Chapter 3. Fragmented protection of trade secrets across the EU leading to a harmonised system: study of the English and German models and the emerging common framework

§ 1 Scattered protection across the internal market before the implementation of the Trade Secrets Directive: Different models

Until the adoption of the TSD, the legal framework for the protection of trade secrets had not been harmonised in the EU. However, all Member States offered some level of redress, in line with the minimum standards set forth in Article 39 of the TRIPs Agreement. The regimes, nevertheless, differed substantially and the level of protection was very limited in some jurisdictions.[793] Such a fragmented legislative landscape was described by some as a "patchwork"[794] and to some extent resulted from the overlap of regimes that are applicable to safeguarding secret information within national jurisdictions. Beyond specific rules dealing with trade secrets, contractual agreements between the parties play a central role in their enforce-

793 Hogan Lovells, 'Study on Trade Secrets and Parasitic Copying (Look-alikes) – Report on Trade Secrets' (MARKT/2010/20/D) (2012) para 290 <ec.europa.eu/internal.../docs/trade-secrets/120113_study_en.pdf> accessed 15 September 2018; see also Recital 6 TSD: "Notwithstanding the TRIPS Agreement, there are important differences in the Member States' legislation as regards the protection of trade secrets against their unlawful acquisition, use or disclosure by other persons. For example, not all Member States have adopted national definitions of a trade secret or the unlawful acquisition, use or disclosure of a trade secret, therefore knowledge on the scope of protection is not readily accessible and that scope differs across the Member States. Furthermore, there is no consistency as regards the civil law remedies available in the event of unlawful acquisition, use or disclosure of trade secrets, as cease and desist orders are not always available in all Member States against third parties who are not competitors of the legitimate trade secret holder. Divergences also exist across the Member States with respect to the treatment of a third party who has acquired the trade secret in good faith but subsequently learns, at the time of use, that the acquisition derived from a previous unlawful acquisition by another party".

794 Hogan Lovells 2012 (n 793) para 5.

ment, along with labour law provisions. Furthermore, most Member States set forth criminal penalties in the case of industrial espionage.[795]

Despite the myriad of legal sources that regulated trade secrets protection in national jurisdictions before the adoption of the TSD, Ohly identified six pre-eminent models across the Single Market.[796] In the first place, he referred to Sweden, the only Member State where a specific statute for the protection of trade secrets had been passed before the adoption of the TSD. The Swedish Act on the Protection of Trade Secrets (1990:409) was enacted in 1990, prior to the approval of the TRIPs Agreement, mainly as a result of the absence of a general unfair competition act and the increasing legal challenges posed by industrial espionage and employee mobility.[797] Next, he mentioned the so-called "IP model", which is best exemplified by the Italian legal system. As noted above,[798] the Italian Industrial Property Code of 2005 included trade secrets within the spectrum of rights traditionally protected under Intellectual Property Law. Indeed, Italy was the first jurisdiction to adopt such a strong property approach. Thirdly, France followed a so-called "hybrid model", whereby manufacturing trade secrets ("*secrets de fabrique*") were included within the Intellectual Property Code.[799] However, trade secrets in the broadest sense ("*secret d'affaires*") were afforded protection only on the basis of general tort law, unfair competition and criminal sanctions.[800] Certain jurisdictions like Spain or Switzerland built their trade secret regimes on civil provisions enshrined within their unfair competition acts.[801] This was the case with Article 6 of

795 By way of illustration, see Articles 278-80 of the Spanish Criminal Code (Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal).

796 Ansgar Ohly 2013 (n 13) 27-28; however, some jurisdictions do not follow any of the above identified models. This is, for instance, the case of Malta, where trade secrets are only protected contractually. In the Netherlands, a general principle of tort law, unlawful act, is applied to misappropriation cases; see further Hogan Lovells 2012 (n 793) paras 159-170.

797 Marianne Levin, 'Trade Secret Protection and the Computation of Damages under Swedish Law' 735, 737 in Thomas Dreier, Horst-Peter Götting, Maximilian Haedicke, Michael Lehmann (eds), *Perspektiven des Geistigen Eigentums und des Wettbewerbsrechts* (C.H. Beck 2005).

798 See chapter 1 § 3 B) I. 3, a).

799 See Article L621-1 Code de la propriété intellectuelle (version consolidée au 25 avril 2016) (French Intellectual Property Code).

800 Jérôme Passa, 'La protection des secrets d'affaires en droit français' 47 in Jacques de Werra (ed), *La protection des secrets d'affaires* (Schulthess 2013).

801 Ansgar Ohly 2013 (n 13) 27-28.

the Swiss Unfair Competition Act[802] and Article 13 of the Spanish Act against Unfair Competition.[803] Notwithstanding this, in these legal systems accessory criminal liability was also foreseen in the event of industrial espionage. In the fifth model, the one followed in countries like Austria, Poland and Germany, protection was built upon criminal provisions that were part of the respective unfair competition acts.[804] Finally, common law jurisdictions such as England and the Republic of Ireland had not enacted any provisions to deal with trade secrets, not even from a criminal law perspective. Effective protection was achieved through the breach of confidence action, which covers confidential information in general i.e. private information, government secrets, and artistic and literary information.[805]

In the light of such a scattered legal framework, the last two models are studied, taking as example cases the German (§ 2) and English jurisdictions (§ 3). By application of the methodology of comparative law, the following sections analyse the legal mechanisms in place in these two national systems, which furthermore belong to two different legal traditions (civil and common law, respectively), in order to achieve effective protection of valuable secret information. Furthermore, both legal regimes were highly influential during the negotiation and configuration of the harmonised system and therefore constitute the point of departure to critically analyse the emerging common framework introduced by the TSD (§ 5). From a methodological perspective, it should be noted that the research for this thesis was completed before the implementation of the TSD in both jurisdictions, and consequently, no reference to resulting harmonised framework in these jurisdictions is made.

§ 2 *Trade secrets protection in Germany before the implementation of the TSD*

The present section delves into the protection of trade secrets in Germany prior to the implementation of the TSD. The German jurisdiction is a civil law jurisdiction with a long tradition of protecting confidential informa-

802 Bundesgesetz gegen den unlauteren Wettbewerb (UWG) vom 19. Dezember 1986 (Stand am 1. Juli 2016).
803 Ley 3/1991, de 10 de enero, de Competencia Desleal (Spanish Unfair Competition Act).
804 Ansgar Ohly 2013 (n 13) 27-28.
805 See more generally Tanya Aplin and others 2012 (n 22).

tion, which has led to a rich body of case law. Section A briefly examines the development of trade secrecy law since its inception in the late XIX century. Next, section B looks into three of the main fields of law that regulated trade secrets disclosure. In this context, special emphasis is given to the intersection between unfair competition law and criminal law.

A) Development of the law of trade secrets

The protection of trade secrets in Germany until the mid-XIX century consisted mostly of scattered pieces of legislation that set forth criminal liability with respect to the misappropriation of trade secrets in specific sectors that were considered of particular relevance for the states economies.[806] Indeed, legislatures concentrated mostly on criminal protection due to the particular vulnerability of secret information and the fact that it was deemed that the persons liable for misappropriation did not have the financial resources to pay for the damages arising from their conduct.[807]

The seed of the system was built upon the German Unfair Competition Act, dated 27 Mai 1899,„[808] which was mostly concerned with the protection of the duty of confidence that the employee owed to the employer, as per § 9 paragraph 1 UWG 1896.[809] In addition, liability was also extended to third parties that had obtained secret information as a result of any of the breaches described in paragraph 1 or in breach of any other law or in a manner contrary to honest commercial practices (and to the detriment of competitors in all instances).[810] Some years later, in 1909, following the influence of embroidery and lace manufacturers, the German legislature de-

806 As noted by Florian Schweyer 2012 (n 99) 390.

807 *Harte-Bavendamm/*Henning-Bodewig (n 376) §§ 17-19 UWG Rdn 6.

808 Gesetz zur Bekämpfung des unlauteren Wettbewerbs 1986 ("UWG 1986").

809 According to Florian Schweyer 2012 (n 99) 390; § 9 paragraph 1 UWG 1886 provided the following: "Mit Geldstrafe bis zu dreitausend Mark oder mit Gefängniß bis zu einem Jahre wird bestraft, wer als Angestellter, Arbeiter oder Lehrling eines Geschäftsbetriebes Geschäfts- oder Betriebsgeheimnisse, die ihn vermöge des Dienstverhältnisses anvertraut oder sonst zugänglich geworden sind, während der Geltungsdauer des Dienstverhältnisses unbefugt an Andere zu Zwecken des Wettbewerbes oder in der Absicht, dem Inhaber des Geschäftsbetriebes Schaden zuzufügen, mittheilt".

810 According to Florian Schweyer 2012 (n 99) 390, § 9 paragraph 2 UWG 1896 provided the following: "Gleiche Strafe trifft denjenigen, welcher Geschäfts- oder Betriebsgeheimnisse, deren Kenntniß er durch eine der im Absatz 1 bezeichneten Mittheilungen oder durch eine gegen das Gesetz oder die guten Sitten

cided to regulate in a separate provision protection against the so-called "piracy of models" ("*Vorlagenfreibeuterei*"), which now corresponds to § 18 UWG.

The following section provides an overview of three of the main legal regimes under which the protection of trade secrets is regulated in Germany. To this end, first, the constitutional dimension of trade secrets protection is briefly examined (§ I). Next, the dissertation looks into the unfair competition provisions that deal with trade secrets and their intersection with criminal law (§ II). Finally, some remarks regarding the applicability of general civil law provisions are made (§ III).

B) Legal regime for the protection of trade secrets

I. Constitutional Law

As outlined in chapter 1, from a civil law perspective, in Germany, it is unclear to what extent trade secrets fall under the category of IPRs or property rights. However, such a discussion has a constitutional dimension. In effect, if trade secrets are regarded as a species of property or a "legal interest" that merits protection,[811] the so-called "property guarantee" ("*Eigentumsgarantie*") provided for in § 14(1) of the German Constitution[812] and all of the implications derived from it should apply to their protection,[813] in particular, §§ 823 I, 812 I, and § 687 II of the BGB.

Against this backdrop, tension arises between "the property guarantee" and the "occupational freedom right" set forth in § 12(1) of the German

---

verstoßende eigene Handlung erlangt hat, zu Zwecken des Wettbewerbes unbefugt verwerthet oder an Andere mittheilt".

811 Stanisław Sołtysiński 1986 (n111) 351; in the same vein, Axel Beater, *Unlauterer Wettbewerb* (2nd edn, C.H. Beck 2011) § 9 Rdn 24 noting that: "Eigentum ist weit auszulegen und erfasst nicht allein Sacheigentum im Sinne des bürgerlichen Rechts, sondern sämtliche vermögenswerten privaten Rechte, die dem Einzelnen ähnlich wie das Sacheigentum zur privaten Nutzung und Verfügung zugeordnet sind. Solche vermögenswerten Rechtspositionen können z.B. Geschäftsgeheimnisse im Sinne der §§ 17 ff UWG. "

812 Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 1001, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 13. Juli 2017 (BGBl. I S. 2347) geändert worden ist.

813 *Ohly*/Sosnitza, *Gesetz gegen den unlauteren Wettbewerb* (7th edn, C.H. Beck 2016) §§ 17-19 Rdn 8.

Constitution, particularly in the context of departing employees and the information that they should be free to use in a new position.[814] This issue garnered a lot of attention during the negotiation of the TSD, and is mostly decided on a case-by-case basis, taking into consideration all of the relevant interests of each specific situation. A more detailed account of this topic and the principles applied by German courts in the ponderation of both rights is provided in chapter 6.[815]

II. Unfair competition law and its intersection with criminal law

The main provisions that govern the legal regime for the protection of trade secrets in the German jurisdiction are enshrined in §§ 17 through 19 UWG. In essence, the primary objective of this statute is to regulate market practices in order to protect competitors, consumers, other market participants and, ultimately, the general public.[816] To this end, § 3 UWG (as amended in 2015) sets forth a general broad clause (§ 3(1) UWG) prohibiting unfair commercial practices (i) among companies in business-to-business relations; (ii) from non-business entities (such as non-governmental organisations); and (iii) with respect to consumers in business-to-consumer relations.[817] In addition § 3(2) UWG establishes a second general clause specifically for the protection of consumers, in the sense harmonised under Article 5(2) of the Unfair Commercial Practices Directive.[818] Both gen-

814 Ansgar Ohly 2014 (n 100) 10.

815 Chapter 6 § 1 A) II. 1. a) cc).

816 See § I UWG: "This Act shall serve the purpose of protecting competitors, consumers and other market participants against unfair commercial practices. At the same time, it shall protect the interests of the public in undistorted competition; " Ansgar Ohly, 'Unfair Competition', *Max Planck Encyclopaedia of European Private Law* (OUP 2012) 1172; Frauke Henning-Bodewig, 'A New Act Against Unfair Competition IIC [2005] 421, 423 stating that: "Originally, the UWG only served the interest of "honest competitors", and thus, to use modern terminology, a "B2B" regulation" and concluding that with time public interest and consumer protection were also recognised as "being of equal importance".

817 Ohly/*Sosnitza* (n 813) § 3 Rdn 6-7.

818 Ohly/*Sosnitza* (n 813) § 3 Rdn 69; Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council [2005] OJ L149/22 (Unfair Commercial Practices Directive).

eral clauses are drafted in a flexible manner so as to allow a broad construction of the "unfair commercial practices" notion, which inevitably entails a certain degree of legal uncertainty.[819] To some extent, this uncertainty is narrowed down by the inclusion of a number of examples of unfair commercial practices with regard to competitors in § 4 UWG and with respect to consumers in § 4a UWG (aggressive commercial practices), § 5 UWG (misleading commercial practices) and § 5a UWG (misleading by omission).[820]

For the purposes of this research, §§ 17 and 18 UWG set out criminal liability in the event of unauthorised communication, acquisition, securing or exploitation of trade secrets, which furthermore trigger civil liability as acts of unfair competition. Drawing on these provisions, § 19 UWG provides that abetting to commit the offences therein established shall also be penalised.[821] This regulation is rather uncommon in view of the systems implemented in other European jurisdictions, where criminal law sanctions and unfair competition remedies are regulated in separate statutes.[822] However, in Germany, the criminal law regime was considered the most appropriate system to protect trade secrets mainly for two reasons, namely: (i) the special vulnerability of trade secrets ("*die besondere Verletzlichkeit*"), and (ii) the difficulty of obtaining appropriate and effective remedies in law.[823] The approach adopted by the German legislature when regulating trade secrets protection demands conditional intent to trigger not only criminal liability, but also civil liability, which is a much higher standard than the one introduced by the TSD (and differs from the applicable gross negligence standard in the U.S. and footnote 10 TRIPs). Accordingly, the two-fold nature of the provisions regulating trade secrets protection in the UWG is likely to be reviewed with the implementation of the TSD.[824]

---

819 Ansgar Ohly 2014 (n 98) 541.

820 Ansgar Ohly 2014 (n 98) 541.

821 Natalie Ackermann-Blome and Joanna Rindell, 'Should trade secrets be protected by private and/or criminal law? A comparison between Finnish and German laws' [2018] 13 JIPLP 78, 78.

822 Hogan Lovells 2012 (n 793) 251, according to which only Austria, Poland and Romania have adopted a similar approach.

823 Henning Harte-Bavendamm, '§ 77 Schutz von Geschäfts- und Betriebsgeheimnissen (§§ 17-19 UWG)' in Michale Loschelderr and Willi Erdmann (eds), *Wettbewerbsrecht* (4th edn, C.H. Beck 2010) § 77 Rdn 3.

824 Mary-Rose McGuire, 'Der Schutz von Know-how im System des Immaterialgüterrechts' [2016] GRUR 1000, 1002; Natalie Ackermann-Blome and Joanna Rindell (n 821) 86; the proposed Trade Secrets Act deletes §§ 17-19 UWG and

Throughout the next sections, the main provisions that regulate trade secrets protection under the two-fold unfair competition and criminal law regime are studied.

1. § 17 UWG Trade secrets disclosure

As already stated, the core regulation of trade secrets protection in Germany is built upon § 17 UWG, which provides the following:

(1) Whoever as the employee of a business communicates, without authorisation, a trade or industrial secret with which he was entrusted, or to which he had access, during the course of the employment relationship to another person for the purposes of competition, for personal gain, for the benefit of a third party, or with the intent of causing damage to the owner of the business shall be liable to imprisonment not exceeding three years or to a fine.

(2) Whoever for the purposes of competition, for personal gain, for the benefit of a third party, or with the intent of causing damage to the owner of the business, acquires or secures, without authorisation,
   1. a trade or industrial secret
   a) by using technical means;
   b) by creating an embodied communication of the secret; or
   c) by removing an item in which the secret is embodied;
   or
   2. without authorisation, uses or communicates to anyone a trade secret which he acquired through one of the communications referred to in subsection (1), or through an act of his own or of a third party pursuant to number 1, or which he has otherwise acquired or secured without authorization shall incur the same liability.[825]

In essence, § 17 identifies three types of conduct as criminal offences, *i.e.* (i) the unauthorised disclosure of trade secrets by an employee; (ii) the unauthorised procurement (acquisition) or securing of trade secrets by any third party; and (iii) the unauthorised exploitation or communication of the information obtained. Each of these is analysed in turn.

---

adopts a gross negligence standard with respect to civil liability. However, it still contains criminal provisions.

825 English Translation extracted from <http://www.gesetze-im-internet.de/englisch_uwg/englisch_uwg.html#p0139> accessed 15 September 2018.

a) Unauthorised trade secret disclosure in the course of employment

Section 17(1) UWG proscribes the unauthorised disclosure of trade secrets in the course of employment. The essential feature of the behaviour described in this provision is that it can exclusively be carried out by a person in an employment relationship with the company.[826]

The term employed person ("*beschäftigte Person*") refers not only to employees ("*Angestellter*"), but also to workers ("*Arbeiter*") and apprentices ("*Lehrlinge*").[827] In fact, the courts have construed this expression in a wide sense, so as to include not only business executives and members of the board,[828] but also unskilled workers, such as trainees, cleaning staff and messengers.[829] The driving factor is that the infringer learnt about the secret information as a result of his relationship with the company.[830] His qualification, the salary that he receives or the type of tasks that he performs are irrelevant for the purposes of this provision.[831] Thus, partners and shareholders are deemed to fall outside the scope of § 17(1) UWG if they do not have a direct relationship with the undertaking.[832] Crucially, there must be causality between the obtention of the trade secret and the employment relationship. In this context, the decisive factor is whether the information could have been acquired outside of the employment relationship.[833]

The object of protection of § 17(1) UWG is a commercial or industrial secret that was entrusted to the employee, or that became known to him by reason of his employment relationship.[834] In particular, a secret is deemed to have been entrusted ("*anvertraut*") when it is conveyed to the employee under an explicit obligation of confidentiality or when such an

826 *Ohly*/Sosnitza (n 813) § 17 Rdn 13.
827 *Ohly*/Sosnitza (n 813) § 17 Rdn 13.
828 *Ohly*/Sosnitza (n 813) § 17 Rdn 13; Richard Schlötter, *Der Schutz von Betriebs- und Geschäftsgeheimnissen und die Abwerbung von Arbeitnehmern* (Carl Heymanns Verlag 1997) 144-145.
829 Henning Harte-Bavendamm 2010 (n 823) § 77 Rdn 18.
830 *Ohly*/Sosnitza (n 813) § 17 Rdn 13.
831 Rudolf Kraßer, 'Der Schutz des Know-how nach deutschem Recht' [1970] GRUR 587, 591; Henning Harte-Bavendamm (n 823) § 77 Rdn 18.
832 *Ohly*/Sosnitza (n 813) § 17 Rdn 13.
833 Richard Schlötter 1997 (n 828) 145-146; Gintare Surblyte 2011 (n 182) 57.
834 Michael Knospe, 'Germany' 62 in Melvine F. Jager (ed), *Trade secrets throught the world* (2012 Thomsom West) 15:12.

obligation can be inferred from the specific circumstances of the case.[835] Similarly, access ("*zugänglich geworden ist*") to undisclosed information during the performance of work activity also gives rise to confidentiality obligations.[836] Furthermore, the employee is bound not to disclose the information developed by him in the course of his employment relationship.[837] This is particularly relevant with regard to inventions, as follows from the Act on Employee Inventions ("*Arbeitnehmererfindungsgesetz*").[838] Specifically, § 24 of this statute sets forth a general presumption, whereby the ownership of the invention is vested on the undertaking instead of the employee, irrespective of whether the former had actual knowledge of its existence.[839]

As regards the scope of the liable conduct, it includes the *unauthorised communication* of the trade secret to anyone when carried out for at least one of the following purposes ("*Absicht*"): (i) for competitive purposes; (ii) for personal gain, (iii) for the benefit of a third party, or (iv) with the intention of causing damage to the enterprise or its owner.[840]

Case law has interpreted that the act of communication ("*Mitteilung*") covers any disclosure that makes trade secrets available to any third parties.[841] However, § 17(1) UWG does not require the recipient to have acquired active knowledge of the information, as the mere possibility of accessing it is regarded as sufficient.[842] As such, the disclosure can be carried out either orally or in a written form.[843] Likewise, pursuant to § 13 of the

---

835 *Köhler*/Bornkamm/Feddersen, *Gesetz gegen den unlauteren Wettbewerb* (36 edn, C. H. Beck 2018) § 17 Rdn 51.

836 *Ohly*/Sosnitza (n 813) § 17 Rdn 14; Henning Harte-Bavendamm 2010 (n 823) § 77 Rdn 19.

837 Henning Harte-Bavendamm 2010 (n 823) § 77 Rdn 19.
Ohly/Sosnitza (n 813) § 17 Rdn 14.

838 Gesetz über Arbeitnehmererfindungen in der im Bundesgesetzblatt Teil III, Gliederungsnummer 422-1,
veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 7 des Gesetzes vom 31. Juli 2009 (BGBl. I S. 2521)
geändert worden ist (Act on Employee Inventions).

839 Michael Knospe (n 834) 15:17; BGH GRUR 1977, 539, 540–*Prozessrechner;* see further § 24 of the Act on Employee Inventions.

840 Michael Knospe (n 834) 15:17; *Harte-Bavendamm*/Henning-Bodewig (n 376) § 17 Rdn 14-17.

841 *Ohly*/Sosnitza (n 813) § 17 Rdn 15; *Köhler*/Bornkamm/Feddersen (n 835) § 17 Rdn 19; Harte-Bavendamm (n 823) § 77 Rdn § 21.

842 *Köhler*/Bornkamm/Feddersen (n 835) § 17 Rdn 28.

843 *Ohly*/Sosnitza (n 813) § 17 Rdn 15; *Köhler*/Bornkamm/Feddersen (n 835) § 17 Rdn 19; Henning Harte-Bavendamm 2010 (n 823) § 77 Rdn 21.

German Criminal Code,[844] an omission that leads to the disclosure of a trade secret may also be penalised under § 17(1) UWG, but only if the offender is in a guarantor position.[845] In that regard, it is worth noting that the recipient of the information can be anyone that it is not acquainted with the secret, such as competitors or colleagues of the infringer.

The act of communication carried out by the employee must be unauthorised ("*unbefugt*"), that is, contrary to an obligation of confidentiality.[846] Notwithstanding this, courts have ruled that such a disclosure might not trigger criminal liability when a ground of justification exists.[847]

Likewise, in its criminal law dimension, § 17(1) UWG requires that the secret is intentionally disclosed and that the infringer has actual knowledge of the secret nature of the information. Although negligent activity does not qualify for a relevant disclosure pursuant to § 17(1) UWG,[848] it has been generally accepted that conditional intent ("*Bedingter Vorsatz*") suffices with regard to all of the objective elements of the actus reus.[849] In the same vein, a mere attempt is also subject to criminal liability pursuant to § 17(3) UWG.[850]

In order to trigger liability, the act of communication must have been completed during the term of the infringer's employment. Accordingly, the disclosure of secret information after termination of the employment relationship can only give rise to an action for a breach of contractual obligations or an offence under paragraph 2 of § 17(2) UWG.[851] The rationale behind this provision is to promote labour mobility and this is examined in greater detail in chapter 6.[852]

---

844 Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 1 des Gesetzes vom 30. Oktober 2017 (BGBl. I S. 3618) geändert worden ist (StGB or German Criminal Code).

845 *Ohly*/Sosnitza (n 813) § 17 Rdn 15.

846 *Köhler*/Bornkamm/Feddersen (n 835) § 17 Rdn 21.

847 Typical examples of justification grounds include Einwillung (§ 138 StGB), Aussagepflicht (§ 38I Nr 6); Rechfertigender Notstand (§ 34 StGB); Notwehr (§ 32 StGB) and Selbdthilfe (§ 229 BGB); as noted by *Köhler*/Bornkamm/Feddersen (n 835) § 17 Rdn 21-21a,

848 Michael Knospe (n 834) 15:52.

849 Gerhard Janssen and Gabriele Maluga, '§ 17 Verrat von Geschäfts- und Betriebsgeheimnissen' in Wolfgang Joecks and Klaus Miebach (eds), *Münchener Kommentar zum StGB* (1st edn, C.H. Beck 2010); *Harte-Bavendamm*/Henning-Bodewig (n 376) § 17 Rdn 13.

850 Axel Beater (n 811) § 22 Rdn 1885.

851 *Ohly*/Sosnitza (n 813) § 17 Rn 15-16; *Köhler*/Bornkamm/Feddersen (n 835) § 17 Rdn 22.

852 Axel Beater (n 811) § 22 Rdn 1885.

In sum, it appears that the scope of § 17(1) UWG is limited to the protection of trade secret holders from the unauthorised disclosure of confidential information by their employees during the course of their labour relationship. However, the UWG in subsequent provisions expands the scope of protection afforded to trade secrets. In particular, the following section examines the legal framework set forth with regard to so-called "industrial espionage".

b) Industrial espionage

The German trade secrets legal regime draws on the roots of the special vulnerability of confidential information against acts of industrial espionage.[853] Under the current legislation, this unlawful behaviour is captured in paragraph 1 of § 17(2) UWG. Pursuant to this provision, the unauthorised procurement ("*sich verschaffen*") or securement ("*sichern*") of a trade secret triggers criminal liability if it is carried out through (i) the use of technical devices or means; (ii) the physical reproduction of the secret information; or (iii) the misappropriation of the object in which the confidential information is incorporated.

One of the distinguishing features of paragraph 1 of § 17(2) UWG is that the unlawful conduct described therein can be carried out by any person (not only employees, unlike § 17(1) UWG).[854]

However, the actus reus is limited to the unauthorised procurement and securement of trade secrets. The former consists of the acquisition of secret information. Hence, if the trade secret is embodied in a given object, its procurement requires obtaining possession of the said item (e.g. a CD containing confidential information).[855] By contrast, if the trade secret is not embodied in any object, its procurement arises from the mere acquisition of the information that constitutes the trade secret. For instance, this would be the case if the infringer memorised the chemical formula used to manufacture a pharmaceutical product. An act of securement takes place when the infringer incorporates secret information in a permanent form; among others, through recording or scanning the data.[856] Yet, often establishing the exact boundaries between these concepts appears rather implau-

853 *Harte-Bavendamm*/Henning-Bodewig (n 376) §§ 17-19 Rdn 6.
854 *Harte-Bavendamm*/Henning-Bodewig (n 376) § 17 Rdn 43.
855 *Ohly*/Sosnitza (n 813) § 17 Rdn 17; Richard Schlötter 1997 (n 828) 156-157.
856 *Ohly*/Sosnitza (n 813) § 17 Rdn 18.

sible, as some acts encompass both types of conduct simultaneously.[857] By way of illustration, this would be the case if the infringer acquired a CD with secret data (procurement), made a copy of the confidential information on his personal desktop and sent it through his private e-mail account to a third party (securement).[858]

The conduct referred to above must be carried out by at least one of the improper means described in paragraph 1 of § 17(2) UWG. If the trade secret is acquired in any other way, the conduct falls outside the scope of this provision.[859] As such, it is regarded that paragraph 1 of § 17(2) UWG identifies and penalises three types of behaviours that constitute a particularly dangerous form of espionage, irrespective of whether the acquired confidential information is subsequently used or disclosed.[860]

The first of the improper means described in paragraph 1 of § 17(2) refers to the procurement or securement of information through "technical means". Case law has construed these terms in a wide sense, so as to include all devices that can be used for such purposes;[861] for example, photographic and recording cameras, as well as the use of computers or other devices to decompile and analyse secret information.[862]

Secondly, the "physical reproduction of the secret information" also constitutes one of the unlawful means of acquiring a trade secret pursuant to paragraph 1 § 17(2) UWG. This provision refers to the reproduction of the trade secret and typically occurs when the infringer makes a photocopy or builds a replica of a machine.[863]

Finally, paragraph 1 of § 17(2) UWG prevents the "misappropriation of an object or device incorporating the secret". This provision refers to the unauthorised acquisition of the item in which the trade secret is embodied, and it includes all actions that allow the infringer to possess the object and use it or allow its use by a given third party.[864] Among others, courts

857 *Ohly*/Sosnitza (n 813) § 17 Rdn 18.
858 *Ohly*/Sosnitza (n 813) § 17 Rdn 18.
859 *Ohly*/Sosnitza (n 813) § 17 Rdn 19.
860 *Harte-Bavendamm*/Henning-Bodewig (n 376) § 17 Rdn 43; Thomas Hören und Reiner Münkner, 'Die neue EU-Richtlinie zum Schutz von Betriebsgeheimnissen und die Haftung Dritter' [2018] CCZ 85, 85.
861 *Harte-Bavendamm*/Henning-Bodewig (n 376) § 17 Rdn 44.
862 *Harte-Bavendamm*/Henning-Bodewig (n 376) § 17 Rdn 44.
863 *Ohly*/Sosnitza (n 813) § 17 Rdn 19.
864 *Ohly*/Sosnitza (n 813) § 17 Rdn 19; *Harte-Bavendamm*/Henning-Bodewig (n 376) § 17 Rdn 44.

have held that the misappropriation of photographs and storage devices may fall within the scope of paragraph 1 of § 17(2) UWG.[865]

As a final note, it should be stressed that in its criminal law dimension, paragraph 1 of § 17(2) UWG requires that the offender acts at least with intent ("*Vorsatz*") or conditional intent ("*Bedingter Vorsatz*").[866] The infringer must know or at least have reason to know that he had acquired or secured a trade secret under at least one of the improper means described in paragraph 1 of § 17(2) UWG and with one of the following purposes: (i) for competitive purposes; (ii) for personal gain, (iii) for the benefit of a third party, or (iv) with the intention of causing damage to the enterprise or its owner.[867] The following section, in which the general prohibition set out in paragraph 2 of § 17(2) UWG is examined, analyses in more detail the implications of demanding intent on the side of the infringer.

c) General prohibition

Finally, paragraph 2 of § 17(2) UWG sets forth a broader prohibition, whereby (i) the use or communication of a secret obtained through an unlawful disclosure from an employee pursuant to § 17(1) UWG or (ii) the unauthorised procurement or securement of confidential information by any of the means set out in paragraph 1 of § 17(2) UWG or by any other means shall trigger criminal liability. Notably, such a broad prohibition renders unlawful any unauthorised acquisition of a trade secret, if it is carried out by either an employee or a third party.[868] In this regard, it should be noted that the use of the same terminology as in the previous types of conduct but in a completely different context has been vehemently criticised.[869] This provision is particularly relevant with regard to the behaviour of former employees, as it captures the exploitation of secrets obtained by employees in an unlawful way while they were still in an employment relationship with the trade secret holder.[870]

---

865 *Ohly*/Sosnitza (n 813) § 17 Rdn 19; *Harte-Bavendamm*/Henning-Bodewig (n 376) § 17 Rdn 44.
866 Natalie Ackermann-Blome and Joanna Rindell (n 821) 82; *Ohly*/Sosnitza (n 813) § 17 Rdn 24 refers to dolus eventualis.
867 *Harte-Bavendamm*/Henning-Bodewig (n 376) § 17 Rdn 25.
868 *Harte-Bavendamm*/Henning-Bedewig (n 376) 17 Rdn 47.
869 Thomas Hören und Reiner Münkner 2018(a) (n 860) 85.
870 *Ohly*/Sosnitza (n 813) § 17 Rdn 20; *Harte-Bavendamm*/Henning-Bodewig (n 376) § 17 Rdn 44.

Crucially, due to its criminal law nature, paragraph 2 of § 17(2) UWG, just like the other relevant types of conduct analysed under § 17 UWG, restricts the liability of former employees and third parties to cases where they acted with intent ("*Vorsatz*"). Yet, positive knowledge that the information has been acquired through the means set out in § 17(1) UWG and paragraph 1 of § 17(2) UWG is not required. It is generally accepted that conditional intent suffices ("*Bedingter Vorsatz*").[871] Accordingly, if the infringer is aware that the information may have been obtained in an unlawful manner pursuant to the previous relevant types of conduct and willingly closes his eyes to it, liability will also arise with respect to indirect acquisition.[872] Crucially, the intent comprises all of the objective elements of the offence. Hence, if the infringer mistakenly believes that he is under an obligation to disclose a trade secret, no liability will arise.[873] In addition, the employee or any other third party must have disclosed the trade secret for at least one of the following purposes ("*Absicht*"): (i) for competitive purposes; (ii) for personal gain, (iii) for the benefit of a third party, or (iv) with the intention of causing damage to the enterprise or its owner.[874]

In view of this, it appears that the standard of liability set out in the UWG with respect to third parties is higher than under the TRIPs Agreement (under footnote 10 of Article 39(2)), and Article 4(4) TSD, by virtue of which gross negligence suffices.[875] Hence, the level of protection of trade secret holders against third party misappropriation is much lower than in other EU jurisdictions, such as England (or even the U.S.).

2. § 18 UWG Use of models

In the UWG of 1909 the German legislature decided to regulate in a separate provision protection against the so-called "piracy of models" (*"Vorlagenfreibeuterei"*). This amendment was introduced as a result of complaints raised by embroidery and lace manufacturers, who argued that their trade

871 Thomas Hören und Reiner Münkner 2018(a) (n 860) 85.
872 Mary-Rose McGuire, Björn Joachim, Jens Künzel and Nils Weber,'Protection of Trade Secrets through IPR and Unfair Competition Law' (2010) AIPPI Report Question Q215, 10 <http://aippi.org/wp-content/uploads/committees/215/GR215germany_en.pdf > accessed 15 September 2018.
873 *Ohly*/Sosnitza (n 813) § 17 Rdn 20; Thomas Hören und Reiner Münkner 2018(a) (n 860) 85.
874 *Harte-Bavendamm*/Henning-Bodewig (n 376) § 17 Rdn 14-17.
875 Rudolf Rudolf Kraßer 1996 (n 585) 224.

secrets were being revealed through the unlawful use of their templates and models.[876] In its current wording, § 18 UWG provides the following:

> § 18 UWG Use of models
> (1) Whoever, acting without authorisation, uses or communicates to another person models or instructions of a technical nature, particularly drawings, prototypes, patterns, segments or formulas, entrusted to him for the purposes of competition or for personal gain shall be liable to imprisonment not exceeding two years or to a fine.
> (2) An attempt shall incur criminal liability.
> (3) The offence shall be prosecuted upon application only, unless the criminal prosecution authority considers that it is necessary to take *ex officio* action on account of the particular public interest in the criminal prosecution.
> (4) Section 5, number 7, of the Criminal Code shall apply *mutatis mutandis*.[877]

Nowadays, this provision aims at protecting technical knowledge that is supplied by the trade secret holder in the context of know-how agreements or during the negotiation of other kinds of contracts.[878] However, its scope of application is limited to two specific kinds of industrial secrets, i.e. models ("*Vorlagen*") and technical instructions ("*Vorschriften technischer Art*"). The former refer to means that are used as prototypes for the production of new items or the delivery of new services, subject to fixation.[879] The latter include the commands and teachings that must be followed in the implementation of technical processes.[880] Segments and formulas, as well as computer programs are often cited by academia and case law as paradigmatic examples of instructions of a technical nature in the sense of § 18 (UWG).[881]

---

876 *Ohly*/Sosnitza (n 813) § 18 Rn 2.

877 Translation obtained from the German Ministry of Justice website <http://www.gesetze-im-internet.de/englisch_uwg/englisch_uwg.html#UWGengl_000P17> accessed 15 September 2018.

878 *Harte-Bavendamm*/Henning-Bodewig (n 376) § 18 Rdn 55.

879 *Köhler*/Bornkamm/Feddersen (n 835) § 18 Rdn 9 stating that: "Vorlagen sind Mitteln, die als Grundlage oder Vorbild für die Herstellung von neuen Sachen oder Dienstungen dinen sollen"; Köhler further notes that the Models ("*Vorlagen*") can be fixated either in a particular embodiment (an exemplary) or in an abstract depiction (such as a description or representation).

880 *Köhler*/Bornkamm/Feddersen (n 835) § 18 Rdn 10.

881 *Ohly*/Sosnitza (n 813) § 18 Rdn 5.

The actus reus consists of the unauthorised communication of models and technical instructions that were entrusted to the infringer in the course of trade for the purposes of hindering competition or for a personal gain.[882]

Case law has again construed the term entrusted ("*anvertraut*") in a wide sense. It includes all the models and technical instructions that the trade secret holder conveyed to another undertaking under an obligation of confidentiality (express or implied from the specific circumstances of the case).[883] However, it is essential that the trade secret was communicated to the confidant with the sole purpose of it being used in the interest of the holder.[884]

Finally, it is necessary that the secret information is conveyed in the course of trade ("*im geschäftlichen Verkehr*") in order to be protected pursuant to § 18 UWG. The limited scope of application of this provision has been criticised by a number of commentators, who regard that it is out of date in the digital world and, consequently, it will most likely be deleted with the implementation of the TSD in Germany.

III. Civil law

The current wording of the UWG sets forth criminal sanctions in the event that §§ 17 and 18 are infringed, but makes no reference to the civil protection afforded in such circumstances.[885] Notwithstanding this, it is generally accepted by courts and academia that trade secret holders are entitled, among other remedies, to claim damages, exercise the right of information and apply for injunctive relief.[886] In that regard, it is worth noting that since § 19 UWG was amended in 2004,[887] no general consensus exists on a

882 Axel Beater (n 811) § 22 Rdn 1887.

883 *Ohly*/Sosnitza (n 813) § 18 Rdn 6; *Köhler*/Bornkamm/Feddersen (n 835) § 18 Rdn 11.

884 *Ohly*/Sosnitza (n 813) § 18 Rdn 6.

885 *Köhler*/Bornkamm/Feddersen (n 835) § 17 Rdn 51.

886 *Harte-Bavendamm*/Henning-Bodewig (n 376) § 17 Rdn 58.

887 Before the 2004 UWG amendment, § 19 UWG set forth the right to claim damages in the event of infringement of §§ 17 and 18 UWG. Accordingly, § 19 provided that: "Violations of the provisions of Sections 17 and 18 also result in liability for damages caused thereby. Where there are several parties, they are jointly and severally liable" (translation from Michael Knospe (n 834) para § 15:32). Notwithstanding this, such a provision was deemed superfluous and was consequently deleted from the Act in the UWG reform of 2004; see in this regard

civil legal basis that triggers their applicability. As regards the available means of redress, Ohly makes a clear-cut distinction between criminal accessory claims ("*Strafrechtsakzessorische Ansprüche*") and civil autonomous claims ("*Zivilrechtsautonome Ansprüche*").[888] The former only arise if the objective elements of the offence ("*objektiver Tatbestand*") and the mens rea or subjective elements of the offence ("*subjektiver Tatbestand*") described in §§ 17 and 18 UWG are carried out by the infringer. The latter, on the other hand, can be claimed irrespective of any finding of criminal liability.[889] In the following section, for the purposes of clarity, the different legal mechanisms available to enforce trade secrets protection in the civil jurisdiction are outlined in accordance with Ohly's classification, with the aim of providing a better and clearer understanding of the legal issues surrounding the enforcement of trade secrets in Germany.

1. Criminal accessory claims

Despite the lack of statutory provisions dealing with the enforcement of trade secrets, as stated above, case law provides that any violation of §§ 17 and 18 UWG may trigger claims both for damages and injunctive relief. Hence, in order to award damages, courts resort to the general clause of 823 II BGB, which provides that a duty of compensation arises if a breach of statute intended to protect another person is found.[890] Likewise, injunctive relief is usually granted in accordance with Article 1004 BGB, pursuant to which the possibility of obtaining an injunction if an interference with a property right occurs is established.[891]

Ohly/Sosnitza (n 813) § 17 Rdn 35; *Köhler*/Bornkamm/Feddersen (n 1299) § 17 Rdn 52.

888 For a more detailed analysis see Ansgar Ohly 2014 (n 13) 7-11.

889 Ansgar Ohly 2014 (n 13) 12.

890 § 823BGB Liability in damages: "(1) A person who, intentionally or negligently, unlawfully injures the life, body, health, freedom, property or another right of another person is liable to make compensation to the other party for the damage arising from this.(2) The same duty is held by a person who commits a breach of a statute that is intended to protect another person. If, according to the contents of the statute, it may also be breached without fault, then liability to compensation only exists in the case of fault" (translation obtained from the German Ministry of Justice website <http://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html#> accessed 15 Sepember 2018).

891 § 1004 BGB – Claim for removal and injunction: "(1) If the ownership is interfered with by means other than removal or retention of possession, the owner

Against this background, an infringement of a trade secret pursuant to § 17 and § 18 UWG is regarded as a breach of § 3a UWG, by virtue of which "the breach of a statutory provision that is also intended to regulate market behaviour in the interest of market participants if the infringement affect the interests of consumers, other entrants or competitor shall be deemed unfair". In the light of the above, a violation of §§ 17 or 18 UWG is deemed to contravene the general prohibition of unfair commercial practices set forth in § 3 I UWG through the application of § 3a UWG.[892] Based on § 3 I UWG, the trade secret holder is entitled to claim the remedies set forth in chapter 2 of the UWG, namely elimination and injunctive relief (§ 8 UWG);[893] compensation for damages (§ 9 UWG); and confiscation of profits (§ 10 UWG). Nonetheless, such a possibility has been highly contested by some commentators on the basis that the behaviours described in §§ 17 and 18 UWG cannot be understood as a provision regulating market behaviour. In particular, it has been argued that IPRs do not fall under such a category, as indeed they are meant to protect individual rights.[894]

---

may require the disturber to remove the interference. If further interferences are to be feared, the owner may seek a prohibitory injunction" (translation obtained from the German Ministry of Justice website <http://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html#> accessed 15 Sepember 2018).

892 *Ohly*/Sosnitza (n 813) § 17 UWG Rdn 44; Franz Hofmann, '"Equity" im deutschen Lauterkeitsrecht? Der "Unterlassungsanspruch" nach der Geschäftsgeheimnis-RL' [2018] WRP 1, 3 para 10.

893 BGH GRUR 1964, 31 – *Petromax II.*

894 Against this background, Wolfgang Schaffert, '4 Nr 11' Rdn 68 in Peter W. Heermann and others (eds), *Münchener Kommentar zum Lauterkeitsrecht* (1st edn, C.H. Beck 2006) argues that exclusive rights and particularly §§ 17-18 UWG do not intended to regulate competition in the market through the establishment of the equal barriers and the creation of equal opportunities among competitors. Contrariwise, he concludes that such provisions do not establish any market behaviour rules ("*Marketverhaltungsregeln*") in the interest of consumers and thus, fall outside the scope of § 3a UWG. As such, the infringement of the above- mentioned provisions cannot be regarded as anticompetitive if it systematically leads to a competitive advantage; the opposite view is held by Ohly 2014 (n 13) 12, who notes that the behaviours described in the UWG provisions that regulate trade secret protection, i.e. §§ 17-18 UWG do not take place before any market activity, as in this scenario the relevant market consists of information and not the products. Hence, he concludes that the tension between market behaviour rules and individual rights is only apparent, as he affirms that IPRs protect individual rights and at the same time establish market behaviour rules. In particular, it is stressed that IPRs determine the behaviours that are allowed in the market.

2. Civil autonomous claims

Civil autonomous claims arise irrespective of the finding of criminal liability pursuant to § 17 and § 18 UWG. Their applicability has proven extremely relevant in practice, as the UWG provisions that expressly regulate trade secrets protection only sanction wilful infringement.[895]

The most relevant civil autonomous claims refer to contractual obligations, and are applicable to the breach of know-how agreements and the use and disclosure of trade secrets by departing employees. In such a context, performance or damages can be claimed on the basis of § 280 I BGB.[896] The applicability of this provision only requires negligence ("*Leichte Fahrlässigkeit*").[897] In addition, fault is presumed in those cases where the breach of a duty is established, as per the second phrase of § 280 I BGB.[898]

Likewise, § 4(3)(c) UWG precludes the offering of goods or services that are replicas of goods or services of a competitor if he dishonestly obtained the knowledge or documents needed for the replicas. This provision may be applied in the event that the replicas embody a trade secret obtained unlawfully.[899] More generally, if not all of the liability conditions set out in §§ 17-18 UWG are fulfilled, courts may still regard that the conduct of a competitor falls under the general obstruction of competition clause set out in § 4(4) UWG, which in turn contravenes the general prohibition of unfair commercial practices set forth in § 3 I UWG and the remedies established in connection with it.[900]

As a final note, it should be pointed out that if trade secrets are regarded as the object of a property right, they shall be protected pursuant to § 823 I (damages in the event of unlawful, wilful or negligent injury of another's property), § 812 I (duty of restitution), and § 687 II (false agency without

---

895 *Ohly*/Sosnitza (n 813) § 17 Rdn 36.

896 § 280 (1) BGB sets out that: "If the obligor breaches a duty arising from the obligation, the obligee may demand damages for the damage caused thereby. This does not apply if the obligor is not responsible for the breach of duty"; (translation obtained from the German Ministry of Justice website <http://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html#p0841> accessed 15 September 2018).

897 *Ohly*/Sosnitza (n 813) § 17 Rdn 43.

898 *Ohly*/Sosnitza (n 813) § 17 Rdn 43.

899 Ansgar Ohly 2014 (n 13) 12.

900 *Köhler*/Bornkamm/Feddersen (n 1299) § 17 Rdn 52.

specific authorisation) BGB.[901] However, this remains highly contested, as no consensus on the legal nature of trade secrets in Germany exists.[902]

§ 3 *Trade Secrets Protection in England before the implementation of the TSD – The law of confidentiality*

The analysis of the law of confidentiality should start by noting that in the UK three different jurisdictions coexist, namely (i) England and Wales; (ii) Northern Ireland; and (iii) Scotland. The first two are common law jurisdictions, while the law in Scotland has a hybrid nature, as it draws both from common law and Roman law origins.[903] As regards trade secrets, the England and Wales jurisdiction has the most developed body of case law and will be used as the case of study in this dissertation. In fact, judicial review regards that the law of confidentiality in Northern Ireland and Scotland is very similar to the law in England and Wales, even though the Scottish system is viewed as being less developed.[904]

In England, trade secrets protection is mostly achieved through contractual provisions and the breach of confidence action, which protects confidential information in general.[905] Notably, trade secrets are protected through the same action that covers other kinds of confidential information, such as artistic and literary information, government secrets[906] and private information,[907] without distinction by subject.[908]

Unlike most civil law countries and the U.S., in England no specific provisions dealing with the protection of trade secrets have been enacted into law.[909] Remarkably, the English legal regime does not contain criminal law provisions penalising industrial espionage,[910] the most common form

901 Ansgar Ohly 2014 (n 100) 3.
902 See chapter 1 § 3 B) 3. b).
903 Hogan Lovells 2012 (n 793) paras 240-241.
904 Hogan Lovells 2012 (n 793) paras 241.
905 Tanya Aplin and others 2012 (n 22) para 1.01.
906 *Attorney General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109 (HL).
907 *Campbell v MGN Ltd* [2004] 2 AC 457 (HL).
908 William Cornish, David Llewellyn and Tanya Aplin 2013 (n 209) para 8-07.
909 In the Law Commission 1981 (n 327) 101 it was argued in favour of establishing a statutory action for breach of confidence in the interests of clarity and legal certainty.
910 The Law Commission published a Discussion Paper (Law Commission, *Legislating the Criminal Code: Misuese of Trade Secrets* (Law Com No 150, 1997)) arguing in favour of the establishment of a criminal liability regime for the deliberate

of trade secrets protection found in other jurisdictions. Consequently, criminal liability for the misappropriation of trade secrets is covered by other offences, such as conspiracy to defraud or theft (but only with regard to a physical object in which a trade secret is embodied).[911] It is a well-established principle that "there is no confidence as to the disclosure of inequity".[912]

The breach of confidence action has considerable breadth, as it "enables any person who has an interest in information that is confidential to prevent others who have received, or acquired the information with notice of its confidential quality from using or disclosing the information".[913]

Case law has set forth that information must present three elements in order to be protected.[914] First, it must entail the quality of confidence. Second, it must have been disclosed in circumstances implying an obligation of confidence. Third, an unauthorised use of the information detrimental to the owner of the information must have taken place.[915]

The following sections delve into the protection of trade secrets in England and Wales under the legal framework created by the breach of confidence action, with the aim of providing a better understanding of the notion of confidentiality. To this end, first section A introduces a number of preliminary remarks regarding the withdrawal of the UK from the EU and its effects on the trade secrets legal regime. Thereafter, section B examines the development of the action since the mid-XIX century, while section C analyses the four causes of action that have traditionally been invoked in cases of breach of confidence and the applicable liability requirements.

---

misuse of trade secrets, but this proposal was never passed; see further Carl Steele and Anthony Trenton, 'Trade secrets: the need for criminal liability' [1998] 20 EIPR 188-192.

911 William Cornish, David Llewellyn and Tanya Aplin 2013 (n 209) para 8-55; Lionel Bently and Brad Sherman 2014 (n 125) 1197; Allison Coleman, *The Legal Protection of Trade Secrets* (Sweet&Maxwell 1992) Chapter 7; pursuant to the Theft Act 1968, s 1 "theft", is the "dishonest appropriation *of property* belonging to another with the intention of permanently deriving the other of it". In turn, s 4 establishes that property also refers to "intangible property". However, a substantial number of cases have stated that information does not fall under the category of "intangible property".

912 Law Commission Report 1997 (n 910) 59, citing *Garstide v Outram* [1857] 26 LJ Ch 113.

913 Tanya Aplin and others 2012 (n 22) para 1.01.

914 The three elements that constitute the breach of confidence action were first established in *Coco v. A.N.Clark (Engineers) Ltd* [1969] RPC 41 (Ch), 46.

915 *Coco v A.N.Clark (Engineers) Ltd* [1969] RPC 41 (Ch), 48.

A) A note on Brexit

On June 23, 2016, 51,9% of the electorate in the UK voted in favour of leaving the EU, following a referendum called for by the European Union Referendum Act of 2015.[916] The results of the referendum were confirmed by the Parliament of the UK in both of its Houses, leading to the adoption of the European Union Notification of Withdrawal Bill.[917] Consequently, on March 29, 2017 the UK Government notified the European Council about its decision to abandon the EU (popularly referred to as "Brexit"), in accordance with the procedure set out in Article 50(2) TUE.[918] At this stage, the European Council and the UK are still in the process of negotiating the terms of the Withdrawal Agreement, which will establish the specific date after which the EU Treaties and secondary legislation of the EU will no longer be applicable in the UK and will also govern the relationship between the parties after that date. In the absence of such an agreement and pursuant to Article 50(3) TEU, the EU legal system will cease to apply two years after the withdrawal notification date (29 March 2019).

Despite the imminent withdrawal of the UK from the EU, the United Kingdom Intellectual Property Office ("UKIPO") has launched a consultation, which includes a proposal to implement the Directive.[919] Irrespective of the outcome of the consultation, the UK played a fundamental role during the negotiation of the TSD, mostly due to the sophisticated and diverse body of case law developed by English courts that allowed stakeholders to achieve an effective level of protection against trade secrets misappropriation. Therefore, the study of the English model in the context of the TSD remains relevant for the purposes of the present research, even after the withdrawal of the UK from the EU.

---

916 European Union Referendum Act 2015 (c. 36)

917 European Union Notification of Withrawal Bill 2017.

918 According to the UK notification under Article 50 TEU dated 29 March 2017 <http://data.consilium.europa.eu/doc/document/XT-20001-2017-INIT/en/pdf> accessed 15 September 2018.

919 According to Will Smith and Robert Williams, 'Brexit and the Trade Secrets Directive - the Clock is Ticking (16 October 2017) <https://www.twobirds.com/en/news/articles/2017/uk/brexit-and-the-trade-secrets-directive-the-clock-is-ticking> accessed 15 September 2018.

B) Development of the law of confidentiality

The origin of the breach of confidence action has often been described as "obscure". Until the early XIX century, the protection of confidentiality was articulated through an array of legal doctrines established in contract law, employment law, criminal law, copyright law and patent law, as well as in the law of inheritance.[920] The basis for the existing breach of confidence action was not settled until the mid-XIX century through two landmark cases: *Prince Albert v Strange*[921] and *Morison v Moat*.[922] These decisions set out the core principles upon which the current breach of confidence action is built, as outlined below.

In the first ruling, the plaintiff obtained an injunction preventing the publication of a catalogue of etchings made by Prince Albert and Queen Victoria for their amusement and private use. The defendant was an employee of the printer in Windsor where the etchings were printed. He decided to make additional copies and compile them in a catalogue, without authorisation from Prince Albert and Queen Victoria. In its ruling, the court stated that the plaintiff had a property right in the etchings and was therefore entitled to exclude the defendant "against the invasion of such right". Notwithstanding this, the most significant contribution of the decision was the finding that a duty of confidence might exist separately from a contractual obligation.[923]

In *Morison v Moat,*[924] the plaintiffs were granted an injunction to prevent the use of a secret recipe to manufacture a cure-all medicine called "Morison's Universal Medicine". The inventor, the plaintiff's father (James Morison), had entered into a partnership with the defendant's father, Thomas Moat, to exploit the invention, under the condition that he did not disclose it. Shortly before his death, Thomas Moat revealed the secret to his son, Horatio Moat, who started producing and marketing the medicine on his own account. As a result, the plaintiffs sought an injunction to restrain such marketing activities. The High Court of Chancery granted the injunction and held that Thomas Moat must have revealed the secret recipe to his son in breach of the contract (and confidence) or he

920 Tanya Aplin and others 2012 (n 22) para 2.02.
921 *Prince Albert v Strange* [1849] 2 De G & Sm 652.
922 *Morison v Moat* [1851] 9 Hare 241.
923 In *Prince Albert v Strange* [1849] 2 De G & Sm 652; ER 293; 1 Mac & G 25, 44 the Court stated that: "a breach of trust, confidence or contract would of itself entitle the plaintiff to an injunction".
924 *Morison v Moat* [1851] 9 Hare 241.

must had acquired it "surreptitiously". Notably, *Morison v. Moat* is regarded as the first authority where "the liability for third-party recipients of trade secrets" was established.[925]

In the mid-XX century, the English courts established a broader equitable jurisdiction, on the basis of good faith rather than property and contract.[926] In *Saltman Engineering v Campbell Engineering* the court stated that "the obligation to respect confidence is not limited to cases where the parties are in contractual relationship".[927] Instead, the court found an implied duty of confidentiality, whereby an obligation of confidence may stem from a relationship where information is imparted under certain circumstances and without a contract.[928]

Despite the recent developments, many aspects of the breach of confidence action remain open, such as the jurisdictional basis and the liability of innocent acquirers. Likewise, the rise of new technologies, such as Artificial Intelligence and Big Data, poses additional challenges that courts will have to address in the near future. The following section analyses the legal regime for the protection of confidential information under the breach of confidence action in England.

C) Legal regime for the protection of confidential information under the breach of confidence action

I. Jurisdictional basis for the action

The legal nature and scope of the breach of confidence action has been the object of debate by scholars and case law, and hitherto no consensus exists on this matter.[929]

On the one hand, it has been argued that there is no single concept that clarifies or comprises all of the causes of action for what has traditionally

925 Tanya Aplin and others 2012 (n 22) para 2.90.
926 William Cornish, David Llewellyn and Tanya Aplin 2013 (n 209) para 8-07.
927 *Saltman Engineering v Campell Engineering* [1948] 65 RPC 203 (CA), 211.
928 Tanya Aplin and others 2012 (n 22) para 2.90; Roger M. Toulson and Charles M. Phipps 2012 (n 326) paras 1-046 - 1-050; Law Commission 1981 (n 327) para 3.11.
929 Law Commission 1981 (n 327); Gareth Jones, 'Restitution of Benefits Obtained in Breach of Another's Confidence' [1970] 86 LQR 463.

been called breach of confidence.[930] On the other hand, more recently, it has been suggested that the said action is of a sui generis nature and, as such, does not fall strictly under one conventional category.[931] The latter view became increasingly popular during the negotiation of the TSD in the light of the new obligations set forth by its implementation.[932]

Courts have mostly relied on four different causes of action, (predominantly contract, equity and to a lesser extent tort and property) to decide on an alleged breach of confidence case.[933] In the light of the above, the following sub-sections intend to provide an overview of the doctrinal grounds of the action.

1. Contract

Courts have extensively invoked contractual obligations in order to protect confidential information, on the basis of both express and implied terms of a contract.[934]

The main issues raised by the enforcement of express terms relate to post-employment obligations that prevent employees from using their acquired skills and knowledge.[935] As such, these contractual provisions have often been deemed unenforceable as an "unreasonable restraint of trade".[936] In contrast, courts have stated that it is possible to infer an obligation of confidence from a contract, even though the contract is silent on

930 Roger M. Toulson and Charles M. Phipps, *Confidentiality* (2nd edn, Sweet&Maxwell 2006) 2 noting that "No single concept satisfactorily explains or encompasses all species of the action for what has traditionally been called breach of confidence".

931 Tanya Aplin and others 2012 (n 22) para 4.09

932 Lionel Bently and Brad Sherman 2014 (n 125) 1139.

933 Tanya Aplin and others 2012 (n 22) para 4.09; Allison Coleman 1992 (n 911) 37 arguing that contract is the main jurisdictional base for actions.

934 John Hull, 'The licensing of trade secrets and know-how'155, 167 in Jacques de Werra (ed), *Research Handbook in Intellectual Property Licensing* (Edward Elgar 2013) argues that the modern course of action is grounded on an equitable duty of good faith; Tanya Aplin and others 2012 (n 22) para 4.13; Allison Coleman 1992 (n 911) 38.

935 Kate Brearley and Selwyn Bloch, *Employment covenants and confidential information* (Butterworths1993) 70.

936 Allison Coleman 1992 (n 911) 41-44.

that point, if the said obligation is necessary to comply with the object of the contract.[937]

Notwithstanding this, contract law is also subject to limitations and has proven insufficient in answering questions regarding third party liability in breach of contract i.e. situations where there is a disclosure from the confidant who received the information under a duty of confidence to a third party.[938] In these cases, the protection of confidential information should be sought through equity or tort law, as contract law does not provide a legal basis to enjoin the use of the trade secret by the third party outside of the contractual relationship .[939]

2. Equity

Originally, the equitable jurisdiction[940] provided supplementary remedies in situations in which authorities or statutory law might not fully address the issue concerned or provided inequitable solutions.[941] In the mid-IVX century, the Court of Chancery was established as a new and distinct court in England,[942] with the aim of creating a body of law based on "principles of justice"[943] that afforded remedies not granted by the increasingly rigid system developed in common law courts.[944] Within this legal framework, the breach of confidence action sought to protect an "equitable right in the confidentiality of information".[945]

Nowadays, the equitable jurisdiction essentially plays two roles vis-à-vis the breach of confidence action. First, it supports the legal jurisdiction exercised by courts on the basis of contractual confidence obligations. In the

937 Tanya Aplin and others 2012 (n 22) para 4.18.
938 Tanya Aplin and others 2012 (n 22) para 4.36.
939 Tanya Aplin and others 2012 (n 22) para 4.36.
940 The Black's Law Dictionary defines 'equity,n' as "The system of law or body of principles originating in the English Court of Chancery and superseding the common and statute law (together called "law" in the narrower sense) when the two conflict" *Black's Law Dictionary* (9th edn, West Publishing 2009).
941 'equity, n', *Black's Law Dictionary* (9th edn, West Publishing 2009).
942 *Encyclopaedia Britannica*, 'Equity' <https://www.britannica.com/topic/equity> accessed 15 September 2017.
943 'equity, n', *Black's Law Dictionary* (9th edn, West Publishing 2010).
944 *Encyclopaedia Britannica*, 'Equity' <https://www.britannica.com/topic/equity> accessed 15 September 2017.
945 Andrew Burrows and David Feldman, *Oxford Principles of English Law* (2nd edn, OUP 2009) 1311.

event that courts find a breach in the contractual obligation of confidence, an injunction may be granted only on the basis of equitable conduct. Second, equity provides an additional jurisdiction to prevent breach of confidence irrespective of the existence of any legal rights, substantially expanding courts' jurisdiction on this subject.[946]

In particular, the independent equitable jurisdiction allows courts to restrain the breach of confidence in three situations where the law provides no remedy.[947] First, equity can serve to restrain parties to a confidential disclosure that are not in a contractual relationship. This may occur, for example, if one of the parties to a negotiation that ultimately broke off seeks to benefit from the disclosed information. Second, equity provides the basis for court intervention where a third party receives confidential information from a confidant in breach of his obligation of confidence. Typically, this might be the case where the recipient of the information knows that the said information was acquired in breach of an equitable or contractual obligation. Third, the equitable jurisdiction also allows for restraining third parties that have acquired information without being bound by a confidential relationship. This covers both the surreptitious acquisition of information and acquisition with knowledge of its confidential nature by any third party.[948]

Against this backdrop, it is noteworthy that from the same fact pattern both contractual and equitable obligations may arise and eventually even overlap.[949] In this scenario, courts have either applied both jurisdictions or proceeded on the equitable basis alone, at their own discretion.[950] In fact, the Supreme Court of England, in one of its latest decisions on trade secrets protection, *Vestergaard v Bestnet*,[951] relied on equity as the applicable cause of action.

3. Property

The possibility of restraining unauthorised uses of confidential information has frequently been justified on the basis of a property right.[952] How-

946 Tanya Aplin and others 2012 (n 22) para 4.38.
947 Tanya Aplin and others 2012 (n 22) paras 4.43-4.46.
948 Tanya Aplin and others 2012 (n 22) para 4.46.
949 Allison Coleman 1992 (n 911) 46-47.
950 Tanya Aplin and others 2012 (n 22) para 4.48.
951 *Vestergaard Frandsen A/S v Bestnet Europe Ltd* [2013] UKSC 31.
952 Allison Coleman 1992 (n 911) 48.

ever, this argument has been, and still is, the object of a vehement debate both by case law and the legal scholarship, and is by no means settled, as discussed in chapter 1.[953]

4. Tort[954]

In the past, tort law was frequently invoked by courts to take action for the protection of confidential information. Nowadays such a jurisdictional basis seems confined to the protection of personal privacy, pursuant to Article 8 ECHR.[955]

Indeed, as noted above,[956] one of the most remarkable features of the English breach of confidence action is that it protects a wide range of interests, and among them, the protection of personal information has given rise to a rich body of case law.[957] This is particularly relevant because under English law there is no specific legislation that explicitly recognises the right to privacy.[958]

Notwithstanding this, for years courts repeatedly rejected the creation of a general tort of privacy, as it was deemed that this fell under the scope of the competences of the Parliament.[959] Accordingly, several bills aiming at

953 A more detailed account of this topic is provided in chapter 1 § 3 B) I. 2. a).

954 'Tort,n', *Black´s Law Dictionary* (9th edn, West Publishing 2009) "A tort is a legal wrong committed upon the person or property independent of contract. It may be either (1) a direct invasion of some legal right of the individual; (2) the infraction of some public duty by which special damage accrues to the individual; or (3) a violation of some private obligation by which like damage accrues to the individual".

955 Roger M. Toulson and Charles M. Phipps 2012 (n 326) 2-017: "It is therefore right that the courts have now come to recognise explicitly that there are separate (sometimes overlapping) causes of action in contract of equity for breach of confidence and in tort for infringement of privacy".

956 See chapter 3 § 3 B).

957 Ansgar Ohly and Agnès Lucas-Schloetter, *Privacy, Property and Personality* (CUP 2005) 85.

958 Tanya Aplin, 'The future of the breach of confidence action and the protection of privacy' [2007] Oxford University Commonwealth J 137, 137 refers to the "piecemeal protection of privacy by different areas of the law".

959 See Lord Hoffman in *Campbell v MGN Limited* [2004] 2 AC 457 (HL), [14] and *Wainwright v Home Office* [2003] 3 WLR 1137 (HL); contrary, Tanya Aplin 2007 (n 958) 137 argues in favour of the establishment of a limited tort of privacy, namely misuse of private information; also Lord Nicholls in *Campbell v MGN Limited* [2004] 2 AC 457 (HL), [43].

the creation of a statutory right of privacy were debated during the second half of the XX century, even though none of them was successfully passed.[960] Instead, the effective protection of privacy was achieved through the application of existing causes of action, such as breach of confidence.[961]

The major turning point in the protection of privacy and its intersection with the breach of confidence action was the enactment of the Human Rights Act in 1998 ("HRA"), which implemented the European Convention of Human Rights.[962] Most notably, Lord Nicholls, in his minority opinion in *Campbell v MGN Ltd*,[963] argued in favour of the inclusion of the misuse of private information within the scope of the breach of confidence action as a liability tort on the basis of the new developments in the privacy right introduced by the HRA. This opinion was followed in some subsequent decisions, such as *McKennith v Ash*.[964]

By contrast, several commentators have argued in favour of establishing a separate tort for the misuse of private information, instead of including it within the already broad scope of the breach of confidence action.[965] This was also the view purported in the Law Commission Report and it remains the object of an intense debate.[966] Yet, providing a more detailed account on the law of privacy in England falls outside the scope of this study.

---

960 A number of Bills intending to provide a statutory regulation of privacy were proposed first by Lord Mancroft in 1961, Alexander Lyon in 1967, Brian Walden in 1969, William Cash in 1987 and John Browne in 1989; among the many Reports that studied the subject of privacy, two are particularly relevant: Gerald Dworkin, 'The Younger Committee Report on Privacy' [1973] 36 Modern LR 399-406 and the Law Commission 1981 (n 909).

961 Tanya Aplin 2007 (n 958) 137; Ansgar Ohly and Agnès Lucas-Schloetter 2005 (n 957) 75-77 state that there are four objections that have impeded the definition of a general right of privacy, namely: (i) the difficulty of providing a definition; (ii) whether privacy is a sufficiently distinctive and coherent value to form the basis of a corresponding coherent substantive legal right; (iii) the inherent difficulty of striking a balance between personal privacy and wider public interest values in freedom of expression; and (iv) a general right to privacy does not seem to fit well.

962 Ansgar Ohly and Agnès Lucas-Schloetter 2005 (n 957) 86 note that, "In a more recent phase of development, breach of confidence has been given a new breadth and strength in the wake of the Human Rights Act 1998 in a series of cases involving press intrusions and the disclosure of private facts"

963 *Campbell v MGN Ltd* [2004] 2 AC 457 (HL), [14].

964 *McKennitt v Ash* [2006] EWCA Civ 1714 (CA), [8].

965 Tanya Aplin and others 2012 (n 22) paras 4.114-1.117.

966 Law Commission 1981 (n 327) para 6.2; Allison Coleman 1992 (n 911) 47.

After examining the potential causes of action invoked for the protection of confidential information, it is possible to conclude that, to some degree, they overlap with the ones resorted to by German legislation and courts. Indeed, trade secrets in both jurisdictions are enforced mostly on the basis of contractual (express or implied) obligations, but also tort law. Similarly, in both jurisdictions, the debate as to the legal nature of trade secrets remains inconclusive and consequently there is uncertainty surrounding their enforcement. Yet, in Germany no correlation with the equitable jurisdiction cause of action exists.

In the light of the above analysis, the following section examines the relevant liability requirements in the form of a four-step-test, which aims to interrogate the confidential (or secret) nature of the information.

II. Liability requirements

The conditions necessary to find liability under the breach of confidence action were first established in the landmark case *Coco v A.N.Clark (Engineers) Ltd*[967] and have been repeatedly followed by subsequent case law. The relevant facts of the case and the legal reasoning are scrutinised in the following paragraphs.

In 1965, the plaintiff, Marco Paolo Coco, designed a new motorcycle, which was known among the parties as the "Coco moped". In April 1967, he entered into negotiations with the defendant, A.N. Clark (Engineers) Limited, with the aim of establishing a partnership to manufacture the vehicle. After some time and the disclosure of very precise information relating to the design of the motorbike the negotiations ultimately broke off. Shortly afterwards, the defendant learnt that A.N. Clark (Engineers) Ltd had started to produce their own motorcycle, the so-called "Scamp moped", which incorporated an engine based on the plaintiff's design. As a result, the plaintiff brought a motion for interlocutory relief on the basis of an alleged breach of confidence.

In its ruling, Megarry J set forth the requirements that trigger liability under this action:

> First, the information itself, in the words of Lord Greene, M.R. in the Saltman case (...), must "have the necessary quality of confidence about it". Secondly, that information must have been imparted in circum-

967 *Coco v A.N.Clark (Engineers) Ltd* [1969] RPC 41 (Ch).

> stances importing an obligation of confidence. Thirdly, there must be an unauthorised use of that information to the detriment of the party communicating it.[968]

The three cumulative relevant requirements described above have been followed by most of the subsequent authorities in finding a breach of confidence. They are: (i) the quality of confidence of the information; (ii) the verification of specific circumstances importing an obligation of confidence; and (iii) the existence of an unauthorised use detrimental to the party source of the communication.

In its legal reasoning, the court started by analysing the second of these requirements and concluded that the information had been conveyed in circumstances importing an implied obligation of confidence. In doing so, Megarry J developed a test according to which:

> If the circumstances are such that any *reasonable man* standing in the shoes of the recipient of the information would have realised that upon reasonable grounds the information was being given to him in confidence, then this should suffice to impose him the equitable obligation of confidence (emphasis added).[969]

Notwithstanding this, the analysis of the first requirement led the court to conclude that Mr Coco had not provided strong evidence that the information was of a confidential nature, as all of the engine components were available on the market separately. As the three conditions were deemed cumulative, the court dismissed the motion subject to the payment of 5s 0d per engine produced.

On the basis of the previous requirements, the English courts have developed a four-step test in order to assess whether information shall be protected under the breach of confidence action. The four steps are as follows:[970]

(i) Is the subject matter of the information eligible for protection under the breach of confidence action?
(ii) Does the information possess the necessary quality of confidence?
(iii) Has the information been imparted in circumstances importing an obligation of confidence?

968 *Coco v A.N.Clark (Engineers) Ltd* [1969] RPC 41 (Ch), 47.
969 *Coco v A.N.Clark (Engineers) Ltd* [1969] RPC 41 (Ch), 48.
970 As noted by John Hull in a personal communication with the author.

(iv) Has the information been disclosed in an unauthorised manner detrimental to the confider?

The following sections analyse the last three liability requirements. First, some remarks as to the quality of confidence are laid down. Section 2 then looks into the content of the obligation of confidence, while section 3 studies the types of conduct that fall within the "unauthorised use" requirement. The first step of the test, which enquires about the subject matter eligible for protection under the breach of confidence action, is examined in chapter 4.[971]

1. The quality of confidence

The quality of confidence of information is a requirement for protection under each of the jurisdictional causes of action examined under section I.[972] Yet, in the case of private information it seems that case law has emphasised that there should be a "reasonable expectation of privacy", which may trigger protection under Article 8 HRA.[973]

The general principle is that for information to qualify as confidential it must not be generally accessible and, consequently, must not form part of the public domain. In such an assessment, courts usually interrogate whether skill and labour are required to access or obtain the information concerned. Thus, in the realm of trade secrets, the term "confidential" appears to be a synonym of the term "secret", which follows from the fact that the breach of confidence action was developed to protect the undisclosed nature of information.[974] It is for this reason that case law does not

971 See chapter 4 § 2 B) II.

972 Tanya Aplin and others 2012 (n 22) para 5.02; Roger M. Toulson and Charles M. Phipps 2012 (n 326) 3-078.

973 Human Rights Act 1998; Tanya Aplin and others 2012 (n 22) para 5.02; *Campbell v MGN Ltd* [2004] 2 AC 457 (HL), 465-466.

974 Roger M. Toulson and Charles M. Phipps 2012 (n 326) 3-112; in the words of Bingham L.J. in *Attorney General v Guardian Newspapers Ltd (No 2)* [1988] 2 WLR 805 (CA): "Forty-four years ago there can have been few, if any, national secrets more confidential than the date of the planned invasion of France. Any crown servant who divulged such information to an unauthorised recipient would plainly have been in flagrant breach of his duty. But it would be absurd to hold such a servant bound to treat the date of the invasion as confidential on or after (say) 9 June 1944 when the date had become known to the world. A pursuit might say that the Allies, as confiders and owners of the information, had by their own act destroyed its confidentiality and so disabled themselves

require formalities with respect to the mode of expression of the information: the object of protection is the underlying ideas and thoughts (semantic information) and not their expression, unlike copyright.[975] Consequently, the general principle is that information need not be expressed in a tangible form to merit protection.[976] The attributes of confidence and the specific circumstances under which the confidential nature of information is lost are examined further in chapter 4.

2. The obligation of confidence

As mentioned above,[977] in order to find liability under the breach of confidence action, "information must have been imparted in circumstances importing an obligation of confidence".[978] This obligation may arise in a variety of contexts, as a result of a contract (express or implied) or in equity. Below, the four main situations that give rise to such an obligation are examined, namely (a) disclosure by confider to confidant; (b) accidental acquisition; (c) surreptitious acquisition; and (d) third party liability.[979]

a) Disclosure by confider to confidant

In the most common case of liability for breach of confidence a person provides information to another on the condition that he will not disclose it.[980] Such an equitable obligation of confidence arises when there is a direct relationship between the parties; among others, as a result of a contract, due to the existence of a fiduciary relationship between the parties or depending on the manner in which the information is conveyed.[981] This

---

from enforcing the duty, but the common sense view is that the date, being public knowledge, could no longer be regarded as the subject of confidence".

975 Tanya Aplin and others 2012 (n 22) para 5.10.

976 For instance, in *Terrapin Ltd v Builders' Supply Co (Hayes) Ltd* [1962] RPC 375 (Ch), 389 Roxburgh J noted that no distinction should be made with respect to the form in which information is expressed, whether orally or in writing.

977 See chapter 3 § 4 B) II. 2.

978 *Coco v A.N.Clark (Engineers) Ltd* [1969] RPC 41 (Ch), 47.

979 Private information may also give rise to an obligation of confidence; yet, its study falls outside the scope of the present research.

980 William Cornish, David Llewellyn and Tanya Aplin 2013 (n 209) para 8.20.

981 Lionel Bently and Brad Sherman 2014 (n 125) 1160-1161.

latter case appears particularly controversial, as identifying in a precise manner all of the circumstances that give rise to an obligation of confidentiality seems problematic.[982] Furthermore, numerous cases point to different tests to determine whether such an obligation arises.[983]

When assessing the existence of a confidentiality obligation on the recipient, most authorities resort to the so-called "reasonable man" test outlined by Megarry J in *Coco v Clark,*[984] whereby an obligation of confidence exists if a "reasonable man" would deem that the information was communicated in a confidential manner. To a large extent, this is an objective factual assessment based on the knowledge of the recipient.[985] Consequently, if information is conveyed, and it is expressly stated that it is secret, it is going to be difficult to argue that a reasonable man would regard it otherwise. However, this has proven more challenging if confidentiality is to be inferred from the circumstances of the case, where a number of elements such as the commonly held views, usages and trade practices of the industry are taken into account by the court deciding on the matter.[986]

Against this background, it is submitted, in line with recent scholarly work, that the preferred test should be the so-called "notice of confidentiality" test, which to a large extent is built on the "reasonable man" yardstick

982 Lionel Bently and Brad Sherman 2014 (n 125) 1161; Roger M. Toulson and Charles M. Phipps 2012 (n 326) para 3-008 noting that it would be "almost impossible to compile a list of all the relationships likely to give rise to duties of confidentiality. They include agents, trustees, partners, directors, employees; professional people; holders of public and private offices; people in close personal relationships; and many others"; similarly, Law Commission 1981 (n 327) para 4.2: "to compile an exhaustive list of such relationships would not be practicable and even if it were, the list would be of limited value because the extent of the obligation of confidence varies according to the exact nature of the relationship".

983 As reviewed in Tanya Aplin and others 2012 (n 22) para 7.02-7.52.

984 Among others, this test is referred to in *De Maudsley v Palumbo* [1996] FSR 447 (Ch); *Mars UK Ltd v Teknowledge Ltd* [2000] FSR 138 (Pat); likewise, Roger M. Toulson and Charles M. Phipps 2012 (n 326) 3-008 highlight that "the common thread is that a reasonable person would understand them as involving an obligation of confidentiality".

985 Lionel Bently and Brad Sherman 2014 (n 125) 1161 highlight that "it is a subjective but assessed in the light of the knowledge of the recipient"; William Cornish, David Llewellyn and Tanya Aplin 2013 (n 209) para 8-20 consider that this test implicitly refers to a "somewhat diffuse notion of good faith", as the obligation of confidence may be breached by unintentional behaviours.

986 Lionel Bently and Brad Sherman 2014 (n 125) 1161.

referred to above.[987] The former considers whether "the circumstances in which the information was acquired or received indicate (objective) knowledge or notice of confidentiality of the information".[988] To conduct this assessment, a number of factors are weighed against each other, namely, (i) the nature of the information; (ii) the measures adopted to preserve confidentiality; (iii) the manner of in which the information was acquired or disclosed; (iv) the perception of the parties, that is, whether they regard the information as being confidential; and (v) whether the information was disclosed for a limited purpose.[989]

Similar to the "reasonable man" yardstick, the notice of confidentiality test demands that the alleged confider has an objective knowledge that the information in question is being disclosed in a confidential manner. However, under the second test, such an assessment may be influenced by the subjective intention or tacit views of the parties.[990] Hence, the subjective element is introduced not with regard to the confidential (secret) nature of

---

987 Tanya Aplin and others 2012 (n 22) para 7.36.

988 Tanya Aplin and others 2012 (n 22) para 7.37

989 Tanya Aplin and others 2012 (n 22) para 7.36; on this point, the Second edition of Gurry on Breach of confidence departs from the first edition, where it was deemed that the limited purpose test should be the prevailing criterion to assess confidentiality, as per para 7.02: "an obligation will exist whenever confidential information is imparted by a confider for a limited purpose. In these circumstances the confidant will be bound by a duty not to use the information or any purpose other than that for which it was disclosed"; similarly, Roger M. Toulson and Charles M. Phipps 2012 (n 326) 3-012 argue that "where information of a personal or confidential nature is obtained or received in the exercise of a legal power or to furtherance of a legal duty, the recipient will in general owe a duty to the person from whom it was obtained or to whom it relates not to use it for unrelated purposes".

990 Tanya Aplin and others 2012 (n 22) paras 7.38-7.39; *De Maudsley v Palumbo* [1996] FSR 447 (Ch), 457, where Judge Knox favoured an objective test informed by the appraisal of subjective views: "The test in my view is objective-the question is where the circumstances such as to import a duty of confidence and, if so, the obligation is not to be avoided simply by not addressing the problem. On the other hand, I accept that a factor, and it may be an important factor, is whether the parties did in fact regard themselves as under an obligation to preserve confidence, just as is a proven trade or industry usage in that regard but I do not accept that the test is exclusively subjective as to the parties' intentions"; by contrast, Jacob J in *Carflow Products (UK) Ltd v Linwood Securities* [1996] FSR 424 (Ch), 428 favoured a subjective test. He argued that under the breach of confidence action, unlike in contract law, the subjective views of the parties had to be taken into consideration, because equity "looks at the conscience of the individual.

the information, but rather with respect to the appraisal of whether an obligation to keep it secret arises.

b) Accidental acquisition

The accidental acquisition of secret information takes place when no direct relationship between the parties exists. It covers situations where one of the parties obtains certain information that is regarded as confidential by the other, as a result, directly or indirectly, of an accident, negligence or a mistake on the part of the party who knew that the information was of a confidential nature.[991] This would be the case, for example, if a member of the public fortuitously found a confidential document on the street that had been lost by the holder of the information.[992] The information is acquired without surreptitious means, merely as a result of carelessness. Nonetheless, despite the fact that no relationship between the parties exists, a duty of confidence may arise.[993]

The leading opinions among legal scholars restrict such a possibility to situations where the acquirer knows that the information is confidential or "is deliberately blind to the likelihood of it being confidential".[994] The underlying rationale is to protect confidential information as such based on

991 Tanya Aplin and others 2012 (n 22) para 7.46.
992 Lionel Bently and Brad Sherman 2014 (n 125) 1163.
993 Lionel Bently and Brad Sherman 2014 (n 125) 1163.
994 Roger M. Toulson and Charles M. Phipps 2012 (n 326) para 3-07.6 This statement is based on a passage from Lord Goff in *Attorney General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109 (HL), 281-282: "A duty of confidence arises when confidential information comes to the knowledge of a person (the confidant) in circumstances where he has notice, or is held to have agreed, that the information is confidential, with the effect that it would be just in all circumstances that he should be precluded from disclosing the information to others. I have used the word "notice" advisedly, in order to avoid the (here unnecessary) question of the extent to which actual knowledge is necessary; though I of course understand knowledge to include circumstances where the confidant has deliberately closed his eyes to the obvious (…) I have expressed the circumstances in which the duty arises in broad terms (…) to include certain situations beloved of law teachers –where an obviously confidential document is wafted by an electric fan out of the window into a crowded street into a crowded street, or when an obviously confidential document, such as a private diary, is dropped in a public place, and it is then picked by a passer-by".

the knowledge that the information was confidential, instead of a pre-existing confidential obligation.[995]

c) Surreptitious acquisition

The surreptitious acquisition of information refers to the obtention of information through "reprehensible means".[996] It encompasses a broad array of activities, such as theft of confidential documents or products to name a few, and may arise in a variety of contexts.[997] The main difficulty in applying the breach of confidence action stems from the lack of a relationship between the parties involved.[998] In fact, The Law Commission Report on Breach of Confidence from 1981 concluded that it was questionable whether an obligation of confidence might arise based only on the use of reprehensible means in the acquisition of information.[999]

Notwithstanding this, subsequently commentators and a number of cases argued in favour of establishing liability on the basis that the acquirer knew that the information was confidential and such knowledge derived from the means through which it was obtained.[1000]

One of the most relevant cases in this regard was *Shelley Films v Rex Featured Limited*,[1001] which concerned the publication of photographs taken during the shooting of a film based on the famous novel Frankenstein by Mary Shelley. The disputed photographs depicted one of the actors in character and were taken inside the studio premises without authorisation

995 Tanya Aplin and others (n 22) para 7.51.
996 Law Commission 1981 (n 327) para 4.7.
997 Tanya Aplin and others (n 22) para 7.53 provide a non-exhaustive list of types of conduct that can be considered to be "surreptitious acquisition". In particular, they mention the following examples: "secret photographic filming, or otherwise recording activities of a person or business, hacking into an encrypted computer to access documents or email correspondence; tapping a telephone or intercepting mail into the post".
998 Tanya Aplin and others 2012 (n 22) para 7.54.
999 Law Commission 1981 (n 327) para 4.10; Roger M. Toulson and Charles M. Phipps 2012 (n 326) 3-031 argue that this statement is largely based on the finding of Megarry VC in *Malone v Commissioner of Police of the Metropolis* (No 2) [1979] 2 All ER 620 (Ch), where it was argued that the accidental acquisition of information (in the case at hand by overhearing a conversation or tapping a phone conversation) did not give rise to an obligation of confidence.
1000 Tanya Aplin and others 2012 (n 22) para 7.55.
1001 *Shelley Films Limited v Rex Features Limited* [1994] EMLR 134 (Ch).

and despite the existence of signs that prohibited the taking of pictures. The plaintiff, the company that produced the film, sought an injunction on the basis of copyright infringement and breach of confidence and argued that the dissemination of the photographs would run counter to the film's marketing strategy. In the legal grounds of the decision, Martin Mann QC ruled that it was impossible under the specific circumstances of the case that the photographer was not aware that the information was of a confidential nature and that he was not allowed to convey it to others.[1002] It further noted that the producing company had an "obvious and stated commercial interest in protecting its substantial investment by, minimally, being able to provide an undisrupted production environment and to control the timing and manner of the release of information about the film (…)".[1003] Hence, the existence of a commercial interest also appears to be one of the elements that courts weigh up when assessing breach of confidence.[1004]

d) Third party liability

The liability of third parties is still, to date, one of the most controversial topics in the field of trade secrecy law. It refers to situations where information is imparted during the course of a confidential relationship and is later disclosed in breach of confidence to a third party by the confidant. Thus, it differs from the accidental or surreptitious acquisition of information in that negligence, mistake or reprehensible means are not involved (just unauthorised disclosure) and there is an obligation of confidence between the holder of the information and the party that reveals it.[1005] The main legal question that arises is whether the recipient outside of the initial confidential relationship is bound by an obligation of confidence.[1006] Against this background, a distinction must be drawn between two main

1002 *Shelley Films Limited v Rex Features Limited* [1994] EMLR 134 (Ch), 148.
1003 *Shelley Films Limited v Rex Features Limited* [1994] EMLR 134 (Ch),148.
1004 Chris D.L. Hunt, 'Rethinking Surreptitious Takings in the Law of Confidence' [2011] IPQ 66 where it is argued that obligations of confidence should not extend to surreptitious takers owing to the absence of a pre-existing relationship. The author argues that imposing liability under breach of confidence would distort the main policies underpinning the action, i.e. relationship preservation and remedying unconscionable conduct.
1005 Tanya Aplin and others 2012 (n 22) para 7.103.
1006 Lionel Bently and Brad Sherman 2014 (n 125) 1028.

situations: (i) the acquisition of information that occurs with knowledge of the breach, and (ii) acquisition by an indirect recipient who is not aware of the confidential nature of the information.

In the first scenario, the case law provides that a third party who receives confidential information knowing that it is confidential will come under an obligation not to disclose it at the time that he receives it.[1007] The extent of knowledge required to come under such a duty is linked to the failure of the third party to "observe the standard which would be observed by an honest person placed under those circumstances",[1008] in line with footnote 10 of the TRIPs Agreement.[1009] Similarly to the accessory liability for breach of trust or fiduciary obligation, dishonesty has been cited by some commentators and in some authorities as a prerequisite to finding third party recipients liable for breach of confidence. In this regard, Toulson and Phipps concluded that:

> The important thing is that for a third party to be held liable in equity for a breach of confidence, more is required than merely careless, naive or stupid behaviour; there must be awareness of the fact that the information was confidential or willingness to turn a proverbial blind eye.[1010]

This passage was later interpreted by Buxton LJ in *Thomas v Peace*[1011] as meaning that dishonesty could be inferred both from the fact that the recipient had actual knowledge of the wrongness and the mere fact that he closed his eyes to it. Bearing this in mind, Aplin, Bently, Johnson and Malynic hold a different view in the second edition of *Gurry on Breach of Confidence*.[1012] In essence, they suggest that dishonest behaviour on the part of the third party should not be considered as a requisite to finding liability. Rather it should be interpreted as a factor pointing towards the existence of actual knowledge. In support of this view, reference is made to *Prince*

1007 *Schering Chemicals Ltd v Falkman Ltd* [1982] QB 1(CA), 27 (Shaw LJ); *Attorney General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109 (HL), 260 where Lord Keith stated that: "it is a general rule of law that a third party who comes into possession of confidential obligation which he knows to be such, may come under a duty not to pass it to anyone else".

1008 *Royal Brunei Airlines Sdn. Bhd v Philip Tan Kok Ming* [1995] 2 AC 378 (PC), 390.

1009 Roger M. Toulson and Charles M. Phipps 2012 (n 326) 3-069 and Lionel Bently and Brad Sherman 2014 (n 125) 1028-1029.

1010 Roger M. Toulson and Charles M. Phipps 2012 (n 326) para 3-071.

1011 *Susan Thomas v Elizabeth Pearce and Another* [2000] FSR 718, 721.

1012 Tanya Aplin and others 2012 (n 22) paras 7.110-7.111

Albert v Strange and the legal position of one of the defendants, Mr Judge. He acquired a number of copies of etchings made by the Queen and Prince Albert for their private use from one of the employees (Mr Middelton) of the printer at Windsor where the impressions had been printed off and intended to make a public exhibition with them. Mr Middelton had in turn taken copies of them in a surreptitious manner.[1013] As regards the liability of Mr Judge, the court ruled that he had obtained the etchings knowing that Mr Middelton must have acquired them with "faithlessness, fraud and treachery".[1014] Hence, the Court of Chancery granted an injunction on the basis of an equitable jurisdiction, restraining him from exhibiting the etchings and publishing the catalogue.

In the second scenario, the recipient acquires information without being aware of its confidential nature. This would be the case, for instance, if an employer conveyed a trade secret to one of his employees and the latter revealed it to his subsequent employer without him knowing that the information was in fact one of his competitor's secrets.[1015] In such cases, the general principle is that if a person receives information innocently, he is liable as of the date on which he was given notice that the information was obtained as a result of a breach of confidence.[1016]

Both approaches seem to be in line with the solution presented by the EU legislature in Article 4(4) of the TSD, by virtue of which, the liability of third parties is established if at the time of the acquisition, use or disclo-

---

1013 *Prince Albert v. Strange* [1849] 2 De G & Sm 652, 714.

1014 *Prince Albert v. Strange* [1849] 2 De G & Sm 652, 714.

1015 A similar case was decided in *English & American Insurance Co Ltd. v Herbert Smith 2* [1988] FSR 232 (Ch), where the papers of the council acting for the plaintiff in an action pending in the Commercial Court were sent by mistake to the solicitors of the other party. Upon reception of the documents the solicitors did not read the content, but informed their clients, who instructed them to look through the documents. As a result, an action for breach of confidence was brought against the solicitors of the defendant in order to restrain the use of information obtained from those papers. The Judge granted the injunction, arguing that as a general rule, the equitable jurisdiction may provide relief against the world and that only bona fide purchasers for value without notice were excluded from liability. He further noted that in the case at hand, there had been a deliberate decision to acquire the confidential information, which was taken with knowledge that the papers were of a confidential nature. Hence, he concluded that the defendants had no right to use the information contained in the privileged document, as it belonged to the plaintiff.

1016 John Hull, *Commercial Secrecy* (1st edn, Sweet&Maxwell 1998) para 4.185; see *Malone v Commissioner of Police of the Metropolis (No 2)* [1979] 2 All ER 620 (Ch).

sure they knew (or should have known under the circumstances) that the information had been obtained unlawfully. Hence, knowledge (or reason to know) are at the centre of the assessment of the liability of third parties, both in the English jurisdiction and the TSD, following a gross negligence liability standard.

As a final note, it is worth highlighting that the position of bona fide purchasers for value remains controversial, as it has been argued that innocent third parties that in good faith "incurred detriment by paying for the information or perhaps incurring expense of money or effort in consequence of obtaining it (for example in further research and development)" may be exempted from liability.[1017] This approach stems from one of the passages in *Morison v. Moat,* where Turner V.C. noted that the purchaser for value in good faith may be in a different position from other innocent third parties:

> It might indeed be different if the Defendant was a purchaser for value of the secret without notice of any obligation affecting it; and the Defendant's case was attempted to be put upon this ground…but I do not think that this view of the case can avail him … So far as the secret is concerned he is a mere volunteer deriving under a breach of trust or of contract.[1018]

In the light of the above, some commentators have debated the existence of a bona fide defence for value that covers innocent third party recipients in good faith.[1019] The implications of adopting this general defence are better explained with an example. Let us take the case of a businessman (X) who pays for confidential information from another (Y) without knowing that the information was obtained by Y breaching the confidence of another person (P). If the above referred to defence is generally accepted, P will not be able to obtain either an injunction or damages against X, even after giving him notice of confidentiality.[1020]

As a result of the foregoing analysis, the preferred approach is a flexible one, where all of the circumstances of the case are balanced against each other taking into account the divergent interests of the parties.[1021] The

1017 Tanya Aplin and others 2012 (n 22) para 7.129.
1018 *Morison v Moat* [1851] 9 Hare 241, 263-264.
1019 For a more in-depth analysis of this issue see Tanya Aplin and others 2012 (n 22) para 7.121.
1020 A similar example was first presented by Gareth Jones, 'Restitution of Benefits Obtained in breach of another's Confidence' [1970] 86 LQR 463, 48.
1021 Tanya Aplin and others 2012 (n 22) paras 7.136-7.143.

bona fide acquisition of information should not afford an absolute right to continue using the information.[1022] Rather, it should be one of the factors taken into consideration by courts when deciding whether to grant the relief. Among these, a key factor should be whether the acquirer of the information changed his position on the information before learning about its confidential nature.[1023] That would be the case, for instance, if the acquirer of the information had invested in new machinery or hired new employees based on the disclosure of confidential information. Under such circumstances, providing economic compensation for using the confidential information appears to be more appropriate than granting an injunction.[1024] The EU legislature has included a similar approach in Article 13 TSD, by virtue of which national courts may allow a third party to continue using a trade secret after receiving notice of its infringing nature provided that adequate compensation is paid (damages in lieu of injunctions).[1025]

3. Unauthorised use

Pursuant to *Coco v AN Clark*, the third requirement to find breach of confidence requires that the information is communicated without authorisation and to the detriment of the party conveying it.[1026] Thus, in the first place it is necessary to establish the scope of the obligation of confidence in order to determine whether it has been breached by use, disclosure or some other act.[1027] If the obligation stems from an express term in a contract, the scope is determined by means of interpreting the relevant provisions. By contrast, if the duty of confidentiality arises implicitly or in equity, the assessment will be a factual one. It will ultimately depend upon the specific circumstances surrounding each particular case.[1028] Accordingly,

---

1022 Roger M. Toulson and Charles M. Phipps 2012 (n 326) paras 3-063- 3-064 are also reluctant to accept a general bona fide defence for value, as the transfer of property rights does not apply to the position of third party acquirers.

1023 For a more detailed analysis see Tanya Aplin and others (n 22) 7.140

1024 Tanya Aplin and others 2012 (n 22) para 7.140.

1025 See further chapter 3 § 5 C) IV. 4. b).

1026 *Coco v A.N.Clark (Engineers) Ltd* [1969] RPC 41 (Ch).

1027 Lionel Bently and Brad Sherman 2014 (n 125) 1172-1173 highlight that under English law the use and disclosure of information may be restricted, but not the acquisition. Accordingly, they argue that British law might be in breach of TRIPS, which refers to the disclosure, acquisition and use of information.

1028 Lionel Bently and Brad Sherman 2014 (n 125) 1161.

the scope of the obligation is to be determined by what "a reasonable person standing in the shoes of the defendant would understand is not permitted".[1029]

In order to find liability under the breach of confidence action it is crucial to show "derivation", that is, that the information in question has been "directly or indirectly" acquired from the confider.[1030] Hence, when information has been generated independently or obtained from other sources no liability arises.[1031] In practical terms, this means that during litigation the plaintiff should provide evidence that the defendant acquired the information from him. A clear example would be the case of an employee who uses one of his former employer's secrets. In this case, the employer should prove that the employee acquired the information from him.

Furthermore, the defendant's state of mind at the time that he receives or uses the information should not be taken into consideration for the purposes of determining whether an obligation has been breached (the fourth prong).[1032] It is irrelevant for the breach whether the defendant acted in good faith or not, or had actual knowledge of the secret nature of the information.[1033]

As stated above, Megarry J in *Coco v AN Clark* raised the question of whether the misuse of confidential information must be detrimental to the confider in order to trigger liability under the breach of confidence action; i.e. whether damage is an essential element of the action. To date the answer to this question remains unclear, as the case law has provided divergent solutions.[1034]

1029 Tanya Aplin and others 2012 (n 22) para 10.50.

1030 *Saltman Engineering v Campell Engineering* [1948] 65 RPC 203 (CA), 213 (Lord Green MR).

1031 Tanya Aplin and others 2012 (n 22) para 15.03; Lionel Bently and Brad Sherman 2014 (n 125) 1176.

1032 William Cornish, David Llewellyn and Tanya Aplin 2013 (n 209) para 8-38 .

1033 Lionel Bently and Brad Sherman 2014 (n 125) 1177.

1034 William Cornish, David Llewellyn and Tanya Aplin 2013 (n 209) para 8-39; in *Douglas v Hello! Ltd and others* [2007] UKHL 21, [111]-[115] and in *Attorney General v Guardian (No 2)* [1990] 1 AC 109 (HL), 270 (Lord Griffith), it is submitted that it is necessary to show detriment to find liability under a breach of confidence action, whereas in the same decision at 256 Lord Keith states, "So I would think it a sufficient detriment to the confider that the information given in confidence is to be disclosed to persons whom he would prefer not to know of it, even though the disclosure would not be harmful to him in any positive way".

Cornish argues that the finding of liability by the mere breaking of confidence is problematic. In particular, he observes that the breach of confidence action imposes limitations on the freedom to use information. Thus, as a matter of public interest, such a restriction requires "sufficient reason".[1035] He further supports the detrimental use requirement by noting that in most economic torts proof of damage is an essential part of an actionable tort.[1036]

By contrast, Aplin, Bently, Johnson and Malynic suggest that the detriment requirement is already encompassed by the nature of the information and the scope of the obligation. Where an obligation exists, it is indeed likely that an infringement will cause a detriment. However, in certain scenarios where that might not be the case, such as technical secrets and private information, it is argued that the detriment is conceived as a loss of the potential licence fee.[1037]

Indeed, a review of the relevant case law shows that damage is a condition to find liability only with regard to government secrets, not private information[1038] or commercial secrets.[1039]

III. The "springboard doctrine"

One of the most notable features of the English legal system in the field of confidential information is the development of the so-called "springboard doctrine". Basically, this doctrine seeks to prevent a situation where a person who breaches an obligation benefits from such conduct.[1040] Accordingly, courts may grant injunctive relief in order to prevent the recipient of confidential information obtaining an "unfair start" over their competitors.[1041] It mainly aims at fulfilling two policy objectives, i.e. fostering the

1035 William Cornish, David Llewellyn and Tanya Aplin 2013 (n 209) para 8-39.
1036 William Cornish, David Llewellyn and Tanya Aplin 2013 (n 209) para 8-39.
1037 Tanya Aplin and others 2012 (n 22) para 15.43.
1038 *McKennitt v Ash* [2006] EWCA Civ 1714 (CA).
1039 Lionel Bently and Brad Sherman 2014 (n 125) 1177.
1040 Lionel Bently and Brad Sherman 2014 (n 125) 1151; Roger M. Toulson and Charles M. Phipps 2012 (n 326) 4-025 noting that, "The object of the springboard doctrine is merely to ensure that the recipient of confidential information does not obtain an unfair start by misuse of information received in confidence".
1041 Lionel Bently and Brad Sherman 2014 (n 125) 1151; Roger M. Toulson and Charles M. Phipps 2012 (n 326) 4-025.

duty of confidentiality by reducing the potential benefits of using the information disclosed and encouraging "fair relationships" among competitors.[1042] It was first formulated in *Terrapin Ltd v Builders' Supply Co (Hayes) Ltd* by Roxburh J, who noted that:

> As I understand it, the essence of this branch of the law, whatever the origin may be, is that as a person who has obtained information in confidence is not allowed to use it as a springboard for activities detrimental to the person who made the confidential communication, and springboard it remains even when all the features have been published or can be ascertained by an actual inspector or member of the public.[1043]

Notwithstanding this, some of its features are highly controversial. It has been argued that this doctrine goes against the general principle according to which once information enters the public domain it cannot be protected under the breach of confidence action.[1044] This issue was addressed by the Law Commission Report on Breach of Confidence. In essence, it was stated that information should not be regarded as effectively in the public domain until it would be "reasonably possible for an interested member of the public in fact to use the information even though some of the information was already available to the public".[1045] In this regard, subsequent decisions have required that protection is only afforded with regard to the unfair advantage that the defendant would obtain if no injunction were granted. Accordingly the scope of such an injunction should not extend beyond the duration of the unfair advantage.[1046] Furthermore, in some cases, courts have required the defendants to pay for the information.[1047]

1042 Lionel Bently and Brad Sherman 2014 (n 125) 1151.

1043 *Terrapin Ltd v Builders' Supply Co (Hayes) Ltd* [1962] RPC 375 (Ch), 391; the decision was rendered in 1959 but only reported in 1967.

1044 Roger M. Toulson and Charles M. Phipps 2012 (n 326) 4-025.

1045 Law Commission 1981 (n 327) para 4.31.

1046 Roger M. Toulson and Charles M. Phipps 2012 (n 326) 4-025; in *Sun Valley Foods Ltd v Vincent* [2000] FSR 825 (Ch), 834-837 it was ruled that the grant of an injunction was subject to the persistence of the unfair advantage on the date of the order.

1047 John Hull 1998 (1016) para 3.43.

§ 4 Concluding remarks on the comparative law analysis

The comparative analysis conducted above underscores that despite the existence of common ground on certain aspects of the protection of trade secrets, there are also substantial differences in their regulation in Germany and England. These range from the lack of clarity as to the cause of action that parties may invoke in England to the two-fold nature of trade secrets protection envisaged in the German UWG. As regards enforcement, there is also uncertainty surrounding the remedies available in Germany and the applicability of the Enforcement Directive in England.[1048] Most notably, in both jurisdictions other unsettled issues include the information that departing employees are free to take to their new positions and the assessment of the liability of third parties. Crucially, there is also uncertainty surrounding the circumstances under which reverse engineering should be deemed lawful.

Similarly, showing that a detriment to the holder of information has taken place is not necessary in England (per se), whereas in Germany the UWG lays down that the acquisition, use and disclosure of trade secrets must be carried out "for the purposes of competition, for personal gain, for the benefit of a third party, or with the intent of causing damage to the owner of the business, " which ultimately leads to a different conceptualisation of when misappropriation has taken place.

Notably, the standard of liability of third parties seems higher in Germany under the scheme set out in the UWG, where at the minimum conditional intent is required as a result of the criminal law nature of the provision. By contrast, the standard of liability in England is much more flexible and is built upon knowledge and "the observance of the standard which would be observed by a honest man".[1049]

In the light of the substantial divergences and their impact on the construction of the Single Market, the EU legislature decided to take legal action to harmonise this area of law. On April 14, 2016 the European Parliament passed the TSD, which provides for minimum standards of protection against the unlawful acquisition, use and disclosure of confidential business information. The main features of the Directive and its legal implications for the assessment of the optimal scope of secrecy constitute the object of study of the remainder of this chapter.

1048 This aspect will become irrelevant after the withdrawal of the UK from the EU.

1049 Roger M. Toulson and Charles M. Phipps 2012 (n 326) para 3-070.

§ 5 The emerging common framework: a critical study of the Trade Secrets Directive

A) Background of the Directive

In November 2013, after months of hermetic negotiations, the Commission issued the much-anticipated Proposal for a Directive on the protection of trade secrets.[1050] This legislative initiative falls within the framework of the Comprehensive intellectual property strategy adopted in May 2011, aimed at the suppression of the remaining barriers within the Internal Market and the achievement of a "true Single Market" for IPRs by 2020.[1051] Strengthening the existing legal regime for the protection of IPRs was identified by the Commission as one of the linchpins of an Innovation Union and an essential factor in order to ensure a growing labour market and the continued competitiveness of the whole EU economy.[1052]

In the 2011 IPRs Strategy, the Commission took the view that the existing disparities in the national regimes led to a fragmented protection of trade secrets within the Internal Market, as examined throughout chapter 3.[1053] In particular, it was noted that the substantial inconsistencies on the national level regarding the nature and scope of trade secrets, as well as the available means of redress and remedies resulted in different levels of protection across the EU. Furthermore, it echoed the increasing vulnerability of trade secrets in relation to unlawful disclosure, acquisition and use.

1050 Commission, 'Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure' COM (2013) 813 final (Commission Proposal).

1051 Commission, 'Communication from the Commission to the European Parliament, the Council, the European and economic and social committee and the committee of the regions. A Single Market for Intellectual Property Rights. Boosting creativity and innovation to provide economic growth, high quality jobs and first class products and services in Europe' COM (2011) 287 final, 3 <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52011DC0287&from=EN> accessed 15 September 2018 (Commission, A Single Market for Intellectual Property Rights).

1052 IPRs are regarded by the Commission as a crucial driver for innovation and creativity. As such, it is believed that enhancing the protection of IPRs within the internal market will foster the EU's economic growth, cultural diversity and international competitiveness; for a more detailed account of the EU's 2011 IPRs Strategy, see Commission, A Single Market for Intellectual Property Rights (n 1051).

1053 Commission, A Single Market for Intellectual Property Rights (n 1051) 6.

Notwithstanding this, it was concluded that further evidence was required before taking an EU approach in this area.

In the light of the above, in March 2011 a study on the legal framework for the protection of trade secrets and parasitic copying in the (at that time) 27 Member States was commissioned to Hogan Lovells International LLP. The primary objective of the study was to conduct a comparative law analysis in order to clarify the legal regime and practices in all of the jurisdictions of the EU. The final report was published in January 2012 and in essence it confirmed what the Commission had hesitantly pointed out in the 2011 strategy: "the law in relation to trade secrets in the EU is a collage".[1054] The outcome of the study showed that there were substantial differences among the 27 Member States with regard to core issues, such as the actual definition of the information that could be protected as a trade secret; the legal basis for protection, i.e. unfair competition, tort law and criminal law; the status of trade secrets as IPRs; the applicability of the Enforcement Directive; and the remedies and means of redress available.[1055]

In June 2012, the Commission held a conference in Brussels entitled "*Trade Secrets: Supporting Innovation, Protecting Know-how*" with the aim of facilitating a dialogue with stakeholders. During the conference, the differences among the (at that time) 27 jurisdictions and the economic importance of trade secrets protection in ensuring competitiveness and innovation were analysed and some of the potential policy options were examined.[1056]

Following the conference with representatives from the industry, a statistical on-the field survey was conducted by Baker McKenzie LLP on behalf of the Commission in order to assess the actual relevance of trade secrets and confidential business information as drivers for innovation, competitiveness and economic growth in the EU. By the end of the consultation period, more than 537 undertakings had participated in the survey, which was included as part of a more extensive study dealing with the economic structure of trade secrets protection in the European Union.[1057] From an economic perspective, the Baker McKenzie empirical study revealed that trade secrets constituted an essential element for performance, growth and competitiveness for the vast majority of the companies that re-

1054 Hogan Lovells 2012 (n 793) para 290.
1055 Hogan Lovells 2012 (n 793) paras 288-304.
1056 For further information see <http://ec.europa.eu/growth/tools-databases/newsroom/cf/itemdetail.cfm?item_id=8270> accessed 15 September 2018.
1057 Baker McKenzie 2013 (n 469) 12.

sponded to the survey (74% of them attached medium or high importance to trade secrets). In the same vein, over a third of them expressed concerns regarding the loss of confidential information.[1058] In this context, current and former employees, together with competitors and suppliers were identified as the main sources of risk. The study further indicated that trade secrets misappropriation (whether actual or merely an attempt) results in a "loss of sales (56%), costs for internal investigation (44%), increased expenditure for the protection (35%), cost for negotiating settlements (34%), and costs for prosecuting and litigating (31%)".[1059]

Notably, most of the participants supported a potential EU action in order to establish common rules regarding the protection of trade secrets. In particular, participants showed a preference for harmonisation in four areas, which guided the legislative process led by the Commission. The issues of concern highlighted by the participants were: (i) the clarification of the information that can be protected as a trade secret (55%); (ii) the prohibition of acts of misappropriation and the definition of such types of conduct (45%); (iii) the establishment of common rules vis-à-vis criminal sanctions (35, 5%) and (iv) ensuring confidentiality during litigation.

At the same time, from December 2012 until March 2013 the Commission carried out an open consultation focussed on the perception and use of trade secrets, which attracted the participation of 386 respondents. Among the contributors were not only private undertakings and business organisations, but also citizens and professionals. The outcome of the consultation showed that most citizens (75%) deemed that trade secrets protection was not a key element for R&D and that the existing legal framework was already too stringent, whereas the vast majority of the responding companies regarded trade secrets as an essential element for R&D and their competitiveness.[1060]

After conducting the aforementioned studies and consultations, the Commission concluded that there was a case for harmonisation. Thus, the ordinary legislative procedure was initiated,[1061] and on November 2012 the "Proposal for a Directive of the European Parliament and of the Council

1058 Baker McKenzie 2013 (n 469) 122-123.

1059 Baker McKenzie 2013 (n 469) 129.

1060 Commission, 'Explanatory Memorandum of the Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure' 6.

1061 The ordinary legislative procedure within the EU is regulated in Articles 289 (1) and 294 of the TFEU, and as its name indicates, it is the most common pro-

on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure"[1062] was published. Along with it, an Impact Assessment was issued by the Commission, in which it was essentially restated that the existing scattered legal protection was detrimental to the competitiveness of the internal market[1063] and five potential policy options were analysed.[1064]

In line with the ordinary legislative procedure, on May 14, 2014 the Council of the European Union presented its General Approach to the proposed Directive.[1065] After months of negotiations, the European Parliament and Council adopted the final Draft of the TSD on June 8, 2016.

The following sections examine the new legal framework created by the TSD. To this end, section B explores the legal basis and ground for harmonising trade secrets protection within the EU legal framework. Next, a legal analysis of the new obligations set out in the Directive and their implications for the assessment of secrecy is conducted in section C below.

---

cedure followed to enact EU legislation. Prior to the entry into force of the Lisbon Treaty in December 2009, most of the legislative initiatives were started by the Commission upon the request of the Council or the European Council. However, the legislative process is now governed by the co-decision procedure, which essentially consists of the adoption, both by the European Parliament and by the Council of the regulations, directives or decisions, of a proposal presented by the Commission. A more detailed account of the legislative procedures in the EU falls outside the scope of the present research. Nonetheless, the following authors provide an insightful analysis of this topic: Paul Craig and Gráinne de Búrca, *EU Law, Text, Cases, and Materials* (5th edition OUP 2011) 121-133; Jörn Axel Kämmerer, 'European Commission', *The Max Planck Encyclopaedia of European Private Law* (OUP 2012) 563-565 and Walter Frenz, *Handbuch Europa-Recht*, vol 6 (1st edn, Springer 2011) 501-528.

1062 Commission, 'Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure' COM (2013) 813 final.

1063 Impact Assessment (n 385) 18-21.

1064 Impact Assessment (n 385) 43-45.

1065 Council, 'General Approach on the Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure' 2013/0402 (COD) (Council's Proposal) <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%209870%202014%20INIT> accessed 15 September 2018.

B) Legal basis and grounds for harmonising trade secrets protection

As mentioned in the first chapter of this dissertation, finding a sound justification to harmonise trade secrets protection within the EU is both necessary and desirable to ensure the good functioning of the internal market. For some, the aspirational rhetoric of the TSD resembles that of the Database Directive, which has not fulfilled the economic improvements it was supposed to bring about.[1066] The remainder of this section surveys the main objectives of the TSD and analyses the legal basis upon which the legislative initiative is based.

The Directive aims to provide a sufficient and comparable level of redress across all Member States against the misappropriation of trade secrets, even though it only provides for minimum standards of protection.[1067] One of the main goals of the EU is to ensure the creation of a Single Market without frontiers in which the four freedoms, "free movement of goods, persons, services and capital", are accomplished.[1068] To achieve the creation of the internal market, over time the CJEU has developed a consistent body of case law preventing the adoption of trade rules by Member States that may directly (or indirectly) hinder trade within the EU.[1069]

1066 This argument is raised by Tanya Aplin 2014 (n 384) 259; a comprehensive evaluation of the economic impact of the Database Directive is provided in Commission, 'First evaluation of Directive 96/9/EC on the legal protection of databases' (2005) DG Internal Market and Services Working Paper 24, where it is noted that the sui generis right "economic impact on database production is unproven".

1067 See Recital 10 TSD.

1068 See Article 26(2) TFEU; in this regard, it is noteworthy that the Treaty does not establish a single right of economic free movement. Instead, a bundle of rights and prohibitions is set forth, in order to limit unjustified restrictions on the freedom of movement and establishment, which would ultimately affect trade between Member States; see further Richard Gordon, *EC Law in judicial review* (1st edn, OUP 2007) para 16.01.

1069 Case 8/74 *Procureur du Roi v Dassonville* [1974] ECR I-837, 852: " All trading rules enacted by Member States which are capable of hindering, directly or indirectly, actually or potentially, intra-Community trade are to be considered as measures having an effect equivalent to quantitative restrictions". The scope of this rule was subsequently limited by the CJEU in Joined Cases C-267/91 and C-268/91 *Keck and Mithurard* [1993] ECR I-6097, para 16, where the Court noted that: "contrary to what has previously been decided, the application to products from other Member States of national provisions restricting or prohibiting certain selling arrangements is not such as to hinder directly or indi-

As regards trade secrets, the disparities among the different national legal regimes resulted in different subject matter being protected and different interpretations of when an unlawful acquisition, use and disclosure of confidential information had occurred.[1070] The available means of enforcement also varied from one Member State to another.[1071] Consequently, it was regarded that this might hamper the free movement of employees (persons), services and goods.

Ohly provided an example of the latter case, which he warned was rather extreme. He explained that it might not be possible to import a product in which a trade secret is embodied into other EU markets, if protection is afforded in the destination market and not the original one.[1072] He further added that from an EU law perspective, this would run counter to the principle of free movement of goods, which can only be limited in two instances: (i) to protect intellectual property (Article 36 TFEU);[1073] and (ii) to protect fair competition following the doctrine set forth by the CJEU in *Cassis de Dijon*.[1074] Similarly, the different national rules on non-

---

rectly, actually or potentially, trade between Member States within the meaning of the Dassonville judgement (Case 8/74 *Procureur du Roi v Dassonville* [1974] ECR I-837*): "so long as those provisions apply to all relevant traders operating within the national territory and so long as they affect in the same manner, in law and in fact, the marketing of domestic products and of those from other Member States*" (emphasis added).

1070 Hogan Lovells 2012 (n 793) para 304.

1071 Ansgar Ohly 2013 (n 13) 39.

1072 Ansgar Ohly 2013 (n 13) 39.

1073 Article 36 TFEU provides the following: "The provisions of Articles 34 and 35 shall not preclude prohibitions or restrictions on imports, exports or goods in transit justified on grounds of public morality, public policy or public security; the protection of health and life of humans, animals or plants; the protection of national treasures possessing artistic, historic or archaeological value; or the *protection of industrial and commercial property. Such prohibitions or restrictions shall not, however, constitute a means of arbitrary discrimination or a disguised restriction on trade between Member States* (emphasis added)";Gintare Surblyte 2011 (n 182) 47 further notes that trade secrets are not covered by Article 36 TFEU.

1074 Case 120/78 *Rewe-Zentrale AG v Bundesmonopolverwaltung für Branntwein (Cassis de Dijon)* [1979] ECR I-649, para 8: "Obstacles to movement within the Community resulting from disparities between national laws relating to the marketing of the products in question must be accepted in so far as those provisions may be recognized as being necessary in order to satisfy *mandatory requirements* relating in particular to the effectiveness *of fiscal supervision*, the protection of *public health, the fairness of commercial transactions* and the *defence of the consumer*" (emphasis added).

disclosure obligations after the termination of a contractual relationship might negatively affect the mobility of employees from one country to another. In the light of the foregoing, he convincingly concluded that the uneven legislative framework constituted an obstacle to trade and that harmonisation seemed the most appropriate mechanism to overcome it.[1075]

Aplin held a different view, which was largely based on the results of the Baker McKenzie Industry Survey referred to above. In the first place, she looked into the figures on the risk of exposure and the attempts at misappropriation suffered by the respondents in the last ten years. As regards the first, 38% of the enterprises were of the opinion that the risk had increased, whereas 20,5% reported at least one misappropriation attempt in the last decade. Out of those, only 5,2% had suffered more than five attempts. She considered that those numbers were not particularly alarming and cast doubt upon whether a harmonised system of protection would yield more investment in innovation. According to the survey, 29% of the respondents adopted different measures if they operated in several jurisdictions. In her view, this indicated that there would not be substantial savings in the means adopted by firms in protecting secrecy, which in turn would not result in a higher investment in R&D. The same rationale was applied in connection to collaborative research, as only 24% of the respondent companies were of the opinion that more collaborative opportunities would derive from the alignment of national legislation. However, it is here submitted that the fact that two out of ten market participants had suffered a misappropriation attempt in the last ten years and that three out of ten of the surveyed companies adopted different protection measures if they operated in more than one market seems persuasive enough to justify the alignment of national laws in the field of trade secrets.[1076]

With the above analysis in mind, the Preamble of the TSD clarifies that the competence to harmonise trade secrets protection across the EU stems from Article 114 TFEU, which sets forth the power of the Parliament and the Council to legislate on measures necessary to ensure the proper functioning of the Single Market. This aspect is further developed in several recitals, where it is explicitly stated that the existing scattered legal framework has a negative impact on the creation of a Single Market without internal barriers to trade.[1077]

1075 Ansgar Ohly 2013 (n 13) 39.

1076 Tanya Aplin 2014 (n 384) 260; the empirical survey commented results can be found in Baker McKenzie 2013 (n 1057) 126 and the following.

1077 See Recitals (4) and (8) TSD.

Notwithstanding this, legal scholars have warned of the excessive reliance of EU legislative powers on this provision to approximate national regimes, and the little attention that is often paid to whether the national divergences actually have a negative effect on intra-community trade.[1078] The CJEU in its *Tobacco Advertising* decision emphasised that Article 114 TFEU should serve as the legal basis only when the divergences among Member States are likely to hinder the Fundamental Freedoms and thus affect the good functioning of the Single Market.[1079] In this context, the role of the Impact Assessment as a means to examine the advisability of taking a legislative action at the EU level is becoming increasingly relevant, as it compels the EU legislature to take into consideration the advantages and disadvantages of each of the policy options analysed.[1080]

As noted above, the Commission prepared an Impact Assessment in which five potential policy options to address the fragmentation of the Single Market vis-à-vis trade secrets were examined. The first one was to maintain the existing status quo, i.e., keeping the scattered legal protection. The second alternative presented compelled Member States to raise awareness and provide information about the existing means of redress in the case of misappropriation of trade secrets. Option 3 considered the harmonisation of national civil law vis-à-vis the unlawful acts of misappropriation (but excluded remedies and the preservation of confidentiality of trade secrets during legal proceedings). Option 4, by contrast, called upon Member States to harmonise their legal regimes with regard to the available civil law remedies and to implement measures to ensure secrecy during litiga-

1078 Paul Craig and Gráinne de Búrca, *EU Law, Text, Cases and Materials* (5th edn, OUP 2011) 92-93; this point is further developed by Stephen Weatherhill, 'Competence Creep and Competence Control' [2004] 23 Yearbook European L 1.

1079 Case C–376/98 *Germany v European Parliament and the Council* [2000] ECR I–8419, para 84 where the Court noted that "(…) A measure adopted on the basis of Article 100a of the Treaty (now Article 114 TFEU) must genuinely have as its object the improvement of the conditions for the establishment and functioning of the internal market. If a mere finding of disparities between national rules and of the abstract risk of obstacles to the exercise of fundamental freedoms or of distortions of competition liable to result therefrom were sufficient to justify the choice of Article 100a as a legal basis, judicial review of compliance with the proper legal basis might be rendered nugatory. The Court would then be prevented from discharging the function entrusted to it by Article 164 of the EC Treaty (now Article 220 EC) of ensuring that the law is observed in the interpretation and application of the Treaty".

1080 Paul Craig and Gráinne de Búrca, *EU Law, Text, Cases and Materials* (5th edn, OUP 2011) 93.

tion. Finally, harmonising both civil law and criminal law remedies was also considered.[1081]

In the end, the preferred policy option was to align the laws of the Member States with regard to national civil law remedies against the misappropriation of trade secrets, that is, to implement option 4. This was deemed the most advantageous of the available alternatives, as it would allow the owners to seek protection vis-à-vis infringing parties and stop imports from third countries. According to the Impact Assessment, the harmonisation of rules that ensure the preservation of confidentiality during legal proceedings should boost litigation. All in all, legal certainty should be improved and, accordingly, cooperation between undertakings should also be facilitated. This should ultimately strengthen the incentives to innovate.[1082]

Consequently, the Impact Assessment concluded that the adoption of the TSD was justified on the basis of two grounds.[1083] Firstly, the ineffective protection of trade secrets discouraged innovation activities (including those that take place at a cross-border scale) due to, on the one hand, the low expected value of innovation relying on trade secrets and the higher costs of protecting it, and on the other, the "higher business risk when sharing trade secrets". This hindered innovation and creativity and diminished investment (Recital 4), which in turn lowered the incentive to engage in cross-border innovative activities (Recital 8). Secondly, it was suggested that the different scope of protection and means of redress available across the 28 Member States caused trade secrets holders to risk losing their competitive advantage and thus reduced their competitiveness. As a result, the Commission determined that there was a case for harmonisation.

C) Legal analysis of the TSD

The body of the TSD is divided into a Preamble and four chapters, from which the first three correspond to the three main areas of trade secrets law that are harmonised. The following sections critically analyse the main provisions of the Directive. In the first place, some general remarks regarding the principles that inform it are outlined (section I). Next, the subject matter and scope of application of the Directive are examined (section II).

1081 Impact Assessment (n 385) 57-58.
1082 Impact Assessment (n 385) 64-65.
1083 Impact Assessment (n 385) 40-41.

Section III then looks into the types of conduct that are considered lawful, as well as those that are considered infringing and the exceptions thereto. Finally, the main obligations in connection to the enforcement of trade secrets are analysed in section IV.

I. General remarks

A detailed analysis of the Directive reveals that the EU legislature has adopted a flexible approach in the regulation of trade secrets protection. This is apparent from the number of open-ended clauses that refer to the general standard of honest commercial practices (in line with Article 10bis(2) PC) enshrined in most of the provisions that regulate the scope of protection, the list of lawful means of acquisition, use and disclosure of trade secrets spelt out in Article 3 and the list of exceptions in Article 5.[1084] Flexibility is central in order to achieve a well-balanced Directive that allows for weighing up all of the relevant interests in each individual case.[1085] Nonetheless, this legislative technique may interfere with the harmonisation objective pursued by the TSD, as the meaning of "honest commercial practices" may be construed differently in each of the 28 Member States.[1086] In fact, this standard is mostly applied as part of the acquis communautaire in the field of trade marks and was excluded from the scope of the Unfair Commercial Practices Directive.[1087] Ultimately, divergences in this field should be solved by the CJEU as part of the EU secondary law interpretation.[1088]

The TSD provides for minimum harmonisation and explicitly mentions that Member States can establish stronger protection than that foreseen in the Directive.[1089] Nonetheless, certain restrictions have also been included

1084 This argument is raised in Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 10; Mary-Rose McGuire 2016 (n 824) 1006, particularly when compared with the German system as per §§ 17-19 UWG, which followed an "Alles-oder-Nichts-Prinzip" .

1085 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 6.

1086 Tanya Aplin 2014 (n 384) 260; a more detailed account of the meaning of the expression "honest commercial practices" is provided in chapter 2 § 1 A) III. 2).

1087 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 10.

1088 Tanya Aplin 2014 (n 384) 265; see further Article 267 of the TFEU. In the words of Martin Höpner, 'Der Europäische Gerichtshof als Motor der Integration' [2011] 21 Berlin J Soziol 203, 204: "The ECJ (now CJEU) has become the engine of European Integration".

1089 As per Recital 10 TSD.

in order to ensure compliance with specific obligations.[1090] Some of the most relevant ones provide that Member States shall not adopt higher standards as regards the definition of lawful acquisition, use and disclosure of trade secrets (Article 3) or interfere with the exceptions laid down in Article 5 of the Directive. In this context, it has been suggested that the maximum harmonisation approach adopted by the TSD precludes Member States from including additional exceptions and lawful means of acquiring a trade secret.[1091] With respect to the enforcement of secrets, national legal regimes should put in place the procedures, measures and remedies necessary to ensure the availability of civil redress against the misappropriation of trade secrets (Article 6(1)) and ensure that these are governed by the principles of fairness, equity and proportionality (Articles 6(2)) and 7(1)). In the interest of legal certainty, national legislatures are compelled to set forth a statute of limitations, which shall not exceed 6 years (Article 8). In line with the objective of protecting secrecy during litigation, Member States shall ensure that the parties, witnesses or any other persons that have access to a trade secret during the course of a misappropriation proceedings are not allowed to use it or disclose it after the legal proceedings have ended (Article 9(1)), provided that it has not become generally known or a final judicial decision has held that it does not meet the statutory requirements of protection. Likewise, as an alternative to precautionary measures, it shall always be possible to continue using an allegedly infringing secret upon the lodging of specific guarantees by the defendant to compensate for any eventual damage (Article 10(2)). However, this does not include the disclosure of the information. In addition, the possibility of granting an injunction and the conditions to which it is subject are regulated as a maximum standard of protection (Article 13).

To be sure, the minimum harmonisation approach conflicts with the ultimate goal of the Directive, i.e. to eliminate barriers within the internal

1090 Article 1(1) paragraph 2 TSD: "Member States may, in compliance with the provisions of the TFEU, provide for more far-reaching protection against the unlawful acquisition, use or disclosure of trade secrets than that required in this Directive, provided that compliance with Articles 3, 5, 6, Article 7(1), Article 8, the second subparagraph of Article 9(1), Articles 9(3) and (4), Articles 10(2), Article 11, 13 and Article 15(3) is ensured.

1091 Christian Alexander, 'Gegenstand, Inhalt und Umfang des Schutzes von Geschäftsgeheimnissen nach der Richtlinie (EU) 2016/943 1034' [2017] WRP 1034, para 19.

market.[1092] Allowing Member States to provide for stronger protection may also raise concerns as to the relationship between trade secrets and IPRs.[1093] From a policy perspective, strengthening the legal regime of trade secrets protection benefits the trade secret holder, but may also have a negative impact on cumulative innovative and creative activities, as there is social value derived from the sharing of information.[1094] However, the fact that reverse engineering and independent discovery are regarded as lawful means of acquiring secret information and at the same time maximum standards of protection prevents the creation of an exclusive right and ensures an equilibrium with the IPRs system (and particularly patent law), in accordance with the wording of Recital 16.

Another remarkable feature of the Directive is that many central aspects of trade secrets protection are left unregulated. The three most salient ones are: (i) non-disclosure and non-competition agreements after the termination of an employment relationship; (ii) the ownership of trade secrets in cooperation agreements; and (iii) the establishment of claims for information and preserving evidence.[1095] As regards the first of these, The Comments of the Max Planck Institute for Innovation and Competition ("the MPI Comments") highlight that despite the practical relevance of this topic, it does not appear likely that the Directive can provide a univocal answer that foresees all of the potential situations of conflict without interfering with national labour and contract law.[1096] The latter points will be dis-

1092 IFRA, 'Comments on the Proposal for a Directive on the Protection of Undisclosed Know-How and Business Information (Trade Secrets)' (2014) 2 <http://www.ifraorg.org/en-us/library/tag/21005/s0> accessed 15 September 2018; see further Valeria Falce 2015 (n 392) 958, arguing that full harmonisation would allow for ensuring uniform transposition among all 28 EU jurisdictions and creating a "level playing field so as to incentivize and facilitate know-how and the exchange of sensitive information agreements, as well as any form of cooperation among enterprises, inventors and trade secret owners operating in Europe"; similar Mary-Rose McGuire 2016 (n 824) 1005; however, industry representatives have welcomed such an approach, as they believe that the existing differences among Member States are an insurmountable obstacle and Member States should be able to establish stronger protection. In this regard see IP Federation, 'The EU Trade Secrets Directive' (2014) Policy Paper PP04/15, 1 <https://www.ipfederation.com/news/ip-federation-comments-on-the-compromise-text-for-the-eu-trade-secrets-directive/> 15 September 2018.

1093 Valeria Falce 2015 (n 392) 948.

1094 See chapter 1 § 2 B) II. on the incentives to disclose theory in the context of trade secrets.

1095 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) paras 8-9.

1096 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) paras 8-9.

cussed in connection with the concept of trade secret holder[1097] and the enforcement measures.[1098]

As a final observation, it should be highlighted that the TSD represents a step forward in the harmonisation of the law of unfair competition in the EU.[1099] In line with this, Recital 17 expressly mentions that because of reverse engineering activities, innovators and creators are exposed to parasitic competition and slavish imitation practices "that free ride on their reputation and innovation efforts".[1100] Hence, the Directive calls on the Commission to investigate whether there is a need to take EU-wide action in this area, although it notes that it is not the purpose of the TSD to harmonise unfair competition in general. The wording used in this recital raises concerns insofar as it does not seem to take into account that fairness and legal protection against parasitic copying and slavish imitation are viewed differently across EU jurisdictions[1101] and that the general principle in competitive economies is that of freedom of imitation, which may be limited only by the operation of IPRs.[1102] Ultimately, such a statement indicates that in the near future these areas will guide the Commission's legislative action.

1097 See chapter 3 § 5 C) II. 2.

1098 See chapter 3 § 5 C) IV.

1099 Valeria Falce 2015 (n 392) 957.

1100 Recital 17 TSD: "In some industry sectors, where creators and innovators cannot benefit from exclusive rights and where innovation has traditionally relied upon trade secrets, products can nowadays be easily reverse-engineered once in the market. In those cases, those creators and innovators may be victims of practices such as parasitic copying or slavish imitations that free ride on their reputation and innovation efforts. Some national laws dealing with unfair competition address those practices. While this Directive does not aim to reform or harmonize unfair competition law in general, it would be appropriate that the Commission carefully examine the need for Union action in that area".

1101 Hogan Lovells, 'Study on Trade Secrets and Parasitic Copying (Look-alikes) – Report on Parasitic Copying' (MARKT/2010/20/D) paras 106-109 (2012) <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwiy8tzludndAhWDaFAKHfYHC3UQFjAAegQICRAC&url=http%3A%2F%2Fec.europa.eu%2Finternal_market%2Fiprenforcement%2Fdocs%2Fparasitic%2F201201-study_en.pdf&usg=AOvVaw2Ws2o9bYEnYOj5RM9bFb8y> accessed 15 September; more generally Frauke Henning-Bodewig and others, *International Handbook on Unfair Competition* (C.H. Beck 2013) para 73.

1102 Ansgar Ohly, 'The Freedom of Imitation and Its Limits – A European Perspective' [2010] IIC 506, 520-524.

II. Scope of application and subject matter covered

1. Scope of application

Article 2 lays down the positive scope of application of the Directive, by defining the concepts of "trade secret",[1103] "trade secret holder", "infringer" and "infringing goods". Conversely, Article 1(2) sets forth the negative scope of application and expressly notes that the rules laid down in the Directive shall not affect the exercise of the fundamental rights of freedom of expression and information, as laid down in the ChFREU. In addition, the national and EU law provisions that mandate the disclosure of trade secrets for reasons of public interest shall remain unaffected. In a similar vein and in the interest of employee mobility, Article 1(3) clarifies that no restrictions on the mobility of employees can be grounded on the provisions of the TSD.[1104]

Recital 39 further delimits the material scope vis-à-vis other areas of law and expressly provides that the provisions set forth in the Directive shall not interfere with "the application of other relevant law in other areas including intellectual property rights and the law of contract". These clarifications are of paramount importance to ensure legal certainty, in particular with regard to employment relations.[1105]

In addition, Recital 35 provides that the rights and obligations embedded within the Data Protection Directive[1106] shall remain unaffected.[1107] In this regard, it should be noted that since the adoption of the TSD, the Data Protection Directive has been repealed by the General Data Protection Regulation ("GDPR"),[1108] which contains no express clarification as to its relationship with the TSD. However, since Recital 35 TSD expressly pro-

1103 A detailed account of the concept of trade secret laid down in the TSD is provided in chapter 4 § 3.

1104 See chapter 6 § 1 A).

1105 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) paras 14 and 15.

1106 Directive of the European Parliament and of the Council 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/0031 (Data Protection Directive).

1107 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) paras 14-15.

1108 Regulation (EU) 2016/679 of the European Parliament and of the Council of of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/01 (GDPR).

vides that the rights of the data subject to access, obtain the rectification, erasure or blocking of the data should not be affected by the TSD and as those same rights are included in the GDPR, it seems that the general principle embedded in Recital 35 TSD should also govern the relationship with the GDPR.[1109] Yet, uncertainty remains as to the relationship between the TSD and the new rights envisaged in the GDPR, such as data portability.[1110] Furthermore, Recital 63 GDPR notes that the right of access to personal data by the data subject "should not adversely affect the rights or freedoms of others, including *trade secrets* or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject". Therefore, it seems that the observance of the rights laid down in the TSD is not absolute and, depending on the specific circumstances of the case, the data subject may have the right to access his personal information, even if it constitutes a trade secret or part of it. Similar concerns were presented in the Opinion of the European Data Protection Supervisor, where it was expressly recommended that an adjudication process be created including national protection authorities, in the event that tension arose between the data subject rights and the trade secret holder rights.[1111]

The relationship between the Enforcement Directive and the TSD is also problematic. Recital 39 TSD provides that in the event that the two overlap, the application of the latter should be favoured as lex specialis.[1112] This statement begs the question of whether the Enforcement Directive is to be

1109 Surblyte Gintare, 'Data Mobility in the Digital Economy' (2016) Max Planck Institute for Innovation & Competition Research Paper No. 16-03, 15 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2752989> accessed 15 September 2018.

1110 Ibid.

1111 See European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the proposal for a directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure' (2014), para 22 <https://edps.europa.eu/data-protection/our-work/publications/opinions/protection-undisclosed-know-how-and-business_en> accessed 27 September 2018.

1112 Recital 39 TSD provides that: "This Directive should not affect the application of any other relevant law in other areas, including intellectual property rights and the law of contract. However, where the scope of application of Directive 2004/48/EC of the European Parliament and of the Council and the scope of this Directive overlap, this Directive takes precedence as lex specialis".

applied to trade secrets in those areas that are not regulated in the latter Directive, namely with regard to the obligation to provide and preserve evidence,[1113] information duties,[1114] and the liability of intermediaries.[1115] Indeed, in 2005 the Commission issued a statement on the rights that were deemed to fall under the scope of protection of the Enforcement Directive and no reference to trade secrets or unfair competition was made.[1116] Notwithstanding this, according to Recital 13 of the Enforcement Directive, Member States are free to extend its scope of application to unfair competition. Against this background, a few jurisdictions have extended the obligations enshrined in the Enforcement Directive to the protection of undisclosed information.[1117] In this respect, it should be noted that during the initial stage of the TSD negotiations, the Commission considered whether the application of the Enforcement Directive to trade secrets would be an adequate solution to achieve effective protection across the Single Market. This option was dismissed based on the argument that trade secrets were not an IPR.[1118] In view of the remaining uncertainty, it is argued that the relationship between the Enforcement Directive and the Trade Secrets Directive will most likely have to be clarified by the submission of a preliminary question to the CJEU.

Another potentially conflicting aspect that has already been outlined above is the applicable law from a private international law perspective, which is explicitly excluded from the scope of the Directive pursuant to Recital 37.[1119] The law applicable to IPR infringement disputes is governed by Article 8, para 1 of the Rome II Regulation (the law of the place in

1113 Articles 6 and 7 Enforecement Directive.

1114 Article 8 Enforcement Directive.

1115 Article 11(3) of the Enforcement Directive.

1116 Commission, 'Commission Statement concerning Article 2 of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights' [2005] OJ L94/37: "The Commission considers that at least the following intellectual property rights are covered by the scope of the Directive: copyright, rights related to copyright, sui generis right of a database maker, rights of the creator of the topographies of a semiconductor product, trademark rights, design rights, patent rights, including rights derived from supplementary protection certificates, geographical indications, utility model rights, plant variety rights, trade names, in so far as these are protected as exclusive property rights in the national law concerned".

1117 Italy, Portugal, Slovak Republic, Rumania and arguably the UK, as noted in Baker McKenzie 2013 (n 1057) 26.

1118 Impact Assessment (n 385) 267-268.

1119 See chapter 1 § 3 B) III; see further Recital 37 TSD: "This Directive does not aim to establish harmonised rules for judicial cooperation, jurisdiction, the

which the damage occurs). By contrast, if trade secrets misappropriation is regarded as an act against unfair competition, Articles 6 and 4 of the Rome II Regulation should be applied (the law of the place in which protection is sought). For the sake of legal certainty, it would have been advisable for the TSD to clarify the applicable law in the case of infringement, even though it clearly seems to lean towards an unfair competition approach.[1120]

As a final remark, it is worth noting that the Directive is limited to civil redress, despite the fact that the comparative law study carried out by Hogan Lovells shows that there are substantial disparities as regards the configuration of criminal penalties and the sanctions imposed in the event of trade secrets infringement.[1121] In the Impact Assessment, the Commission took the view that the alignment of criminal law provisions in the field of trade secrets was not appropriate owing to the lack of harmonisation of criminal law at the EU level, the potential deterrence effect it may shield in regard to employment mobility, and the proportionality principle that governs criminal law.[1122]

2. Definition of trade secret holder and infringer

The concept of "trade secret holder" is defined in Article 2(2) as a natural or legal person who is *lawfully in control of the information*, in line with Ar-

---

recognition and enforcement of judgements on civil and commercial matters, or deal with applicable law. Other Union instruments which govern such matters in general terms, should, in principle, remain equally applicable to the field covered by this Directive"; and as noted by Thomas Hören and Reiner Münker, 'Die EU-RL für den Schutz von Geschäftsgeheimnissen und ihre Umsetzung' [2018] WRP 150, 151 para 4.

1120 This is developed in Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 17.

1121 Hogan Lovells 2012 (n 793) paras 254-256.

1122 Impact Assessment (n 385) 64-65; Björn H. Kalbfus, 'Die EU-Geschäftsgeheimnis-Richtlinie - Welcher Umsetzungsbedarf besteht in Deutschland?' [2016] GRUR 1009, 1009; the consultations for the Directive started while the Anti-Counterfeiting Trade Agreement (ACTA) was still being negotiated and was eventually rejected by the European Parliament on June 2012. In this post-ACTA scenario, the Commission considered that any attempt to harmonise criminal sanctions would face strong opposition from the Parliament and the citizens of the EU in general.

ticle 39(2) TRIPs.[1123] Article 4(1) further adds that the trade secret holder is the person entitled to apply for the measures, procedures and remedies set forth in chapter III of the Directive.

Against this background, it might be noted that the Directive does not refer to the owner, but instead resorts to the notion of *control*.[1124] Hence, the decisive factor is not who has created the information, but rather who exercises control over it.[1125] Yet, the TSD does not provide any rules regarding the assessment of the control over the information and the establishment of the ownership of trade secrets; this is left unregulated.[1126] Accordingly, it is up to the Member States to set forth the rules that determine who is the rightful holder and who has a standing to sue. This is particularly relevant in the context of collaborative agreements and with regard to the possibility that exclusive and non-exclusive licensees bring legal action against alleged infringers,[1127] in contrast to the DTSA, which refers to "owners".[1128] The wording used by the Directive also leaves open whether those who obtain a trade secret after reverse engineering a marketed product or employees who gain knowledge of secret information during the course of their employment with consent should also be regarded as trade secret holders.[1129] It has been suggested that the Directive should not aim at providing such a detailed and precise regulation, but instead it should be agreed upon contractually between the parties or determined by the application of the relevant law.[1130] Indeed, the ownership of trade secrets is largely dependent on the regulation of employee creations and in-

1123 Article 39(2) TRIPs provides that: "*Natural and legal persons* shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices (10) so long as such information (…)" (emphasis added).

1124 On this specific issue, the TSD differs from the DTSA, pursuant to which only owners have legal standing.

1125 Thomas Hören and Reiner Münker 2018(b) (n1119) para 9.

1126 Thomas Hören and Reiner Münker 2018(b) (n1119) para 9.

1127 Tanya Aplin 2015 (n 306) 435.

1128 Further Victoria A. Cundiff and others 2016 (n 789) 740 note that: "Plaintiffs may argue that this definition confers standing to more than just the owner or exclusive licensee of the trade secret, such as non-exclusive licensee who controls the trade secret, which potentially broadens the application of the Directive as compared with the DTSA".

1129 Tanya Aplin 2014 (n 384) 264; Christian Alexander 2017 (n 1091) para 69 convincingly argues that those that create the trade secret independently should also be regarded as trade secret holders.

1130 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 9.

ventions, which in most Member States consist of a piecemeal regulation in the employment and labour statutes.[1131] Consequently, aligning the regulations of Member States with regard to such a complex topic might have exceeded the scope of harmonisation in the context of trade secrets. However, the absence of a uniform approach may lead to a divergent solution among Member States' courts and may potentially interfere with the harmonisation goals pursued by the Directive.[1132]

At the other end of the spectrum, the term infringer is defined as "any natural and legal person who has unlawfully acquired, used or disclosed trade secrets". This provision is one of the milestones of the Directive, as it provides common ground across the EU on the potential liability of legal persons for trade secrets misappropriation.

3. Infringing goods

The term infringing goods is used to refer to "goods the design (in French "*conception*"), characteristics, functioning, production process or marketing of which significantly benefit from trade secrets unlawfully acquired, used or disclosed". This definition poses a number of interpretative questions, particularly in connection with the causal relationship between trade secrets and the infringing goods.

Firstly, in accordance with Recital 26 TSD, it appears that the term "infringing goods" refers both to products and the provision of services. However, while it is true that establishing causality between the design and manufacturing process of a product and a trade secret may be rather straightforward, this appears more problematic in other instances, such as in the provision of services based on the unlawful acquisition, use or disclosure of a trade secret or the marketing strategy followed to commercialise certain products. In particular, it has been suggested that according to the literal wording of Article 2(4) TSD, if a company unlawfully acquires a competitor's customer list to position his products in the marketplace better, the product as such may be considered as infringing, even though its characteristics bear no connection with the misappropriated

1131 For an overview of the provisions that govern the ownership of employee inventions in Germany see Kurt Bartenbach and Franz-Eugen Volz, *Arbeitnehmererfindungen* (6 edn, Carl Heynemanns Verlag 2014).

1132 Tanya Aplin 2014 (n 384) 265.

list.[1133] In this respect, the MPI Comments convincingly conclude that it is beyond the scope of the Directive to regard as infringing products that are commercialised under a marketing campaign that was conceived on the basis of an unlawfully acquired customer list.[1134]

In this context, it is worth noting that initially the Draft Proposed by the Commission in 2013 referred to goods, the *quality* of which significantly benefitted from the misappropriated trade secret. The inclusion of this term was vehemently criticised, as it was noted that ascertaining the relationship between the quality of a product and a trade secret is extremely difficult. It was argued that the term "characteristics" was more suitable, as it encompassed a broader spectrum of features other than just its quality. In the final version of Article 2(4), the expression "quality" was replaced by "characteristics".[1135] However, surprisingly Recital 28 still refers to the quality of the product resulting from the misappropriation of trade secrets in the context of the seizure of products and the prohibition of importation, which may lead to an over-extensive application of this provision.

Indeed, requiring that the "infringing goods" "significantly benefit" from the allegedly infringed trade secret seems a very open-ended standard that puts little emphasis on the causal link between the production of the goods and the actual use of a trade secret.[1136] This benchmark is manifestly different to the test usually applied in other fields of intellectual property.[1137] For instance, in patent law, in order to find an infringement it is required that the products are "directly" obtained from the patented pro-

1133 Thomas Hören und Reiner Münker 2018(a) (n 860) 86.

1134 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 23; GRUR, 'Opinion on the proposal for a Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, COM (2013) 813 final', para 1.b) <http://www.grur.org/uploads/tx_gstatement/2014-03-19_GRUR_Stellungnahme_zum_Know-how-Schutz_EN.pdf> accessed 15 September 2018 .

1135 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 23.

1136 GRUR, 'Opinion on the proposal for a Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, COM (2013) 813 final', 5 <http://www.grur.org/uploads/tx_gstatement/2014-03-19_GRUR_Stellungnahme_zum_Know-how-Schutz_EN.pdf> accessed 15 September 2018; also Thomas Hören und Reiner Münker 2018(a) (n 860) 86; Björn H. Kalbfus 2016 (n 1122) 1014.

1137 Tanya Tanya Aplin 2014 (n 384) 267-269.

cess[1138] or that a third party knows that the means supplied to him are intended to infringe a patented invention.[1139]

Against this background, some have suggested that if at least half of the total expenditure required for the development, production or distribution of a product can be attributed to the trade secret, it should be regarded as "infringing".[1140] However, such an absolute test seems too rigid, because with complex products that incorporate multiple inventions (for example, smart phones), if only one of them is misappropriated, it is likely that it represents less than 50% of the total expenditure in view of the other inventions incorporated in the product. However, the product as such should be considered as infringing. Consequently, it is submitted that courts should follow a more nuanced approach, whereby the percentage of expenditure in the development, production and marketing is just one of the factors to be taken into consideration, alongside the importance of the information for the commercial success of the product or service rendered or the potential harm to the lawful holder, to name some. In this regard English courts resort to a degree test in order to consider whether a given product infringes a trade secret, which seems particularly pertinent:[1141]

> It is not every derived product, process or business which should be treated as camouflaged embodiment of the confidential information and not all on-going exploitation of such products, processes or business should be treated as continued use of the information, it must be a matter of degree whether the extent and importance of the use of the confidential information in such a continued exploitation of the derived material should be viewed as continued use of the information.[1142]

In the light of the previous arguments, it appears that courts will have to emphasise the need to establish a causal link between the trade secret and the allegedly infringing good, which will ultimately be a matter of degree. Otherwise, the potential to regard goods as infringing may be too far-

1138 See Article 64(2) EPC: "If the subject matter of the European patent is a process, the protection conferred by the patent shall extend to the products directly obtained by such process"; see further Article 25 Agreement on a Unified Patent Court.

1139 Agreement on a Unified Patent Court [2013] OJ C175/1 (Agreement on a Unified Patent Court), Article 26 (1).

1140 Christian Alexander 2017 (n 1091) para 107.

1141 Tanya Aplin 2014 (n 384) 268.

1142 *Ocular Sciences Ltd v Aspect Vision Care Ltd* [1997] RPC 289, [404].

reaching, much broader than the concepts traditionally applied in intellectual property law and expand to items that bear no factual connection with the confidential information in question. Ultimately, this may impose undue limitations on the ability of other market participants to commercialise competing products.[1143]

III. Scope of protection: the assessment of misappropriation and lawful conducts

Chapter III of the Directive sets forth the circumstances under which the acts of acquisition, use and disclosure of trade secrets are deemed lawful (Article 3) or unlawful (Article 4), and the exceptions thereto (Article 5). The following sections delve into the study of the scope of protection of the TSD following the systematic structure of this chapter. Hence, it starts by examining the cases of lawful acquisition, use and disclosure (section 1); next, it looks into the regulation of the types of infringing conduct (section 2) and finally it studies the exceptions to the latter (section 3).

1. Lawful acquisition, use and disclosure

Article 3 spells out a number of types of conduct that should be considered lawful, thereby enhancing legal certainty for market participants[1144] and maintaining the equilibrium with the intellectual property law system. From a systematic perspective, the types of conduct regulated under Article 3 seem to exclude ex ante liability for misappropriation, while the exceptions set out under Article 5 require the competent judicial authorities to carry out a balancing test, taking into account the specific circumstances of the case.[1145]

Firstly, in accordance with most Member States' practice, the Directive clarifies that independent discovery or creation shall be considered lawful means of acquiring undisclosed information (Article 3(1)(a) TSD). This topic is discussed further in chapter 6[1146] as one of the limitations to secrecy. For now, it suffices to note that regarding independent discovery as a

1143 Christian Alexander 2017 (n 1091) para 107.
1144 Christian Alexander 2017 (n 1091) para 74.
1145 Thomas Hören and Reiner Münker 2018(b) (n 1119) para 19.
1146 Chapter 6 § 2 A).

lawful way to acquire confidential information is consistent with the fact that trade secrets are not deemed the object of an exclusive right (Recital 16) and at the same time maintains the balance with the intellectual property system.[1147]

One of the milestones of the Directive is the introduction of a general clause that allows for reverse engineering lawfully acquired products. Article 3(1)(b) defines this as the "Observation, study, disassembly or test of a product or object that has been made available to the public or that is lawfully in the possession of the acquirer of the information who is free from any legally valid duty to limit the acquisition of the trade secret".

The establishment of common ground rules on reverse engineering represents a major step forward in the light of the divergent interpretations adopted by the EU Member States[1148] and their economic impact on the Internal Market.[1149] Indeed, with the introduction of the general reverse engineering exception, the EU has taken a similar approach to the governing principle in the U.S., where it has been accepted for many years and is deemed a necessary counterbalance to the patent system. In effect, the U.S. Courts and the DTSA regard reverse engineering as a valid and powerful defence against misappropriation actions.[1150] The implications of such an approach for the interpretation of secrecy are further discussed in chapter 6.[1151]

In addition, Article 3(1)(c) deems lawful the acquisition of information that constitutes a trade secrets if it is acquired by employees (or employees'

1147 James Pooley 2002 (n 66) § 5.01[1] 5-3.

1148 In Germany, for instance, reverse engineering was not allowed as such. Following the German Federal Supreme Court Decision RGZ 1935 149, 329, 335– *Stiefeleisenpresse*, courts should assess whether the information is obtained through great difficulty and cost, that is, whether it is secret. If that is the case, the obtention of information through reverse engineering will be deemed unlawful.

1149 Baker McKenzie 2013 (n 1057) 125.

1150 Against this background, it is important to note that the UTSA does not expressly refer to independent creation or reverse engineering as exceptions to the rights in a trade secret; Roger M. Milgrim 2014 (n 160) § 1.05(2), 1.07(01) argues that courts have regarded both of them as an inherent corollary to the secrecy requirement. Consequently, a number of States have incorporated these exceptions into the wording of their Trade Secrets Acts. This is the case of § 3426.1(a) of the California Civil Code.

1151 Chapter 6 § 2 B).

representatives) during the exercise of their right to information and consultation, as regulated under EU or national statues.[1152]

In line with the flexibility principle that informs the Directive, Article 3(1)(d)[1153] resorts to a broad unfair competition clause and provides that the acquisition of a trade secret should be regarded as lawful so long as it is in accordance with honest commercial practices. Ultimately, the appraisal of whether secret information has been lawfully acquired will depend upon the interpretation of the *broader* and *splendidly imprecise* expression of what is regarded as "honest commercial practices".[1154] As noted above, such a flexible approach may contribute to enhancing the legal fragmentation among Member States, but at the same time may allow for better adaptation to the evolving technological means and the different legal traditions. Some have in fact drawn parallels between this provision and the fair use limitations that govern trade mark and copyright limitations in the U.S. legal system.[1155]

Finally, Article 3(2) provides that the acquisition, but also the use and disclosure mandated or permitted pursuant to EU or national provisions should be deemed lawful.[1156]

2. Types of infringing conduct

In line with the minimum standards set out in Article 39(2) TRIPs, the EU legislator stipulated that the unlawful acquisition, use and disclosure of trade secrets constitute infringing types of conduct. Due to their broad scope, these rules appear to be related more to unfair competition than to intellectual property law provisions, which seems to indicate that the Directive leans towards an unfair competition approach, even though this is not expressly mentioned in the text.[1157] Remarkably, the Directive does not define any of the infringing types of conduct. Instead, the EU legisla-

---

1152 Christian Alexander 2017 (n 1091) para 74.

1153 Ultimately, the unlawful acquisition, use and disclosure of secret information is premised on acts contrary to honest commercial practices, as per Art 4(2)(b) TSD.

1154 For a detailed account of the interpretation of the "honest commercial practices" see chapter 2 § 1 A) III. 2.

1155 Thomas Hören and Reiner Münker 2018(b) (n 1119) para 23.

1156 This is discussed further in chapter 4 § 4 C) 2. c).

1157 Contrary, Mathias Lejeune 'Die neue EU Richtlinie zum Schutz von Know-How und Geschäftsgeheimnissen' [2016] CR 330, 331.

ture preferred to spell out a list of examples and included a final open-ended clause that refers to the general standard of "general commercial practices" enshrined in Article 10bis PC with regard to unlawful acquisition. Consequently, some commentators have argued that Article 4 sets forth a "blacklist" of types of conduct that, when carried out by the infringer, are *objectively* deemed unlawful (strict liability).[1158] However, this statement is not completely accurate, particularly because the liability of third parties and importers requires at least gross negligence.

In the light of the above consideration, the following four sections look into the types of conduct that are deemed illicit by the Directive, namely the unlawful acquisition of secret information (section a); the unlawful use and disclosure of trade secrets (section b); the liability of third parties (section c); and the import and export of infringing goods (section d).

a) Unlawful acquisition

Pursuant to Article 4(2), the acquisition of a trade secret will only be regarded as unlawful if it is carried out without the consent of the trade secret holder.[1159] Next, the Directive provides a number of examples of actions that are to be considered unlawful acquisition of undisclosed information. These are the "unauthorised access to, appropriation of, or copy of any documents, objects, materials, substances or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deduced".[1160] Thereupon, section (b) clarifies that any other conduct contrary to honest commercial practices may also be deemed an unlawful acquisition under the circumstances. Thereby, it expands the scope of Article 4(2) beyond the acts previously listed. Ultimately, the inclusion of such a flexible clause is in line with Article 10bis of the PC and Article 39(2) TRIPs and underscores the unfair competition nature of the protection afforded by Directive.[1161] It also provides sufficient leeway to adapt to future technological developments that

1158 Mary-Rose McGuire 2016 (n 824) 1007-1006; Clemens Koós, 'Die europäische Geschäftsgeheimnis-Richtlinie – ein gelungener Wurf? Schutz von Know-How und Geschäftsinformationen – Änderungen im deutschen Wettbewerbsrecht' [2016] MMR 224, 225.

1159 Björn H. Kalbfus 2016 (n 1122)1013.

1160 Article 4(2)(a) TSD.

1161 Thomas Hören and Reiner Münker 2018(b) (n 1119) 152.

may create new means of misappropriating information that could not have been foreseen at the time that the TSD was drafted.

At this point, it is worth noting that in the first draft presented by the Commission, "intentionality" or "gross negligence" were prerequisites to regard an acquisition as unlawful. Yet, such an approach was criticised because these standards of fault should only be taken into consideration in the establishment of sanctions, not vis-à-vis the infringing conduct as such.[1162] In addition, it was suggested that section (b), which has an overarching effect, is an unfair competition law provision, where fault is not a requirement to find liability.[1163] In this context, it is not required that the acquisition of a trade secret is detrimental to the trade secret holder or that it is carried out "for the purposes of competition", "for personal gain", "for the benefit of a third party", or "with the intent of causing damage to the owner of the business or trade secret holder", as required by several national jurisdictions before the adoption of the Directive, such as Spain (Article 13(3) of the Spanish Unfair Competition Act) and Germany (as per § 17 UWG).

In the Commission's draft, additional examples of types of infringing conduct were also included, namely theft, bribery and deception. However, these are criminal law concepts that require, at least, an implicit intent on the part of the infringer to be actionable. Gross negligence is insufficient to find criminal liability in these cases.[1164] More importantly, these offences have not been harmonised across the 28 EU Member States. Therefore, inconsistencies in their interpretation may have arisen, thus hampering the ultimate harmonisation objective.[1165] In view of this, in the final version "intentionality" and "gross negligence" were omitted as preconditions to find an infringement under Article 4(2).[1166] Similarly, theft, bribery and deception were deleted from this provision, in line with the exclusion of harmonisation in the field of criminal sanctions. However, this has given rise to some criticism from commentators, who understand

1162 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 27 noting that "as a matter of principle, fault on the part of the infringer should only play a role when determining the sanctions. As such, a claim for damages usually requires fault, while it is not taken into consideration in a claim for injunctive relief"; Mary-Rose McGuire 2016 (n 824) 1007; Mathias Lejeune 2016 (n 1157) 334.

1163 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 27.

1164 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 27.

1165 Tanya Aplin 2014 (n 384) 265.

1166 Thomas Hören and Reiner Münker 2018(b) (n 1119) 153.

that the mere fact that any of the types of conduct spelt out in Article 4(2) TSD are objectively carried out allows for the application of the sanctions set out in chapter III of the TSD is at odds with many national legal regimes (namely Germany) and equates trade secretes protection with IPRs protection.[1167]

b) Unlawful use and disclosure

Article 4(3) regulates the unlawful "use" and "disclosure" of trade secrets. The term "use" refers to the commercial exploitation of the secret in any manner, whereas the term "disclosure" captures the act of making available information to unauthorised third parties or the general public.[1168]

Just as in the case of unlawful acquisition, this provision also requires lack of consent. In addition, the infringer (a) must have acquired the trade secret unlawfully, as per article 4(2); or (b) must be in breach of a confidentiality agreement or a duty to maintain secrecy; or (c) must be in breach of a contractual or any other duty to limit the use of the trade secret.[1169]

Following the legal reasoning applied above in connection with unlawful acquisition, intentionality and gross negligence were deleted from the final draft as preconditions for finding liability in the case of unlawful use and disclosure.[1170] This has not been without criticism, as many have suggested that the objective nature of the liability set forth in paragraphs 2 and 3 of Article 4 affords intellectual property-like protection to trade secret holders, because if the types of conduct that they refer to are objectively carried out, they will trigger the same consequences as formal IPRs infringement.[1171] However, such an approach disregards the fact that Article 3 and 5 seem to provide sufficient safeguards against erga omnes enforcement of trade secrets irrespective of the manner in which the information is acquired. Consequently, the EU legislature rightfully stipulated that fault should only play a role in connection to acquisition by third parties, as discussed in the following section.[1172]

1167 Thomas Hören and Reiner Münker 2018(b) (n 1119) 153.
1168 Christian Alexander 2017 (n 1091) para 74.
1169 Mathias Lejeune 2016 (n) 333-334.
1170 Tanya Aplin 2014 (n 384) 265.
1171 Thomas Hören and Reiner Münker 2018(b) (n 1119) para 15.
1172 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 31.

c) Third party liability

The term "third party liability" refers to those situations where information is obtained from someone who is under an obligation of confidence or someone who has acquired it unlawfully, and it is subsequently used or disclosed by the third party, who has not breached any duty of confidence as such, or employed improper means to obtain it. This issue is addressed in Article 4(4) of the Directive, which to a large extent mirrors the wording of § 1(2)(ii)(B) UTSA.[1173] In essence, it expands the scope of the unlawful use or disclosure of a trade secret to any third parties who knew or should have known under the circumstances that the information was acquired by a person who acquired it, used it or disclosed it unlawfully.[1174] The secret may have been obtained directly or indirectly from another person.

The wording of Article 4(4) refers to "knowledge" and the fact that the trade secret holder "should have known under the circumstances" that the information was unlawfully acquired. This seems to introduce an element of fault in the appraisal of liability by imposing a duty of care on the side of the acquirer, in line with footnote 10 of the TRIPs Agreement, where gross negligence (not strict liability) is the applicable liability standard in the case of third party acquisition.[1175] The rationale behind this provision is to prevent third parties hiding behind a so-called "veil of wilful ignorance".[1176] However, this has also given rise to criticism from some commentators, who believe that the fact that the mere "knowledge" and "gross negligence" in the use of a trade secret illicitly obtained suffices to trigger the sanctions set out in chapter III of the Directive leads an overprotection of the trade secret holder.[1177] Such an approach seems to be in line with the prevailing case law in England, but broadens the liability of third par-

1173 § 1(2)(ii)(B) UTSA provides that, "Misappropriation includes acquisition by one who knows "or has reason to know" that the secret was acquired by improper means, or who gets it from such a person and thereafter uses or discloses it"; in a similar vein, see Restatement (Third) of Unfair Competition § 40 (Am. Law Inst. 1995) comment d.

1174 Article 4(4) TSD.

1175 Mathias Lejeune 2016 (n 1157) 334; footnote 10 of the TRIPs Agreement, provides as an example of practices contrary to honest commercial practices in the context of undisclosed information "the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition".

1176 James Pooley 2002 (n 66) § 6.04[1] 6-31.

1177 Thomas Hören and Reiner Münker 2018(b) (n 1119)153.

ties in Germany, which is limited to conditional intent ("*Vorsatz*" or "*Bedingter Vorsatz*").[1178]

This complex scenario is best illustrated with an example. Let us take for instance the case of a supplier of raw materials (Raw S.L.) that provides exclusively all the necessary materials and compounds to a French cosmetic firm (Beauty Care) for the production of a very effective antiaging cream (Stop fine lines), which competitors have since unsuccessfully tried to reverse engineer and which is the company's most valuable trade secret. As the sole supplier, the members of the Board of Raw S.L. and its chemists (Mr. Smith) have had access to the formula of Stop fine lines under strict confidentiality obligations. After some years, the parties cannot reach an economic agreement and the supply contract is terminated. A few weeks after the termination of the agreement, Raw S.L. approaches a competing cosmetic company in Germany (SKIN Harmony) claiming that it has developed a cream that is just as effective as Stop fine lines (the so-called "Magic Cream") and offers to provide the formula to SKIN Harmony under the condition that Raw S.L. becomes the sole provider of SKIN Harmony. Once the new product reaches the market, SKIN Harmony realises, upon receiving a cease and desist letter from Beauty Care, that the new competing product in fact uses the secret formula of their best-selling cream Stop fine lines, with a few minor variations regarding the perfume used. Under this factual scenario and following the new Directive rules, Raw S.L. could be held liable for trade secrets infringement pursuant to Article 4(3) (unlawful disclosure) and SKIN Harmony under Article 4(4) from the date on which the cease and desist letter was sent.[1179]

Against this background, Article 13(3) TSD along with Recital 29 provides further guidance regarding the potential liability of a legal or natural person who gained knowledge of a trade secret in good faith but after some time became aware that the information had been acquired from the original holder in an unlawful manner. In such a case, where appropriate, instead of granting injunctions or corrective measures that would disproportionately affect the third party, national courts shall award a pecuniary compensation (i.e. damages in lieu of injunction), in line with the bona

1178 Björn Kalbfus 2016 (1305) 1014.

1179 To avoid such situations in the context of departing employees, in the U.S. it is a common practice that employers demand that their new employees sign written statements declaring that their new position will not require them to breach any duty of confidence; see further James Pooley 2002 (n 66) § 6.04[1] 6-31.

fide defence for value discussed in the context of England.[1180] This should not exceed the amount of a reasonable royalty for the period of time for which the use of a trade secret could have been prevented, as analysed below.[1181]

Finally, the liability of third parties in the digital age raises the question of whether intermediary service providers (such as Reddit or Facebook) may be considered liable under Article 4(4) TSD for the mere hosting of information that was unlawfully acquired, used or disclosed by a third party that uses the services provided by these intermediaries to disseminate the trade secret. In particular, liability may arise if upon being notified by the trade secret holder about the infringing nature of the information, the intermediary service provider does not proceed to take it down. In such a context, it may be considered that the intermediary is carrying out a disclosure that triggers liability under Article 4(4) TSD and which falls outside of the scope of the hosting safe harbour established in Article 14(1) of the Directive on electronic commerce.[1182] Pursuant to paragraph (a) of this this provision, "actual knowledge" of the infringing conduct triggers liability for the service provider. Considering this uncertainty and the fact that the TSD does not allude to the responsibility of intermediaries, unlike Article 11 of the Enforcement Directive, it seems that the CJEU will ultimately have to provide guidance regarding the potential liability of intermediary service providers for the disclosure of trade secrets that they host, the relationship between the TSD and Article 11(3) of the Enforcement Directive and the applicability of the safe harbour established in Article 14(1) of the Directive on electronic commerce.

d) Import and export

Article 4(5) of the Directive sets out additional circumstances that constitute an unlawful use of a trade secret. This paragraph aims to preserve the good functioning of the internal market against (i) the exportation of infringing goods manufactured within the EU into another Member State,

1180 Chapter 3 § 3 C) II. 2. d).
1181 Chapter 3 § 5 C) IV. 4. b).
1182 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178 (Directive on Electronic Commerce).

and (ii) the importation of goods manufactured outside the Single Market. The wording of the provision is as follows:

> The production, offering or placing on the market of infringing goods, or the importation, export or storage of infringing goods for those purposes, shall also be considered an unlawful use of a trade secret where the person carrying out such activities knew, or ought, under the circumstances, to have known that the trade secret was used unlawfully within the meaning of paragraph 3.

In the Explanatory Memorandum, the Commission noted that in recent years confidential information has become increasingly vulnerable due to a number of factors, including globalisation, outsourcing, longer supply chains and the increased use of ICT. This, in turn, can lead to a situation where goods manufactured outside of the EU by an infringer have to compete in the internal market with those produced by the trade secret holder.[1183] Accordingly, Recital 28 highlights the importance of banning the importation or storage of these goods with the aim of putting them into the market. Such a prohibition has crystallised in Article 4(5), reproduced above, and appears to echo the spirit of the ACTA, which was finally rejected by the European Parliament in July 2012 after a long and controversial negotiation process.[1184]

The starting point of this analysis should be to note that Article 4(5) TSD proscribes the use of infringing goods and not the trade secret as such.[1185] It suffices that the traders know or have reason to know that the products derived from the trade secrets of a third party are being unlawfully produced, offered or placed in the market, or exported, imported or stored for any of these purposes.[1186] In such a context, the liability of importers and exporters extends to every member of the distribution chain who had "knowledge" or should have known under the circumstances that the trade secret was used unlawfully. Consequently, the applicable stan-

1183 Commission, 'Explanatory Memorandum of the Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure' 3.

1184 In essence, the Agreement aimed at strengthening the effective enforcement of IPRs at an international level vis-à-vis "the proliferation of counterfeit and pirated goods".

1185 Thomas Hören und Reiner Münker 2018(a) (n 860) 86.

1186 Thomas Hören und Reiner Münker 2018(a) (n 860) 86.

dard of liability is the same one as with respect to third parties, as set out in Article 4(4) TSD.[1187]

To be sure, the rules spelt out in Article 4(5) affect not only the export of products from third countries, but also intra-Community trade, which may lead to restraint of the free movement of goods under Article 34 TFEU.[1188] Such a limitation could nonetheless be justified as a mandatory requirement to protect fair competition following the *Cassis de Dijon* Doctrine and its subsequent development by the CJEU.[1189] Yet, forbidding the production, offering or placing in the market of infringing goods already ensures the protection of trade secrets across the 28 Member States. Hence, as argued in the MPI Comments, such a restriction appears unnecessary and should only be taken into consideration as regards export and import activities vis-à-vis third countries.[1190] The MPI Comments also convincingly note that the Directive should have expressly clarified that any importing and exporting conduct that is carried out for personal use is not to be regarded as infringing, based on the fact that the personal use of goods that embody a trade secret is not regarded as unlawful either.[1191]

Finally, it should be stressed that trade secrets do not fall under the scope of the Customs Regulation[1192] and that the Directive does not refer to the establishment of any border control measures, which may facilitate the entrance of infringing goods into the Single Market. This, on the other hand, is consistent with the fact that trade secrets are not regarded as an exclusive right and thus should not fall under the scope of protection of a Regulation that deals with the enforcement of IPRs by customs authorities.

1187 Thomas Hören and Reiner Münker 2018(b) (n 1119) para 18.

1188 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 34.

1189 See chapter 3 § 5 B).

1190 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 34, stressing that "the European legislature should not enact provisions thar are specifically aimed at hindering the cross-border movement of goods within the internal market".

1191 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 34.

1192 Council Regulation 608/2013 of 12 June 2013 concerning customs enforcement of intellectual property rights and repealing Council Regulation (EC) No 1383/2003 [2013] OJ L181/1 (Customs Regulation), Article 2 defines "intellectual property" as meaning trade marks; designs; copyright and related rights; geographical indications; patents; supplementary protection certificates for medicinal products and plant protection products; community and national plant varieties right; topography of semiconductor products; and utility model and trade names.

3. Exceptions

Article 5 spells out a list of four exceptions to the rights conferred by Article 4, which attempt to reconcile the interests of trade secret holders in keeping their information undisclosed and the concerns of third parties in accessing and using such information.[1193] Unlike the types of conduct set out in Article 3 TSD, the exceptions are conceptualised as specific limitations to the rights conferred by a trade secret that should be assessed on a case-by-case basis by courts, weighing the specific competing interests at stake in order to proceed to the enforcement of the rights, where appropriate.[1194] These exceptions have been phrased in an open-ended manner to safeguard (a) the right to freedom of expression and information; (b) whistle-blowing; (c) the disclosure of secrets by workers to their representatives in the course of their representation task; and; (d) the protection of a legitimate interest recognised by Union or national law. Each of these will be analysed in turn.

One of the main concerns raised during the negotiation of the Directive was that the fundamental right to freedom of expression and information (recognised in Article 11 ChFREU)[1195] was not hindered by the establishment of common ground rules on the protection of trade secrets,[1196] especially in connection with investigative journalism.[1197] To this end, Article 5(a) provides for a general exception that permits the acquisition, use and disclosure of a trade secret, if it is necessary in order to exercise the abovementioned freedoms. This is in line with the case law of the ECtHR that provides that the principle of freedom of information and expression has to be weighed against the interest of maintaining information in confidence considering the specific circumstances of the case, as per Article 10(2) ECHR.[1198] Ultimately, the inclusion of such an exception seems redundant, in view of the fact that Article 1(2)(a) TSD already sets forth that

1193 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 38.
1194 Christian Alexander 2017 (n 1091) 1014.
1195 The right to Freedom of expression and information is expressly recognised in Article 11 of the ChFREU.
1196 This point is raised by the Commission, 'Public Consultation On The Protection Against Misappropriation Of Trade Secrets And Confidential Business Information, Summary Of Responses,' 11 <http://ec.europa.eu/growth/industry/intellectual-property/trade-secrets/index_en.htm> accessed 15 September 2018; in the same vein see Mathias Lejeune 2016 (n 1157) 334.
1197 Björn H. Kalbfus 2016 (n 1122)1015.
1198 Christian Alexander 2017 (n 1091) para 114.

the Directive shall not affect the exercise of the right to freedom of expression and information, including respect for pluralism and the media.

Notably, paragraph (b) introduces common ground rules on the liability of so-called "whistle-blowers". The Oxford Dictionary defines them as persons who inform "on a person or organisation regarded as engaging in unlawful or immoral activity".[1199] Accordingly, the acquisition, use or disclosure of secret information does not trigger the application of the measures, procedures and remedies set out in the Directive, when they are performed:

> For revealing a misconduct, wrongdoing or illegal activity, provided that the respondent acted for the purpose of protecting the general public interest.

This is typically the case for an employee who reveals criminal or dangerous conduct by his employer. Prime examples include the sale of tax evaders' data to the competent national authorities or the disclosure of environmental damage caused by a company.[1200] The establishment of such a defence was one of the most contested aspects during the negotiation process and was redrafted on several occasions.[1201] It is one of the features that has garnered more attention from media and civil organisations in the wake of the WikiLeaks and Panama Papers cases. However, there are still a number of civil organisations and political parties that claim that the protection for whistle-blowers is too weak and that the most recent political developments call for the enactment of a new and more comprehensive Directive on their protection.[1202]

The whistle-blower exception is only applicable if the person revealing the information acts with the aim of "protecting the general public interest".[1203] Pursuant to Recital 21 TSD, the public interest would include

---

1199 'whistle-blower, n' (*OED Online*, OUP June 2013) <https://en.oxforddictionaries.com/definition/whistle-blower> accessed 15 September 2018.

1200 Ansgar Ohly 2013 (n 13) 43.

1201 Victoria A. Cundiff and others 2016 (n 789) 744 noting that no similar provision has been included in the DTSA.

1202 The European Corporate Observatory, 'A New Right To Secrecy For Companies, And A Dangerous EU Legislative Proposal Which Must Be Rejected' (30 March 2016) <https://corporateeurope.org/power-lobbies/2016/03/trade-secrets-protection> accessed 15 September 2018.

1203 Jean Lapousterle, Christophe Geiger, Norbert Olszak and Luc Desaunettes, 'What protection for trade secrets in the European Union?' (2015) Centre for International Intellectual Property Studies (CEIPI) Research Paper No. 2015-02, 8 <https://ssrn.com/abstract=2970461> accessed 15 September 2018.

among others, disclosures for the benefit of public safety, consumer protection, public health and environmental protection.[1204] However, legal uncertainty may arise as regards the interpretation of the wording of paragraph (b), in particular in connection to the differentiation between "misconduct, wrongdoing or illegal activity" and their relationship with the public interest.[1205] These terms are undoubtedly broad and the constellation of acts they may cover ranges from the mere misuse of a company's resources to the disclosure of a hygiene scandal.[1206]

Furthermore, the wording of the provision does not clarify when the acquisition, use and disclosure of a trade secret is to be regarded as *necessary* and thus unenforceable.[1207] Rather than providing a universal standard, it seems that the assessment of necessity should be appraised on a case-by-case basis, in such a manner that it is possible to take into consideration the individual circumstances and all of the relevant interests at stake. Hence, the protection of whistle-blowers will have to be assessed in accordance with the extensive case law of the ECtHR on the subject.[1208] In addition, pursuant to Recital 20, if one of the requirements for the application of Article 5(b) is missing, judicial authorities may not enforce trade secrets protection when the whistle-blower believed in good faith that his conduct complied with the requirements set out in this provision.[1209] In this regard, it should further be borne in mind that the Directive does not aim to harmonise criminal law.[1210] Consequently, the revelation of a secret, when justified on the basis of a prevailing public interest, may not trigger civil sanctions, but may still be subject to criminal law liability under the relevant national provisions.[1211]

1204 Christian Alexander 2017 (n 1091) para 116.

1205 IP Federation, 'The EU Trade Secrets Directive' (2014) Policy Paper PP04/15, 3 <https://www.ipfederation.com/news/ip-federation-comments-on-the-compromise-text-for-the-eu-trade-secrets-directive/> 15 September 2018; Thomas Hören and Reiner Münker 2018(b) (n 1119) para 25.

1206 Tanya Aplin 2014 (n 384) 272.

1207 Tanya Aplin 2014 (n 384) 272.

1208 Jean Lapousterle, Christophe Geiger, Norbert Olszak and Luc Desaunettes, 'What protection for trade secrets in the European Union?' (2015) Centre for International Intellectual Property Studies (CEIPI) Research Paper No. 2015-02, 8 <https://ssrn.com/abstract=2970461> accessed 15 September 2018.

1209 Christian Alexander 2017 (n 1091) para 117.

1210 Impact Assessment (n 385) 57-58.

1211 Against this background, Mathias Lejeune 2016 (n 1157) 334 notes that in Germany the right of an employee to disclose the circumstances and conduct of an employer is not an absolute one. According to case law from the German Con-

The inclusion of paragraph (c) regarding the disclosure of secrets by workers to their representatives ensures that the rules laid down in the Directive are not used to circumvent the safeguards provided for in national labour legislations. However, the application of this exception is confined to situations where the disclosure (i) is carried out in the course of legitimate exercise by the employee representatives of their functions, (ii) and is necessary in order to perform such functions.[1212]

Finally, paragraph (d) sets forth that when the acquisition, use and disclosure are carried out with a view to protecting a legitimate interest, liability does not arise. This is an open balancing clause, which allows for weighing in the interests of trade secret holders and third parties,[1213] when none of the previously analysed exceptions are applicable.[1214] Crucially, this provision provides that the "legitimate interest" must be "recognised by Union or national law". This allows for taking into consideration some of the objectives promoted by the EU in the assessment of lawfulness. Of particular relevance in the context of trade secrets are innovation (Article 173 TFEU) and competition (Article 101-103, 116 and 117 TFEU).[1215] Yet, the scope of this exception is so broad and flexible that it may allow courts to consider any relevant interest that may inform the action of the EU powers in the years to come.

IV. Enforcement

As noted above, the initial intention of the Commission was to expand the scope of application of the Enforcement Directive to undisclosed information. However, this possibility was declined, based among other reasons, on the argument that trade secrets are not IPRs.[1216] Consequently, chapter III of the TSD, which also constitutes its central part, extensively regulates enforcement, mirroring the former Directive, even though some relevant

---

stitutional Court, the interest in the disclosure of information has to be balanced against the right of the company to keep the information undisclosed. However, Lejeune anticipates that the implementation of this provision into German Law will not be very problematic.

1212 Christian Alexander 2017 (n 1091) para 119.

1213 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 38.

1214 Christian Alexander 2017 (n 1091) para 120.

1215 Tanya Aplin 2014 (n 384) 271-272.

1216 The relationship between the Enforcement Directive and the TSD is analysed in chapter 3 § 5 C) II. 1. above.

omissions and specific provisions on procedural aspects have been included in order to address the particularities raised by trade secrets protection. The remainder of this chapter analyses the main features of the enforcement of trade secrets as laid down in the TSD. To this end, section 1 examines the general principles that should guide the enforcement of trade secrets. Next, some legal considerations as to the limitation period set forth in Article 8 are presented in section 2. Section 3 then looks into the specific measures that Member States may adopt to preserve confidentiality during litigation. Finally, the remedies against trade secrets infringement are analysed in section 4.

1. General provisions

Article 6 of the Directive lays down a general obligation for Member States to implement the measures, procedures and remedies necessary to ensure the availability of civil redress against trade secrets misappropriation. These should not only be fair and equitable, but also effective and dissuasive.[1217] Likewise, they should be applied by national courts in a manner that is not too complicated and costly or involves unreasonable delays.[1218]

Most notably, Article 7 TSD places special emphasis on the principle of proportionality and the prevention of abusive litigation. This echoes the concerns expressed by the respondents in the economic survey carried out by Baker McKenzie, in which 23,6% of the participants considered that harmonisation in the field of trade secrets would spur abusive litigation and consequently raise market barriers for competitors.[1219] On this point, the TSD follows the structure implemented in the Enforcement Directive, where compensation in the case of abuse of litigation is left to Member States to regulate. Yet, a lack of harmonisation on such a salient aspect may lead to a structural imbalance, whereby trade secrets holders could seek redress if their rights were infringed, but those who face unfounded claims could not seek compensation across the several EU jurisdictions.[1220]

1217 Article 6 (2)(a) TSD and Article 6(2)(c) TSD.

1218 Article 6 (2)(b) TSD is very similar to Article 3(1) Enforcement Directive.

1219 Baker McKenzie 2013 (n 1057) 131.

1220 This argument is raised in Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 41; the MPI Comments also highlight that the sanctions envisaged in the case of abusive litigation should be just as efficient and have the same deterring effect as those applicable in the event of infringement; see further Mathias Lejeune 2016 (n 1157) 335.

To offset this potential imbalance, Article 7(2) provides that judicial authorities may, if requested by the defendant, award damages, impose sanctions or order the dissemination of the judicial decision when the claim is deemed manifestly unfounded and the plaintiff is found to have initiated the proceedings in bad faith, in accordance with national law. Pursuant to Recital 22, such conduct may have as its ultimate purpose, for example, delaying or limiting the defendant's access to the market or harassing or intimidating him.[1221] As a whole, the wording of the provision poses several interpretative questions, which will be discussed in the following paragraphs.[1222]

First, it is worth noting that the Directive does not provide guidance as to how courts are to assess whether a claim is ill-founded and if defendants can bring an action or file a counterclaim.[1223] Furthermore, the provision refers to sanctions in a generic manner, and does not specify the particular measures that should be adopted beyond the publication of the decision and the possibility of claiming damages.[1224] Following wording of the Directive, the measures that judicial authorities may adopt are left to the Member States. This runs counter to the harmonisation goals pursued by the Directive, as sanctions may vary substantially from country to country.

Finally, some authors take the view that the defendant should be able to claim full compensation for the cost that he incurred as a result of the abusive litigation. This is particularly relevant in those jurisdictions where the amount of the attorney's fees that the prevailing party can recoup is statutorily limited in order to ensure equality of arms between the parties.[1225]

2. Limitation period

With a view to enhancing legal certainty, Article 8 TSD mandates Member States to lay down a limitation period to take legal action. In essence, such a limitation aims at imposing a duty of care and the obligation to monitor the use of trade secrets on right holders.[1226]

1221 See Recital 22 TSD.

1222 Mathias Lejeune 2016 (n 1157) 335 notes that such a possibility is not provided for under German law, but its inclusion in the TSD as a minimum standard is to be welcomed.

1223 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 42.

1224 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 43.

1225 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 44.

1226 See Recital 23 TSD.

Pursuant to Article 8, it is up to the Member States to determine when the limitation period begins, its duration and the circumstances that may be invoked to interrupt or suspend it. The only restraint is that it shall not exceed six years.[1227] Even though the latter approach appears weak from a harmonisation perspective, it might also be overambitious to interfere to such a large degree with Member States' procedural law.[1228] In this context, it has been suggested that information is afforded protection as a trade secret for as long as the requirements set out in Article 2(1) TSD are complied with, similarly to the protection afforded in Germany under § 4 (3) UWG regarding the offering of goods and services that are replicas of the ones offered by competitors.[1229]

3. Preservation of confidentiality during litigation

Drawing upon the results of the empirical study conducted by Baker McKenzie,[1230] the Directive has introduced specific measures to preserve secrecy during litigation. Before its adoption, only a limited number of jurisdictions had put in place effective means to protect confidentiality. This is crucial to ensure that the object of the proceedings, undisclosed information, is not lost during litigation.[1231] In the absence of such measures, information would become publicly known by the mere fact of bringing legal proceedings and the enforcement of trade secrets would be substantially hindered. In the light of this and in accordance with the right to a fair trial recognised in Article 47 ChFREU, the Directive sets forth two general obligations.

1227 Thomas Hören and Reiner Münker 2018(b) (n 1119) para 33.

1228 Tanya Aplin 2014 (n 384) 275.

1229 Christian Alexander 2017 (n 1091) para 72.

1230 Baker McKenzie 2013 (n 1057) 131 noting that lack of trust in the judicial system and fear of losing the trade secret were identified as two of the reasons that dissuaded trade secret holders from seeking legal redress after misappropriation.

1231 Hogan Lovells 2012 (n 793) para 301, considers that: "The courts need to have means to protect secret information during proceedings. This can be achieved with confidential schedules to pleadings and restricting the disclosure of information during trial and in the judgement itself. At the moment there is inconsistency between Member States on the use of "in camera" hearings (hearings excluding the public) and the protection of information contained in court documents".

Firstly, Article 9(1) provides that Member States are bound to ensure that the parties and any other persons who intervene in the legal proceedings do not disclose or use information of a confidential nature that they have acquired during the course of litigation, even after the legal proceedings have ended, provided that the information has not lost its secret nature over time or that there is a final court decision that stipulates that the object of the proceedings no longer meets the requirements of protection.[1232]

The general obligation set forth in Article 9(1) is conditioned upon the submission of an application by the interested party with the competent judicial authorities where the alleged trade secret is clearly identified. Yet, in the implementation of the TSD, Member States may also allow judicial authorities to act on their own motion.

Thereafter, Article 9(2) spells out a list of three specific measures that national courts may adopt ex parte or on their own initiative (if allowed by national law) with the purpose of maintaining secrecy during litigation. These include: (a) restricting access to documents where the trade secret is disclosed, and (b) restricting access to the hearings and their transcripts. In order to avoid the leakage of information to competing parties, the circle of people that have access to evidence or hearings should be limited to those for whom this is strictly necessary. However, in order to comply with the transparency demands set out in Article 47 ChFREU, the Directive provides that such a circle should always include at least the legal representatives of the parties and one natural person from each of the parties, as well as any other legal representatives in accordance with national law, who are also under an obligation of confidence.[1233] Finally, paragraph (c) of the provision sets out that any passages of the ruling where trade secrets are disclosed may be deleted or redacted from the published decision.

In deciding whether to adopt the measures referred to above, courts should weigh up the interests of the parties to the proceedings, but also any potential harm to third parties (as per Article 9(3) TSD).

1232 Mary-Rose McGuire 2016 (n 824) 1007-1008, highlighting the similarities with the German "in camera hearings"; in this regard, Mathias Lejeune 2016 (n 1157) 335-336 notes that until the implementation of the TSD the application of the said proceedings to trade secrets cases was subject to a balance of interests test of the competing interests of the parties.

1233 As per Recital 25 TSD; consequently Björn H. Kalbfus 2016 (n 1122)1015-1016 notes that the TSD does not call for the introduction of a true "in camera hearing" in the German sense, because at least one representative and legal person from each party should be allowed.

4. Remedies available in case of infringement

The remedies laid down in the TSD are very similar to those enshrined in the Enforcement Directive. They are of a civil nature and encompass provisional and precautionary measures (Article 10), injunctions and corrective measures (Article 12), damages (Article 14) and the publication of judicial decisions (Article 15). Yet, there are some salient differences. The TSD does not harmonise the measures for providing and preserving evidence[1234] or the right to information, which are left to Member States to regulate.[1235] The following sections start by providing an analysis of the remedies set forth in the TSD and conclude by looking into the policy reasons that may justify the exclusion of some of the remedies embedded in the Enforcement Directive.

a) Provisional and precautionary measures

It usually takes some time from the moment a trade secret holder realises that their rights are being infringed to the final judicial decision on the merits, just as with any other IPR.[1236] To avoid the right holder's interests being hindered during this time, the Directive lays down in Article 10(1) a number of provisional and precautionary measures that national competent judicial authorities should adopt at the request of the trade secret holder against the alleged infringer. These include: (a) a temporary cessation of, or prohibition on the use or disclosure of the infringed trade secret; (b) a prohibition on the manufacture, offering and placing on the market of the infringing products, as well as their import and export or storage for the same purpose. Finally, paragraph (c) provides for the seizure and delivery of the suspected infringing goods with the purpose of precluding their entrance in the internal market.

In line with the Enforcement Directive,[1237] the TSD sets out in Article 10(2) the possibility that the allegedly infringing conduct might continue (use, but not disclosure), provided that appropriate guarantees are lodged.[1238] Such an approach poses a number of issues as regards trade se-

1234 See Article 7 Enforcement Directive.
1235 See Article 8 Enforcement Directive.
1236 Lionel Bently and Brad Sherman 2014 (n 125) 1100.
1237 See Article 9(1)(a) Enforcement Directive.
1238 Mathias Lejeune 2016 (n 1157) 336.

crets, particularly as the object of protection, undisclosed information, would be put at risk.[1239] One of the principles upon which the law of trade secrets is built is that once the secret becomes generally known it no longer merits protection. Hence, if its subsequent use is allowed, secrecy might be lost. In this context, it is noteworthy that the Directive does not mention whether acquisition may be permitted upon the lodging of the appropriate guarantees. Following the above rationale, in the interest of secrecy, it should be deemed as falling outside the scope of Article 10(2) TSD. Consequently, it is submitted that the wording of Article 10(2) interferes with one of the main goals pursued by the TSD, ensuring that secrecy is preserved during litigation.

In a similar vein, Article 11(2) spells out a number of criteria that should be duly examined by the competent judicial authority when granting the measures envisaged in Article 10(1). Accordingly, courts should take into consideration the value of the secret, the steps adopted to protect it, the conduct of the defendant, the impact of an unlawful use or disclosure, as well as the effect of the adoption of interim measures on the parties. This provision has no corresponding rule in the Enforcement Directive and it also raises a number of interpretative questions. According to its wording, the assessment of proportionality should be carried out based on the specific circumstances of each case, and deems the criteria listed as an open-ended enumeration of examples.[1240] Yet, surprisingly, among those, no reference is made to the urgency of the measures. From a procedural law perspective, the grant of interim measures is justified by the negative consequences that waiting for a final decision on the main proceedings may entail. Thus, the urgency of the measures is of paramount importance in the appraisal of the pertinence of their adoption.[1241] In this vein, it is worth noting that pursuant to Article 11(4) TSD, the grant of precautionary measures is in any case conditioned upon the establishment of the appropriate securities by the applicant.[1242]

Remarkably, the Directive foresees the revocation of any interim measures adopted in accordance with Article 10 if proceedings are not instituted within a reasonable period, as set forth by the competent judicial authorities, or, in the absence of such a determination, after 20 working days

1239 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 50.
1240 See Article 11(2) TSD.
1241 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 52.
1242 Mathias Lejeune 2016 (n 1157) 337.

(or 31 calendar days, whichever is longest).[1243] Similarly, if the requirements for protection, as per Article 2(1) TSD, are no longer fulfilled for reasons independent of the conduct of the defendant, the application of interim measures should also be revoked. This would typically be the case for a trade secret that becomes publicly known and thus loses one of its essential qualities, its secret nature.

b) Injunctions and corrective measures

A trade secret is infringed when its acquisition, use or disclosure is regarded as unlawful, pursuant to the wording of Article 4 (in conjunction with Article 3 and Article 5). In such a case, the holder is entitled to ask the court to adopt an array of measures against the infringer (Article 12(1)). These include: (a) the cessation of, or prohibition on the use and disclosure of the trade secret; (b) the prohibition on producing, offering and placing on the market goods in which the trade secret is embodied, or their import, export and storage to this end; (c) the adoption of corrective measures in connection to the infringing goods; and (d) the destruction of all or part of any document, object, material, substance or electronic file containing or embodying the trade secret, as well as their delivery to the applicant. The corrective measures available are stipulated in 12(2) and encompass (a) the recall of the infringing goods from the market; (b) the modification of the infringing goods with the purpose of eliminating their infringing features; and, (c) the destruction of the infringing goods, as well as any documents (both physical and electronic) or other items where the trade secret is disclosed.

The wording of Article 12(1)(b) has been regarded as redundant and superfluous by some, as the types of conduct therein described are already regarded as infringing by Article 4(5) TDS and thus fall under the scope of Artice 12(1)(a).[1244] While such criticism is well-founded, it is true that such clarification, albeit redundant, may avoiding differences in the implementation among Member States. Similarly, bearing in mind that the main purpose of the Directive is to restore the market position of the trade secret holder by conferring upon him a lead time advantage, the content of paragraph 2 of Article 13(1) appears particularly relevant.[1245] This provision

1243 As per Article 11(3)(a) TSD.
1244 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 54.
1245 Mary-Rose McGuire 2016 (n 824) 1007.

stipulates that the duration of injunctions can be limited, but courts should always ensure that they are sufficient to eliminate commercial advantage gained by the misappropriation, in line with the springboard doctrine discussed in connection with the English breach of confidence action.[1246]

Considering the interim measures regulation and with a view to limiting the liability of bona fide third parties, Article 13(3) foresees the possibility of establishing alternative financial compensation instead of granting injunctions or corrective measures (i.e. damages in lieu of injunctions). The continuous use of the trade secret or the marketing and distribution of the goods in which it is embodied is only possible if (i) the information was acquired in good faith, as a sort of bona fide defence, (ii) the execution of the injunctions or corrective measures in question would be very harmful to the acquirer, and (iii) the monetary compensation seems reasonable.[1247] In addition, Article 13 provides that when damages are awarded instead of an injunction, the said compensation shall not exceed the royalties that the parties would have agreed if the misappropriated trade secret had been licensed.[1248] Ultimately, this provision equates the position of the third party infringing user with that of the lawful user.[1249] In addition, it shows a clear parallel with Article 12 of the Enforcement Directive, even though its scope of application is more limited (it is only applicable to bona fide acquirers) and its implementation into national legislation is mandatory as a maximum standard of protection, and not optional, as in the case of the Enforcement Directive.[1250] As a final note, Recital 29 provides that the award of damages in lieu of injunction shall not be permitted when it results in an infringement of any other provision (such as labour law or criminal law) and it may harm consumers. In view of this, it is submitted here that a central factor in assessing whether granting an injunction is disproportionate should be whether the acquirer of the information changed his position on the information before learning about its confidential nature, for instance, by buying new machines or hiring new

1246 See chapter 3 § 3 C) III.
1247 See Article 13(3) TSD; however, establishing the amount of the said licences may in practice prove quite difficult.
1248 As discussed in chapter 3 § 3 C) II. 2.d) in connection to the liability of third parties.
1249 Clemens Koós 2015 (n1158) 227; Franz Hofmann, '"Equity" im deutschen Lauterkeitsrecht? Der "Unterlassungsanspruch" nach der Geschäftsgeheimnis-RL' [2018] WRP1, para 27.
1250 See Article 1(1) TSD.

employees to develop, produce or commercialise a new product on the basis of such information.[1251] Also, due consideration should be paid to the likelihood that by allowing the use of the trade secret it becomes generally known or easily accessible.

c) Damages

The TSD foresees the award of damages in the event of infringement, the most common remedy in the enforcement of IPRs.[1252] Just as in the intellectual property scenario, compensation through damages intends to restore the holder of secret information to the position in which he would have been prior to the unlawful acquisition, use and disclosure.[1253] The assessment of damages follows a similar scheme to that laid down in the Enforcement Directive,[1254] which represents considerable progress in view of the divergent approaches followed by national regimes before the adoption of the TSD and the legal uncertainty that it entailed. Accordingly, three calculation methods are foreseen.[1255] In the first place, the plaintiff can claim the lost profits resulting from the infringement of his trade secret. Alternatively, the compensation can be calculated on the basis of the unfair profits made by the defendant following the misappropriation of the trade secret. In this context, the Directive also mentions that the trade secret holder can claim moral damages derived from the infringement. The third option is the computation of damages as a lump sum, using as a benchmark the reasonable royalties that the trade secret holder would have received in the case of licensing. In all of those cases, the award of damages is conditioned upon the finding of at least gross negligence on the side of the infringer, "who knew or ought to have known" that the acquisition, use or disclosure of the information was illicit.[1256] Nonetheless, it should be noted that in the light of the CJEU decision in *Jørn Hansson v Jungpflanzen*, it has been contested whether damages under Article 13(1)(a)

1251 For a more detailed analysis see Tanya Aplin and others (n 22) para 7.140
1252 Lionel Bently and Brad Sherman 2014 (n 125) 1117.
1253 See Recital 30 TSD.
1254 For an overview of the assessment of damages in the Enforcement Directive see Annette Kur, 'The Enforcement Directive - Rough Start, Happy Landing?' [2004] IIC 821, 827-830.
1255 Thomas Hören and Reiner Münker 2018(b) (n 1119) para 33.
1256 Mary-Rose McGuire 2016 (n 824) 1007; Franz Hofmann 2018 (n 1249) para 14.

of the Enforcement Directive (and by extension under Article 14(2) TSD) may be calculated on the basis of the infringer's profits.[1257]

With respect to the regulation of damages, two features stand out. In the first place, there might be a great asymmetry between the infringer's profits and the lost profits on the side of the right holder. In effect, the unlawful acquisition, use and disclosure may render the information generally known. In this context and linked to the lack of an exclusive nature of trade secrets as opposed to other IPRs, the trade secret holder would lose the object of protection. By contrast, the profits gained by the infringer may be rather limited if compared to the economic consequences that losing the trade secret entails. Secondly, it is unclear in which context moral (or immaterial) damages should arise, which is an aspect that has been particularly controversial in the implementation of the Enforcement Directive.[1258] If one accepts the privacy justification, moral damages could derive from the violation of a privacy right.[1259]

Against this background, paragraph 2 of Article 14(1) TSD provides that in the implementation of the Directive, Member States may restrict the liability for damages of employees towards their employers in the case of unlawful acquisition, use or disclosure of a trade secret if they have acted without intent. At first glance, the wording of this provision seems obscure, as it is not clear whether it should also apply to former employees. Following a systematic and teleological interpretation, and bearing in mind that fostering employee mobility is one of the principles that informs the Directive, it is submitted that the non-intentional disclosure of departing employees should fall under the scope of such a limitation.

d) Publication of the judicial decision

In line with Article 15 of the Enforcement Directive, if the plaintiff prevails, he may request that the court publishes the judicial decision at the expense of the infringer. In such a case, all of the necessary measures to

---

1257 Case C–481/14 *Jørn Hansson v Jungpflanzen Grünewald GmbH* [2016] (CJEU, 9 June 2016) para 42; Franz Hofmann 2018 (n 1249) para 14.

1258 GRUR, 'Opinion on the proposal for a Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, COM (2013) 813 final' (2014), para 5.b) <http://www.grur.org/uploads/tx_gstatement/2014-03-19_GRUR_Stellungnahme_zum_Know-how-Schutz_EN.pdf> accessed 15 September 2018.

1259 See chapter 1 § 2 B) IV.

preserve the secret nature of the information should be adopted in accordance with the rules laid down in Article 9 TSD.

In the assessment of the suitability of the publication and proportionality of such a measure, a number of factors should be taken into consideration. These include, among others, the potential harm to the reputation of the infringer, the value of the secret and the likelihood of further use or disclosure. During the final phase of the negotiation process, some amendments were introduced with a view to enhancing the privacy of the infringer and preventing his personal identification, which have crystallised in paragraph 2 of Article 15(3) of the Directive.[1260]

e) Claims for information and preserving evidence

One of the central differences between the Enforcement and the TSD is that the latter does not establish any obligations concerning claims for preserving evidence[1261] and for obtaining orders as to the origin or distribution networks of the infringing goods.[1262] These are left to Member States to regulate, and, as a result, their availability will ultimately depend on national law provisions. Consequently, the practices among member states may vary from one country to another, putting at risk the harmonisation goals. Yet, it is true that claims for information and preserving evidence may be unduly used to acquire confidential business data. In view of this, it is submitted that a uniform EU framework on the protection of trade secrets should also have included rules on these issues and ensured that the necessary safeguards were adopted to avoid abuses on the side of the plaintiff.[1263]

Moreover, this approach is consistent with the fact that placing infringing goods on the market, and their import or export is regarded as an unlawful use of a trade secret, pursuant to Article 4(5) of the Directive. As a result, the wording of the provisions regulating claims for information should be adapted to ensure that the plaintiff is able to learn not only the

---

1260 Article 15(3) para 2 TSD: "The competent judicial authorities shall also take into account whether the information on the infringer would be such as to allow a naural or legal person to be identified and, if so, whether publication of that information would be justified, in particular in the light of the possible harm that such measures may cause to the privacy and reputation of the infringer".

1261 See Articles 6 and 7 Enforcement Directive.

1262 See Article 8 Enforcement Directive.

1263 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 56.

channels of distribution, the quantity and the prices of infringing goods, but also the identities of the subsequent acquirers.[1264] This seems crucial to prevent subsequent infringements and assess the extent to which the confidential information has been made available.

§ 6 Conclusion

Drawing from the foregoing legal analysis, it is submitted that despite some criticism, the alignment of national Member States' laws on the protection of trade secrets is justified as a measure that is necessary to ensure the good functioning of a Single Market without barriers, in which the fundamental freedoms are accomplished (particularly the free movement of goods and workers).

Indeed, the comparative law examination conducted above has underscored that the legal regimes for the protection of trade secrets across the Single Market prior to the implementation of the TSD were completely scattered and, consequently, the level of protection varied substantially from one member state to another. For instance, the liability threshold for third parties was much higher in Germany than in England. In the former jurisdiction, conditional intent was required on the side of the infringer and at least one of the following purposes in the performance of the relevant conduct: a competitive purpose, a personal gain, to benefit a third party or to hinder the position of the trade secret holder. In contrast, in England liability arose merely if the standard of care followed by a honest person placed under the same circustances was not observed.

In the light of the above, it is submitted that the Directive manages to strike a balance between the interest of trade secrets holders in keeping their information concealed and the interest of third parties in accessing such information. This is mostly achieved through the establishment of a number of flexible and open-ended clauses in the provisions that govern the appraisal of the lawfulness of the allegedly infringing conduct, which mostly resort to the general standard of honest commercial practices embedded in Article 10bis PC and the inclusion of common ground regarding the standard of liability of third parties, which requires at least gross negligence on the side of the infringer. Likewise, the consideration of independent discovery and reverse engineering as lawful forms of obtaining a trade secret is also crucial to maintain the aforementioned equilibrium.

1264 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 57.

They are essential to ensure the complementarity between the patent system and the trade secrets regime. In this context, the EU legislature has further laid down an array of exceptions to the rights conferred by a trade secret that safeguard the fundamental freedoms of expression and information and most notably deem as lawful whistle-blowing conduct. The applicability of such exceptions will ultimately depend on the balance of interests conducted by the competent national authorities, considering the individual circumstances of the case.

Such a flexible approach presents both advantages and disadvantages. On the one hand, it allows for considering all of the relevant interests in each individual case and adapting to future technological developments, a key aspect in the protection of trade secrets. Yet, on the other, it may also lead to divergent interpretations of the same provision among Member States, thus hindering the ultimate harmonisation objective. As a whole, it seems that establishing minimum standards with regard to the civil protection of trade secrets (as well as maximum standards with respect to central aspects such as the exceptions, as well as lawful and unlawful conduct) will enhance legal certainty across the Single Market.[1265]

Remarkably, it is submitted that the Directive does not provide a univocal answer as to the legal nature of trade secrets. Only Recital 16 refers to this matter and spells out that the provisions of the Directive should not create an exclusive right. However, such a statement does not clarify whether the misappropriation of confidential information is to be protected as an infringement of an IPR, a property right or just as an act of competition contrary to honest commercial practices under unfair competition rules. The Directive seems to adopt an unfair competition approach in the provisions that regulate the unlawful acquisition, use and disclosure of trade secrets, as they keep referring to the standard of honest commercial practices. On the other hand, the list of remedies spelt out in chapter III mostly corresponds to those envisaged for the infringement of an IPR. Wisely, the EU legislature has not attached specific legal consequences to the categorisation of information as the former or the latter. However, as noted above,[1266] this has implications outside the scope of the Directive vis-à-vis the applicable law in the case of infringement and the relationship

1265 A different view is purported by Tanya Aplin 2014 (n 384) 279, where the author notes that, "only a modest amount of harmonisation is likely to ensue from implementation of this Directive".

1266 Chapter 1 § 3 III.

with the Enforcement Directive. In this context, clarification will ultimately have to be sought by reference to the CJEU.

From a policy perspective, the Commission and the Council expect that the implementation of the Directive will yield enhanced competitiveness and cross-border innovation, which ultimately should lead to remarkable employment growth. Yet, only time will tell whether these ambitious objectives will be met or, to phrase it better, if any causal link between the harmonisation of trade secrets law in the EU and an improvement in the economic results within the Single Market can be established. Without doubt, the comprehensive regulation of the measures, procedures and remedies that trade secret holders may claim in the enforcement of their rights creates a level-playing fied for stakeholders across the EU.

As a final note, it is also noteworthy that the Directive sheds little light on the interpretation of the secrecy requirement, as the definition provided in Article 2 simply reproduces the wording of Article 39(2) TRIPs. In addition, by virtue of Article 1(3)(b) and Recital 14, the skills and knowledge acquired by employees during the normal course of their employment are excluded from the scope of protection in the interest of employee mobility. Again, the legislature provides little guidance regarding how to delineate the contours of such information.

In view of the increasing vulnerability of information in the digital age, the following chapter is devoted to the study of the notion of secrecy and, more specifically, to the analysis of the circumstances under which information enters the public domain. Having regard to the harmonisation goals pursued by the TSD, it proposes a number of case-specific guiding principles to ensure a homogeneous interpretation of this notion across the different EU Member States.