EU Commission in 2009 for incomplete transposition of the Dir. PSI I. However, it is now among the leading countries in promoting Open Data.
- In 2018, Italy was ranked in 4th place in Europe for Open Data Maturity and has been awarded a designation as a leading "trendsetter" in Europe for Open Data.

The 'Open Data' Directive (Directive (EU) 2019/1024) ("**Dir. PSI III**") relies upon the fundamental principle that over the past few years, "*the amount of data in the world, including public data, has increased exponentially and new types of data are being generated and collected. In parallel, there is a continuous evolution in technologies for analysis, exploitation and processing of data*". For that reason the Dir. PSI III extends the scope of the PSI Directives even to:

(i) **public undertakings** acting as public service operators (e.g. water supply, energy, transportation, mail services etc.), which can provide very valuable and strategic datasets;

(ii) **research data** deriving from publicly funded project or entities;

(iii) **dynamic data**, i.e. data generated by sensors and any other data subject to frequent or real-time updates characterised by their volatility and rapid obsolescence. Dynamic data should be made available for re-use immediately after collection by Application Programme Interfaces (APIs) or bulk download.

The transposition of the PSI Directives in Italy and Open Data

Initially, Italy was flagged by the European Commission for having incorrectly and only partially implemented Dir. PSI I. However, in recent years Italy has committed itself to fostering Open Data awareness and has become a leading jurisdiction in promoting Open Data.

Many efforts have been addressed in digitalising public sector bodies and setting the legal conditions to ensure effective open access to PSI. As a result, there are now numerous available datasets which have reached impressive size and the policies adopted reveal a exploitation-oriented approach.

Italy's developments in Open Data are shown by the annual reports on Open Data Maturity in Europe, released by the European Data Portal. In only three years, Italy improved its ranking from 13th (in 2015) to 4th (in 2018) place among all European Countries and has been awarded a designation as a leading "trendsetter" in Europe for Open Data.

Despite the recognised maturity of Italy in this matter, further steps can be made to spread the potential of Open Data, especially regarding general awareness of the commercial opportunities given by PSI and Open Data. Best practices and good examples of successful exploitation are still very few or, at least, unknown. Furthermore, legal adjustments are necessary. In particular, codifying the various laws and regulations on this matter into a unified source of law and clarifying the boundaries and interplay between the three main pillars of Open Data ((i) transparency; (ii) re-use for economic exploitation; and (iii) protection of personal data and confidential information) would aid jurisdictions, such as Italy, to make further developments in Open Data.

The incoming transposition of the Dir. PSI III could be the occasion to address these issues and continue the path towards an Open Data economy.

ITALY

Andrea Andolina / Andrea Tuninetti Ferrari

ITALY DEFINES "DISTRIBUTED LEDGER TECHNOLOGY" AND "SMART CONTRACT"

With the entry into force of article 8-*ter* of Law no.12/2019, the Italian Parliament has provided legislative definitions of "*Distributed Ledger Technologies*" ("**DLTs**") (in Italian "*tecnologie basate su registri distribuiti*") and "*Smart Contracts*" ("**SCs**").

Although both the definitions refer to technical standards which are yet to be released by the competent authority ("*Agenzia per l'Italia digitale*", "**AGID**", Agency for Digital Italy), Law no.12/2019 represents the first attempt by the Italian legislator to address the legal nature of DLTs and SCs and their applications.

The definition of Distributed Ledger Technologies

DLTs are defined as "*technologies and informatic protocols which use a ledger which is shared, distributed, replicable, simultaneously accessible, architecturally decentralised with cryptography, insomuch as it enables the registration, the validation, the update and the storage of data, both unencrypted and further encrypted, verifiable by each participant, not alterable nor changeable*" (art. 8-*ter* par. 1).

The uploading of a file in a DLT has "*the legal effect of the electronic time stamp pursuant to article 41 of Regulation (EU) no.910/2014*" (art. 8-*ter* par. 3), provided that the DLTs meet the technical standards which will be released by the AGID (art. 8-*ter* par. 4).

The key elements of the definition rely on:

(i) the nature of the ledger (*shared, distributed, replicable, simultaneously accessible, architecturally decentralised*);

(ii) the actions to be enabled by the ledger (*registration, validation, update and storage*); and

(iii) the nature of the data (*verifiable by each participant, not alterable nor changeable*).

The definition is construed broadly in order to include, in principle, all the DLTs currently offered in the market *(i.e.*, private/consortium, and permissioned or permissionless). In any case, to fall within the definition of DLTs, the technology must ensure that data is "*not alterable nor changeable*." Commentators consider that this requirement, if literally interpreted, will never be met, since no DLTs will ensure a 100% non-alterability of data; therefore, it should be expected that the requirement will be interpreted with a reasonability standard, i.e. data should be "*[reasonably] not alterable nor changeable*." But, even if interpreted this way, the requirement could cause some implementation difficulties: on the one hand, permissioned DLTs (private and consortium) can ensure non-alterability thanks to a "*barrier to entry*" of the permission which gives some form of control. However, this could conflict with the statutory requirement that the ledger should be "*architecturally decentralised*". On the other hand, permissionless DLTs (such as the famous Bitcoin blockchain) can ensure (again, reasonably) that data are not

Key Issues

- DLTs and SCs must meet certain technical standards, which the competent authority AGID will issue in future.
- DLTs require data to be unalterable and unchangeable: requirements that are potentially impossible to meet.
- The uploading of files in DLTs will have the legal effect of the electronic time stamp pursuant art. 41 of Reg. (EU) 910/2014.
- Only SCs operating with DLTs are "Smart Contracts" according to law no.12/2019.
- It is still unclear whether SCs fall (or will fall) within the definition of contracts under Italian civil law or whether SCs will merely become the tools for the (digital) performance of a (traditional) contract.

alterable nor changeable. Oddly, this number (or an equivalent threshold) is not present in the recently issued law nor is referred to the AGID's guidelines; in other words, we do not know *how* DLTs must be to meet a DLT threshold according to Law no.12/2019. Therefore, it will be a matter of interpretation on a case-by-case basis.

The definition of Smart Contracts

A SC is "*a computer program which operates with distributed ledger technologies and the performance of which binds automatically two or more parties according to effects predetermined by the same parties. The smart contracts fulfil the requirement of the written form subject to previous informatic identification of the parties involved*". Such an informatic identification must meet the technical requirement which will be set forth by the AGID (art. 8-*ter* par. 2).

Firstly, Law no.12/2019 sets out a basic requirement: although from a technical standpoint SCs can run on technologies other than DLTs (as previously defined), only the ones which operate with DLTs will be "Smart Contracts".

It is unclear whether SCs are considered to fall within the definition of "contracts" according to Italian civil law. While art. 8-*ter* par. 2 defines SCs as "*computer programs*", the effects described in that article can lead to an interpretation of SCs either as an execution tool of a pre-existing contract (*performance*) or a contract within the strictest, civil law meaning (*binding nature for the parties*).

According to the national council of the notary public (*Consiglio Nazionale del Notariato*, the board representing notaries in Italy) the technical features of SCs in general prevent that SCs can, in principle, fulfil the essential elements of a contract under Italian law, given that SCs *per se* are essentially construed by *prescriptive / executive* rules. From a technical standpoint, therefore, there is no room for a *descriptive* section where the parties can agree the legal justification of the agreement (in Italian "*causa,*" i.e. the rationale underlying a transaction), which is one of the mandatory requirements to which the validity of a contract is subject. For instance, a SC can perform a payment between the parties (automatically upon the occurrence of a given circumstance), but the legal ground of such a payment is not contained (nor "containable") in the SC and, therefore, it would not be possible to refer that payment to a loan, a compensation, a penalty, royalties etc.

The national council of the notary public concludes that either SCs are the mere executive tool to perform a pre-existing agreement (which is the contract) expressing the legal justification of the actions performed by means of the SC *or* the legal justification of the agreement between the parties should in some way be expressed within the SC, *e.g.* by the inclusion of a descriptive part, useless from a technical standpoint but necessary to express the legal justification of the agreement; or through the standardisation of SCs in one form for each kind of agreement.

GERMANY

Stefan Lohn / Nikita Rolsing

SMART PRODUCTS AND LIABILITY PITFALLS

'Smart products' are tangible objects characterised by: *"increasing level of complexity and variety of ecosystems, actors and value chains; autonomy in decision making and actuating; generation, processing and reliance of big volumes of data; and openness to software extensions, updates and patches after the products have been put into circulation"*[1]. From self-driving cars to smart factories incorporating machine-to-machine communication and smart supply chains, smart products are able to act autonomously allowing for an economical and flexible production of goods.

Key Issues

- Smart products put the current liability regime to the test.
- European and German legislators recognise that the product liability laws may require a revision in respect of smart products and AI.
- Market participants should act to analyse and monitor their risk and take appropriate counter-measures to limit liability risks.

The increasing degree of autonomy facilitated by artificial intelligence ("**AI**") has many advantages but also gives rise to previously unknown risks. Autonomous and interconnected products are increasingly becoming harder to control and can make independent and sometimes unforeseeable decisions when interacting with their environment. The unforeseeability of AI is very much a feature rather than a bug.

Smart products and AI are likely to cause a paradigm shift in terms of the rule of law and traditional liability regimes which typically attach liability to a person (legal or natural), rather than an autonomous system.

Current and future rules of law and the risks from autonomous products

It has been questioned whether the current liability regime adequately covers all aspects of smart products. While there seems to be a consensus that established legal principles are generally sufficient to address the current risks posed, European (and German) legislators are carefully considering the implications that may give rise to a change in the rule of law.[2]

Smart products and AI under the current liability regime

The current European (and German) liability regime differentiates between contractual and non-contractual liability. While contractual liability typically relates to a warranty defect of a product, the non-contractual liability is governed by tort law in the shape of product and manufacturer's liability.

1. European Commission, Commission Staff Working Document – Liability for emerging digital technologies, 25 April 2018, SWD(2018) 137 final, p. 4; see also European Commission, Communication from the Commission to the European Parliament, the European Council and Social Committee and the Committee of the Regions, Artificial Intelligence for Europe, 25 April 2018, COM(2018) 237 final.
2. For the European perspective, see, e.g. European Commission, Report on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning the liability for defective products (85/374/EEC), 7 May 2018, COM (2018) 246 final, page 8 et seq.; for the German perspective *see*, e.g. German Federal Ministry for Economic Affairs and Energy, Plattform Industrie 4.0 – Working Paper, Künstliche Intelligenz und Recht im Kontext von Industrie 4.0 (*Artificial Intelligence and the law in the context of industry 4.0*), February 2019, pp.14 et seqq.

For contractual warranty claims, smart products put the contractual warranty laws to the test as liability arises from defects in the product at the time of the passing of risk. Given that smart products are able to adapt to their environment by machine-learning or over-the-air updates, implementing new features after the passing of risk of the product itself, this may no longer be an appropriate stand-alone solution. If a smart product shows an undesired (and unforeseen) behaviour after the passing of risk, it is an arduous task to prove that it was already defective at the transfer of risk. Notwithstanding, these contractual risks can be addressed by the parties to a certain extent. An issue remains, for example, for German manufacturers purchasing software or network services from U.S. based vendors. The extensive limitation of liability allowed by U.S. based jurisdictions is not mirrored in German law and may possibly effect a liability gap of German manufacturers with a view to supply chain recourse.

The same issue also arises in respect of non-contractual tort liability, for example, under the German Product Liability Act. The relevant point in time for determining whether or not a product is defective is when it is put into circulation. This raises the issue for smart products that can self-learn or be altered by software updates implementing new functions of the product as to whether the product was already defective when it was put in circulation.[3]

Additionally, there are significant problems regarding the burden of proof as smart products are a combination of hardware and software with various interfaces and the possibility that the software updates itself through learning. For the customer, this complexity results in a lack of transparency when trying to determine the root cause of an alleged defectiveness. Moreover, it is questionable whether an unintended autonomous action of a smart product would qualify as a defect at all.[4]

Addressing legal risks from smart products and AI: a look into the future

Market players are already reacting to the legal uncertainty and liability risks caused by smart products and AI. Some manufacturers, in an attempt to address the concerns of their customers, have promised special guarantees relating to the autonomous product risk.[5] It is unlikely that this position will be universally followed in light of the unfathomable liabilities that may arise.[6]

European and German legislators currently attach the responsibility arising from smart products and AI to the (natural or legal) person creating and controlling the respective risk, i.e. typically the user of a smart product as well as the manufacturer. For

3 European Commission, Report on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning the liability for defective products (85/374/EEC), 7 May 2018, COM (2018) 246 final, page 8 et seq.

4 See European Commission, Commission Staff Working Document, 7 May 2018, SWD(2018) 157 final, page 56.

5 Jonathan Gitlin, Talking the safety of self-driving cars with Volvo, 15 October 2015, available at https://arstechnica.com/cars/2015/10/talking-the-safety-of-self-driving-cars-with-volvo/ (last accessed 6 August 2019) citing Håkan Samuelsson, CEO of Volvo: "*When you drive manually, the driver is responsible. When it's automatic, we as the manufacturer are liable. If you're not ready to make such a statement, you're not ready to develop autonomous solutions*". Google and Mercedes-Benz were quoted with similar statements, see Bill Whittaker, Hands off the Wheel, CBS News, 4 October 2015, available at https://www.cbsnews.com/news/self-driving-cars-google-mercedes-benz-60-minutes/ (last accessed 6 August 2019).

6 Danielle Muoio, Elon Musk: Tesla not liable for driverless car crashes unless it's design related, Business Insider, 20 October 2016, available at https://www.businessinsider.de/elon-musk-tesla-liable-driverless-car-crashes-2016-10 (last accessed 6 August 2019).

manufacturers and users alike, it is thus certainly worthwhile to be proactive in identifying and addressing risks by defining areas of responsibility in relation to defects.

With increasing autonomy of smart products and AI, the duty to maintain the safety of the product may evolve. For example, the duty to design a product so that it poses no unforeseeable risk may require a manufacturer of a smart product to limit the range of autonomy developed through machine learning to a socially acceptable level. If these principles are not borne in mind during the design and development of the product, it may be regarded as defective and the manufacturer may possibly be liable for an undesired function of the smart product. In addition, due to the increased connectivity of products, the product monitoring duty may require monitoring systems to collect, evaluate and efficiently respond to data obtained from the market.

While not imminent, both European and German legislators have considered the introduction of an independent 'e-person' status for smart products and AI systems. However, numerous questions and issues remain unanswered as of yet, for example, whether there should be a general registration of autonomous/AI systems, requirements of mandatory insurance and mutual liability pools in case no insurance coverage is available, as well as the ethical boundaries relating to a use of autonomous products and AI.[7] At least for the time being, an introduction of an e-person status for autonomous systems appears to remain a proverbial "dream of the future".[8]

Summary and outlook

While the discussion of smart products and AI is certainly prevalent and has been considered by legislators in the EU and Germany, legislative action does not appear to be imminent. Rather, the current liability regime has been deemed to address the risks posed by smart products for the time being.

Both European and German legislators already have noted that a revision of the existing liability regimes may be required in the future to ascertain their effectiveness. As noted by the EU Commission in relation to the product liability directive: "*2018 is not 1985. The EU and its roles on product safety have evolved, as have the economy and technologies. Many products available today have characteristics that were considered science fiction in the 1980s.*"[9]

In the meantime, businesses will have to assess whether or not they are sufficiently protected against liability risks arising from smart products, be it as users or manufacturers. This includes not only an adequate identification and assessment of relevant risks, but also an appropriate response to manage and dispose of the respective exposure, for example, by means of contractual arrangements with suppliers and/or customers or by taking out appropriate insurance coverage.

7. See, e.g. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics, P8_TA(2017)0051, *Official Journal of the European Union*, 18 July 2018, page C 252/239 et seqq., at pages 243 through 251.
8. German Federal Ministry for Economic Affairs and Energy, Plattform Industrie 4.0 – Working Paper, Künstliche Intelligenz und Recht im Kontext von Industrie 4.0 (*Artificial Intelligence and the law in the context of industry 4.0*), February 2019, pp.14 et seqq.
9. European Commission, Report on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning the liability for defective products (85/374/EEC), 7 May 2018, COM (2018) 246 final, page 8 et seq.

GERMANY

Michael Kümmel / Susanne Werry

IOT IN LIGHT OF THE GDPR

*The Internet of Things ("**IoT**") is on the rise. As a result, a huge volume of personal data is being processed, often even sensitive personal data. With consumers' awareness for data protection growing, it is important that when companies develop new technology for smart devices, they ensure they consider IT security and data protection during the whole lifecycle of a product.*

Key Issues

- Consider IT security and data protection from the outset.
- Include data protection requirements in the complete lifecycle of a smart device.
- Implement Privacy by Design, Privacy by Default measures in solutions.
- Ensure state of the art IT security.

This article sets out the challenges for developing smart devices for the IoT under the General Data Protection Regulation ("**GDPR**") and highlights the actions required to not only be competitive but to avoid fines or damage claims.

IoT and data

Terms such as "Smart Home", "Connected Car" or "Industry 4.0" have been ubiquitous in recent years. They describe business models in which devices or machines ("**Things**") connect and communicate via the internet with other Things. During this communication, the device will send and receive data that has been processed (e.g. collected) by itself or another device. This data may be non-personal data (e.g. for industrial machine-to-machine communication) or personal data, especially for Business-to-Consumer applications.

Application of the GDPR

IoT services are based on business models that rely upon data exchanges between networked devices or between these devices and a central infrastructure. Therefore, several requirements must be considered in order to comply with the GDPR, which applies to the processing of personal data within the European Union ("**EU**") and the European Economic Area ("**EEA**"). In some cases, the GDPR also applies to companies outside the EU/EEA, e.g. if they offer goods or services to EU citizens or monitor their behaviour (e.g. profiles generated through smart devices).

Processing of personal data means any operation which is performed on information relating to an identified or identifiable natural person. This definition covers any kind of personal data being processed (e.g. collection, transfer or even anonymisation). A connected car, for example, processes its owner's locations, routes and driving habits. Similarly, fitness wearables process biological or health data of the person wearing the object. A smart refrigerator as part of a smart home processes information about its owner's living habits.

As a consequence, various obligations apply to suppliers of consumer goods and suppliers of industrial IoT products.

Obligations under the GDPR include:

(i) consent or other legal basis for processing data,

(ii) transparency,

(iii) granting of special rights to the data subject and being able to fulfil these rights,

(iv) ensuring security of personal data, and

(v) implementing Privacy by Design and Privacy by Default.

Challenges resulting from the IoT

Data processing requires a legal basis in order to comply with the GDPR. These can include: the data subject's consent, that the processing is required for the performance of a contract (e.g. if the supplier also enters into a service agreement with the customer) or an interest balance. In many cases, suppliers will need to rely on consent as the other possibilities usually do not cover the broad range of processing. When basing the processing on consent, this needs to be validly obtained, i.e. given freely, sufficiently clear and specific. For consent to be valid, the customer must know who processes which data, for what purpose and with whom the data will be shared.

Beyond this requirement for a legal basis, and irrespective of whether consent is required, suppliers must communicate specific information to their customers regarding the processing of their data. All this information must – again – be given in a clear and transparent way. This information must include, for instance, a comprehensive description of the customer's rights as a data subject. A supplier also needs to ensure that it is able to fulfil these rights, e.g. be able to provide each customer with information on what data is stored about him or her and be able to delete such data upon request. To be able to fulfil these obligations, developers must know which data the smart device processes and where it is stored. This might be a complicated task considering the often large amounts of data and – potentially – the limited access to the data by the controller itself, considering that a significant amount of such data is typically stored within the smart device.

As part of the IoT business model, smart devices usually need access to data collected by other devices via the IoT and vice versa. Such access can sometimes be in the interest of the customer but not necessarily, especially as it might increase the risk for data breaches. According to a recent study by a data security company, only 48% of suppliers can detect if their smart devices suffer a data breach (https://www.gemalto.com/press/pages/almost-half-of-companies-still-can-t-detect-iot-device-breaches-reveals-gemalto-study.aspx). In this context, suppliers of IoT products and services should keep in mind that such data breaches will not only damage their reputation but will likely also have legal consequences. Especially if the IT security is not state of the art, sanctions of up to EUR 20,000,000 or 4% of worldwide annual turnover can be imposed. In recent months the the UK's Information Commissioner's office ("**ICO**") has shown that these are not idle threats, with notices to fine British Airways (£183.4 million or 1.5% of its global turnover) and Marriott (£99.2 million).

One of the intentions in the implementation of the GDPR was that companies should protect data subjects through IT measures and security. Therefore, when planning

new devices, developers need to consider the concepts of Privacy by Design (i.e. adopting appropriate technical and organisational measures to provide for data minimisation in an effective manner) and Privacy by Default (i.e. setting the strictest privacy settings by default).

Suppliers should also keep an eye on the new EU Regulation on Privacy and Electronic Communication, which is planned for 2020 that would implement further requirements regarding IoT devices and applications.

Regulation

In Germany, authorities have not yet responded to the challenges resulting from IoT. However, a look at other European countries can show how IoT business models could be regulated in the near future. In October 2018, the UK Department for Digital, Culture, Media and Sport released a 'Code of Practice for Consumer IoT Security' (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf) setting out guidance and non-binding security standards for IoT manufacturers. Moreover, in May 2019, the UK Government released a consultation paper on the potential to create binding regulation as there are still 'significant shortcomings in many products on the market'. The consultation paper suggests mandating legislation that retailers may only sell IoT products that conform to all or certain parts of the 'Code of Practice' and/or mandatory labelling stating whether or not manufactures have complied with the 'Code of Practice'. Due to the change in government in the UK, it remains to be seen whether this specific legislation for IoT security will come into force. In Germany, it is still unclear whether the government will follow this development towards a stricter regulation of IoT business models.

Required actions

To face these challenges, developers should consider data protection requirements throughout the whole engineering process. It is often too late to take these requirements into account when the technical planning has been finalised. As shown, many obligations under the GDPR require a technical solution. As smart devices often develop during their lifecycles, it is necessary that the processing of personal data and related IT security is regularly reviewed. From the beginning, developers must install and develop functional support services to enable reviews and amendments. It is therefore key for every developer and supplier to have a good understanding of its data processes. Only then can data protection compliance be achieved.

Conclusion

Companies developing and offering smart devices in the IoT need to increase their attention to IT security and data protection by including data protection requirements in their planning and review process. Due to consumers' increased awareness of data protection, compliance is no longer only a legal risk but is increasingly reputational.

The keys to a competitive product will be considering measures to best implement, IT security and data protection from the outset.

GERMANY

Günter Barth / Julian Scheerbaum

THE GERMAN TRADE SECRET ACT AND THE IMPLICATIONS ON EMPLOYMENT AND BUSINESS CONTRACTS

On 26 April 2019, the German Trade Secret Act ("**TSA**") implementing Directive (EU) 2016/943 ("**Know-How Directive**") came into force. While the TSA creates new possibilities for protection, it also presents certain challenges for companies looking to take advantage of this protection, in particular, regarding employment and business contracts. This article will discuss the changes in this area of the law and the associated challenges.

Concept of Trade Secrets

The TSA introduced a legal definition of trade secrets for the first time. Section 2 No.1 of the TSA states that for information to be considered a trade secret, such information must be (i) "*neither in its entirety nor in the exact arrangement and composition of its components generally known or readily accessible to persons in the circles that normally handle this type of information and therefore be of economic value*"; (ii) "*subject to appropriate secrecy measures by its lawful owner;*" and (iii) "*subject to a legitimate interest in secrecy*". However, terms such as "*legitimate interest in secrecy*" and "*appropriate secrecy measures*" create uncertainty and raise questions about the practical implementation of the law.

Interpretation of Appropriate Secrecy Measures

Unlike under the previous law, the owner of a trade secret must now actively take measures to protect information as he/she bears the burden of proof of demonstrating that information is a trade secret. Otherwise, the relevant information will not be subject to the new law. However, it is unclear yet how the demands imposed by the TSA can be met. Some guidance is given in the explanatory memorandum to the TSA, which sets out seven guiding factors which include: (i) the value of the information and its development costs; (ii) the nature of the information; (iii) its significance for the company; (iv) the size of the company; (v) the usual standard of confidentiality; (vi) the way in which the information is labelled; and (vii) the scope of corresponding contractual arrangements with business partners.

A prudent company should adopt the following strategy, bearing in mind that the law requires "reasonable" measures to be taken to protect trade secrets:

- comprehensive use of binding non-disclosure agreements both internally with employees and externally with contractual partners (best practises: contractual fine or right for preliminary injunction);
- agree procedures for the disclosure of trade secrets during transactions;
- notarial deposit of the most crucial trade secrets ("crown jewels");

Key Issues

- Newly inforced German Trade Secret Act requires companies to take active secrecy measures to ensure protection.
- The required adjustment of company policies and employment contracts is complicated by the various indefinite terms used in the legal wording of the new Law.
- Reverse engineering of shared products is of particular importance and should, unlike previously, be contractually excluded to the extent legally permitted.
- Another threat for companies must be seen in the possible loss of trade secrets through whistleblowing.
- Procedural changes aim to prevent the loss of rights during proceedings.

- internal diversification regarding access to business secrets on a strict need-to-know basis;
- supplementary technical access restrictions in addition to existing physical barriers (buzzword: IT security).

It is important, given the burden of proof to demonstrate information is a trade secret, that the implementation of the actions above is documented carefully.

However, the TSA does not require owners of trade secrets to implement the best available secrecy measures. There is no perfect secrecy in business operations and the TSA does not impose unrealistic obligations on market participants.

Reverse Engineering

One area of concern for companies (especially during corporate transactions) is the reverse engineering of products and the outflow of know-how during this process. Reverse engineering means the deconstruction or any other analysis of products (including software), objects or substances in order to derive the embodied know-how. Reverse engineering was generally prohibited in Germany by the provisions of the German Unfair Competition Act. This prohibition has been eased by recent case law, which has focused on the necessary technical complexity of deconstruction.

Reverse engineering is now generally permitted in order to obtain a trade secret under the TSA if the object at issue "*has been made publicly available*" or "*is in the lawful possession of the actor*". However, there are some key differences between these two scenarios.

In the latter case (lawful possession) the product in question "*shall not be subject to any obligation to restrict the acquisition of the trade secret*". This allows for the possibility of contractually excluding the application of the TSA in cases of lawful possession, e.g. development agreements between companies. Additionally, a contractual penalty could be agreed in order to avoid difficulties in proving the amount of damages. The actual use of the know-how gained through reverse engineering will most likely already be prevented by corresponding confidentiality regulations.

As regards public availability (e.g. by the free sale of goods), it can be difficult to determine when the availability of a product is in the public domain. For example, is a machine that is only offered to certain companies in a niche industry and not to the world at large regarded as publicly available? The TSA lacks a possibility to exclude its application in such a scenario. An attempt to do so through, for example, a company's general terms and conditions may not be compatible with the TSA.

It remains to be seen how such a clause in a company's general terms and conditions could be effective against the background of the German Civil Code which prohibits the deviation from essential principles of the underlying statutory provision. The essential principle of the TSA is the general permissibility of reverse engineering. The overall principle of the underlying Know-How Directive is the EU-wide protection of trade secrets which gives companies the possibility of preventing reverse engineering. The German application of the Know-How Directive must not be stricter than in other

countries that do not have a similar restriction of general terms and conditions in their Civil Code.

Whistleblowing

Section 5 No.2 of the TSA on permissible disclosures of trade secrets is of specific relevance in the context of criminal sanctions. The provision states that anyone who discloses a trade secret "*for the protection of a legitimate interest", namely "for the disclosure of an unlawful act or professional or other misconduct*", is justified and thus exempt from punishment.

Accordingly, whistleblowing, i.e. the disclosure of business secrets to criminal prosecution authorities or the media in order to prove the unlawful conduct of the employer, is to be exempt from punishment under certain circumstances. However, whistleblowing should only be justified "*if the acquisition, use or disclosure is suitable to protect the general public interest*". Firstly, it remains open to debate in which cases the general public interest is concerned. Secondly, taken in the literal sense, *any* disclosure of even the slightest "misconduct" – not necessarily one of unlawful nature – could be declared legal. The extended explanatory memorandum of the TSA had demanded a "*misconduct of some extent and weight*" – a requirement which was unfortunately not implemented in the final wording.

Furthermore, the wording of section 5 No. 2 of the TSA does not expressly require any previous attempts by the whistleblower to resolve the matter in-house. However, pursuant to Section 1 (3) No. 4 TSA, rights and obligations resulting from employment contracts fall within the scope of the new Act. Thus, it follows from the loyalty obligations of the employee that he first needs to contact responsible authorities within the company. Despite that, it is preferable to include secondary obligations in employment contracts under which the employee is obliged to resolve the matter internally. Likewise, the recitals of the Know-How Directive emphasise that the whistleblower's approach needs to be appropriate.

It remains to be seen whether the EU Directive on the Protection of Persons Reporting on Breaches of Union law (proposal COM (2018) 218/973471), which was adopted in April 2019, can contribute to an overall whistleblowing protection system. Article 1 of the draft version provides that the directive shall cover, among other things, the protection of privacy and personal data and the security of network and information systems.

Procedural effects

A major concern of the Know-How Directive was the preservation of confidentiality during court proceedings. Owners of trade secrets should not be deterred from enforcing material claims due to the danger of excessive disclosure during court proceedings, which may even lead to a loss of rights according to the trade secret definition. Unfortunately, the new provisions do not completely resolve the dilemma of the trade secret owner.

Section 16 (1) TSA grants the court the possibility to classify information as "*requiring secrecy*" upon request of a party. If classified as such, section 16 (2) TSA states that the parties and other persons involved in the proceedings are obliged to treat the information confidentially and are prohibited to use and disclose the information outside of the proceedings. Infringements can be sanctioned by the court with an administrative fine of up to EUR 100,000 (or up to six months of detention) under section 17 TSA. However, this fine could still be too low for enormously valuable trade secrets, such as recipes for high-revenue products or specialized production know-how. Besides, a fine does not solve the core problem that the opposing party may gain actual knowledge of the secret – albeit subject to legal restrictions – at the latest during the process.

In addition, section 19 TSA gives the parties a right to request that only a certain number of reliable persons have access to documents or oral hearings (including protocols and recordings). However, in any case at least one natural person of each party and one of their (legal) representatives must be granted unlimited access.

Moreover, under section 15 (2) TSA, in the event of an unlawful use of trade secrets, the (regional) court in whose districts the defendant has his general place of jurisdiction has exclusive local jurisdiction, meaning that the owner of the secret – as customary in German intellectual property law – is barred from bringing an action at the place of the infringement.

SPAIN

Juan Cuerva de Cañas

REGULATIONS IMPLEMENTING THE AMENDED SYSTEM FOR THE PAYMENT OF FAIR COMPENSATION FOR PRIVATE COPYING ENTER INTO FORCE

In November 2018, the Spanish legislator passed Royal Decree 1398/2018 (the "**2018 Decree**"), which implemented the current system for fair compensation for private copying based on establishing an amount payable by manufacturers, importers and distributors of equipment, devices and material media for reproduction. The Royal Decree entered into force on 2 January 2019. This article summarises and examines the key provisions of the Royal Decree.

Key Issues

The 2018 Decree:

- Implements the procedure for the payment of Fair Compensation for private copying and provides legal certainty.
- Imposes the obligation for debtors and distributors of equipment or material media that are subject to the payment of Fair Compensation to break down the price of the product and the amount of Fair Compensation in their invoices.
- Regulates the scenarios in which there is an exemption from the payment of Fair Compensation and the procedure to be followed. In addition, it sets out the procedure for the refund of Fair Compensation when appropriate.

Background to the 2018 Decree

In June 2016, the Court of Justice of the European Union ("**CJEU**") held that the system in force in Spain for the payment of fair compensation for private copying ("**Fair Compensation**"), funded by the general state budget, was contrary to Directive 2001/29/EC[1] in that the Spanish system was not capable of guaranteeing that the cost of fair compensation was ultimately borne solely by the users of private copies. Accordingly, the Spanish legislator passed Royal Decree-Act 12/2017 (the "**2017 Decree**")[2], which amended article 25 of the Spanish Copyright Act[3], regulating fair compensation for private copying. Under the 2017 Decree, the Spanish Government had one year to implement the amendment.

The 2018 Decree[4] fulfilled the mandate conferred in the 2017 Decree.

Obligation to pay Fair Compensation for private copying and procedure for making the payment

Under the Spanish Copyright Act, the reproduction of already released works exclusively for private use, rather than professional or business use, with no direct or indirect commercial purpose, generates the obligation to pay Fair Compensation. Such payment is designed to constitute proper compensation for the copyright holders for the harm caused by reproductions carried out under the legal limit of private copying[5].

1. See judgments of the CJEU of 21 October 2010 (case C-467/08; Padawan *v* SGAE) and of 9 June 2016 (case C-470/14; Egeda *v* Ametic) and judgment of the Spanish Supreme Court (Third Chamber) of 10 November 2016.
2. Royal Decree-Act 12/2017, of 3 July, which amends the restated text of the Intellectual Property Act, approved by Royal Legislative Decree 1/1996, of 12 April, on the system of fair compensation for private copying.
3. Royal Legislative Decree 1/1996, of 12 April, which approves the revised text of the Spanish Copyright Act, standardising, clarifying and harmonising the legal provisions currently in force on the subject.
4. Royal Decree 1398/2018, of 23 November, which implements Article 25 of the restated text of the Intellectual Property Act, approved by Royal Legislative Decree 1/1996, of 12 April, on the system of fair compensation for private copying.
5. This limit is regulated in Article 31.2 and 3 of the Spanish Copyright Act.

Debtors and creditors of Fair Compensation

The debtors obliged to pay Fair Compensation are (i) manufacturers in Spain, where acting as commercial distributors, and (ii) acquirers outside of Spain (importers), for commercial distribution or use within Spain, of equipment, devices and material media suitable for making reproductions of copyright protected works.

Meanwhile, the creditors of Fair Compensation are the authors of books or similar publications, together with editors, producers of phonograms and videos and the artists who perform the works.

As for the amount of Fair Compensation, it depends on the equipment or material media in question. In the case of equipment, the amount varies from 0.33 cents/unit for CD recorders to 6.54 euros/unit for external disks (SSD and HDD). In the case of media, the amount varies between 0.08 euros/unit for recordable CDs and 0.28 euros/unit for recordable DVDs.

In accordance with the 2018 Decree, debtors and distributors[6] of equipment or media subject to the payment of Fair Compensation have to include separately on the invoices issued to their customers (i) the price of the equipment or media, and (ii) the amount of Fair Compensation applicable to said equipment/media. In order to strengthen this obligation, the 2018 Decree prohibits distributors from accepting supplies of equipment or media from their suppliers unless invoiced in the manner indicated.

Communication to the collecting entity of the list of equipment or media subject to the payment of Fair Compensation

Within 30 calendar days following the end of each quarter, the debtors are obliged to present to the collecting entity, *Ventanilla Única,*[7] a list of the units of equipment, devices and media in relation to which the obligation to pay Fair Compensation arose in that quarter. From that list, the amounts corresponding to units destined for export from Spain and those that are exempted from payment of Fair Compensation must be deducted. The same obligation to notify *Ventanilla Única* applies to distributors.

Payment of Fair Compensation

After making the necessary checks of the quarterly lists received, the collecting entities have to issue an invoice in the name of the debtor (or jointly liable party[8]) which is notified in unified form via the *Ventanilla Única*. The debtor (or jointly liable party) then has one month, as of receipt of the invoice in question, to pay Fair Compensation. The 2018 Decree also establishes mechanisms for the refund of any Fair Compensation unduly paid or for supplementary invoices when, due to an error, equipment or materials subject to payment of Fair Compensation were not declared (or were exempted).

6. "Distributors" is understood to mean the distributors, wholesale or retail, successive acquirers of the equipment, devices and material media.
7. This legal entity manages payment of the Fair Compensation centrally. The amounts collected are subsequently distributed among the different collecting entities that represent the rightsholders (AGEDI, AIE, AISGE, CEDRO, DAMA, EGEDA, SGAE and VEGAP).
8. A distributor who fails to demonstrate that is has paid the Fair Compensation to a debtor is a "jointly liable party".

Exemption and refund of the payment of Fair Compensation

Finally, under the 2018 Decree, in the event equipment or media are acquired by persons to be used exclusively for professional purposes (i.e. not for private copying), then:

(i) no Fair Compensation shall be payable when the equipment or material media is purchased (**exemption**); or

(ii) such persons may apply for a refund for the amount of Fair Compensation paid (**refund**).

Both the exemption procedure – which is subject to a prior certificate being obtained – and the refund procedure, are duly regulated by the 2018 Decree.

In both procedures it is essential to demonstrate by formal means that the equipment or material media will not be used to make private copies (which generates the obligation to pay Fair Compensation).

Upcoming Event

TALKING TECH LIVE: INNOVATION IN BUSINESS

EXPLORING THE LEGAL CHALLENGES AND OPPORTUNITIES
OF DIGITAL BUSINESS AND NEW TECHNOLOGY

BERLIN | 19 SEPTEMBER 2019

Join us in Berlin, Germany at our inaugural Talking Tech Live conference, where we will be talking tech and looking at managing innovation in business. We'll be joined throughout the afternoon by a series of expert panelists and keynote speakers for a series of energetic and insightful talks by tech industry leaders like Airbus, Microsoft, Nokia and Spotify among others. On request you will also have the unique opportunity to exchange with our tech experts from around the globe in individual one-on-one-meetings.

PURPOSE
Immerse yourself in dialogue, gather knowledge about what's coming next and discuss the legal and economic implications of new technologies and digital change. Meet with other legal and business experts who are actively exploring tech issues.

LOCATION
The Kabbalah Centre Berlin
Hauptstraße 27 (Entrance E, 3rd floor)
10827 Berlin (Germany)

AGENDA TOPICS

AI AS A NEW PROBLEM FOR APPLIED ETHICS AND POLICY MAKING
Prof Dr Thomas Metzinger, Professor of Theoretical Philosophy at Johannes Gutenberg-Universität Mainz, Adjunct Fellow at Frankfurt Institute for Advanced Study, Member of AI High-Level Expert Group nominated by the EU Commission

THE FUTURE OF MOBILITY – FROM THE ROAD TO THE SKY
What is the regulatory framework like where geographical borders are no longer the first priority?
Vincent Barbaud, Regulatory Legal Affairs at Airbus; Ingmar Dathe, Legal Advisor Public Affairs Manager at MOIA, a subsidiary of Volkswagen – In dialogue with CC partners

TEAMING UP AND MANAGING CHANGE
What legal challenges do companies face when using new technologies to implement new business models? A cross-border view from Europe, Asia and the US.
Clemens Heusch, Head of European Litigation at Nokia; Michael F. Spitz, CEO at main incubator, the R&D unit of Commerzbank; Frank H. Lutz, CEO at CRX Markets – In dialogue with CC partners

OPERATIONAL EXCELLENCE THROUGH DOCUMENT AUTOMATION
Jeroen Plink, CEO and Jennifer Paybody, Head of Commercial at Clifford Chance Applied Solutions, a subsidiary of Clifford Chance

PAVING THE WAY FOR FAIR COMPETITION – SPOTIFY VS. APPLE
How does Apple's anti-competitive behaviour in the App Store affect both consumers and competitors?
Horacio Gutierrez, General Counsel at Spotify; Thomas Vinje, Chairman of the Global Antitrust Group at Clifford Chance, who is currently advising Spotify in its complaint against Apple before the European Commission for anti-competitive conduct in the App Store

BIG DATA, BIG COMPETITION HEADACHES? THE NEW INTERSECTION OF COMPETITION AND DATA LAW
Competition regulators are now focused on data, data gathering and consumer protection like never before. How do companies navigate this complex new landscape?
Horacio Gutierrez, General Counsel at Spotify; Carel Maske, Director Competition EMEA at Microsoft; Holger Temme, Head of Growth at Ververica – In dialogue with CC partners

ACKNOWLEDGEMENT OF CONTRIBUTORS TO THE CURRENT EDITION

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

Dr. Florian Reiling
Counsel
Düsseldorf
T: +49 211 4355 5964
E: florian.reiling@cliffordchance.com

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

Tim Grave
Partner
Sydney
T: +61 2 8922 8028
E: tim.grave@cliffordchance.com

Jack Oakley
Associate
Sydney
T: +61 2 8922 8091
E: jack.oakley@cliffordchance.com

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

Francesca Zambuco
Associate
Rome
T: +39 064229 1235
E: francesca.zambuco@cliffordchance.com

Andrea Andolina
Associate
Milan
T: +39 02 8063 4240
E: andrea.andolina@cliffordchance.com

Andrea Tuninetti Ferrari
Senior Associate
Milan
T: +39 02 8063 4435
E: andrea.tuninettiferrari@cliffordchance.com

Dr. Stefan Lohn
Counsel
Düsseldorf
T: +49 211 4355 5366
E: stefan.lohn@cliffordchance.com

Dr. Michael Kümmel
Associate
Frankfurt
T: +49 69 7199 1620
E: michael.kuemmel@cliffordchance.com

Susanne Werry, LL.M
Senior Associate
Frankfurt
T: +49 69 7199 1291
E: susanne.werry@cliffordchance.com

Günter Barth
Associate
Düsseldorf
T: +49 211 4355 5963
E: guenter.barth@cliffordchance.com

Juan Cuerva de Cañas
Associate
Barcelona
T: +34 93 344 2279
E: juan.cuerva@
cliffordchance.com

Jonathan Coote
Trainee
London
T: +44 20 7006 1910
E: jonathan.coote@
cliffordchance.com

FURTHER CONTRIBUTORS

Fabian Pollex
Katarzyna Kuchta
Nicola Kung
Joshua Malek
Nikita Rolsing
Julian Scheerbaum
Laura Rayak
Noël Lücker

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

Belgium

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

France

Diego de Lammerville
Partner
Paris
T: +33 1 4405 2448
E: diego.delammerville@
cliffordchance.com

Germany

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

Florian Reiling
Counsel
Düsseldorf
T: +49 211 4355 5964
E: florian.reiling@
cliffordchance.com

Italy

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

Poland

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

Russia

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

Singapore

Nish Shetty
Partner
Singapore
T: +65 6410 2285
E: nish.shetty@
cliffordchance.com

Spain

Miquel Montañá
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

The Netherlands

Jaap Tempelman
Counsel
Amsterdam
T: +31 20 711 3192
E: jaap.tempelman@cliffordchance.com

United Kingdom

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

United States

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

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

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

NOTES

OUR INTERNATIONAL NETWORK
32 OFFICES IN 21 COUNTRIES

Abu Dhabi
Amsterdam
Barcelona
Beijing
Brussels
Bucharest
Casablanca
Dubai
Düsseldorf
Frankfurt
Hong Kong
Istanbul
London
Luxembourg
Madrid
Milan
Moscow
Munich
Newcastle
New York
Paris
Perth
Prague
Rome
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

www.cliffordchance.com

Clifford Chance, Königsallee 59, 40215 Düsseldorf, Germany

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 • Barcelona
Beijing • Brussels • Bucharest
Casablanca • Dubai • Düsseldorf
Frankfurt • Hong Kong • Istanbul
London • Luxembourg • Madrid
Milan • Moscow • Munich • Newcastle
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.

1908-000346