Chapter 6. The internal and external spheres of secrecy and their limitations

§ 1 The two shperes of secrecy

This dissertation started in chapter 1 by highlighting that the intrinsic significance of trade secrets revolves around two conflicting forces: the principles of openness, freedom of discourse and communications, which clash with the principles of privacy, secrecy and a restrictive flow of information.[2207] Ultimately, such a dichotomy has guided the dissertation so far, as it has surfaced in each of the jurisdictions studied and the empirical analysis conducted by reference to the perfume industry. As argued in chapter 1, it appears justified and necessary to protect undisclosed information. However, overprotecting secrecy may have negative effects on freedom of speech and innovative and creative activities.

To be sure, secrecy is the cornerstone upon which the law of trade secrets is built: "so long as a secret remains unrevealed, its cloak is everlasting".[2208] Crucially, the secret nature of information is largely a matter of fact and degree. Once a piece of information becomes generally known, even in the event of misappropriation, it ceases to be protected. It is for this reason that trade secrets are said to be of an inherently perishable nature.[2209] To a certain extent, this results from the underpinning strong public policy that encourages the dissemination of information and is wary of the protection of ideas by law.[2210] In the same vein, the factual nature of secrecy imposes a duty of care on the side of the trade secret holder: protection is conditioned upon the adoption of reasonable measures.[2211]

2207 William van Caenegem 2014 (n 7) 11.

2208 Jeanne C. Fromer, 'Trade Secrecy in Willy Wonka's Chocolate Factory' 3, 13 in Rochelle C. Dreyfuss and Katherine J. Strandburg (eds), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research* (Edward Elgar 2011).

2209 *Attorney General v Newspaper Publishing Plc and Others* [1989] 2 FSR 27 (Ch), 48.

2210 *INS v. Associated Press*, 248 U.S. 215, 250 (1918).

2211 Such a requirement has been criticised by Robert G. Bone, 'Trade Secrecy, Innovation and the Requirement of Reasonable Secrecy Precautions' 46-76 in Rochelle C. Dreyfuss and Katherine J. Strandburg (eds), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research* (Edward Elgar 2011).

As examined above,[2212] it is not possible to extract a normative standard that allows for delineating the contours of secrecy in a precise manner. Instead, secrecy is best conceptualised by reference to its negative aspects, i.e. when information enters the public domain.[2213] However, it cannot be overlooked that trade secrets are most frequently ascribed to companies, which usually adopt physical and legal measures to protect them. In particular, in the adoption of these measures two distinct spheres can be identified. The first is the internal sphere of secrecy, which refers to the preservation of confidential information within the company and mostly concerns employees, because they are the ones that regularly have access to valuable secret information in the performance of their duties. Secondly, the external sphere of secrecy refers to the adoption of legal and physical measures in order to avoid the unauthorised use and disclosure of trade secrets by third parties such as suppliers, service providers, licensees or R&D partners that may have accessed the information with authorisation, but for a specific purpose. More generally, it also intends to preserve trade secrets from the interference of third parties.

Considering the previous distinction, this chapter delves into the understanding of secrecy by analysing first, its internal sphere (intra company) and, second, its external sphere (extra company) and the role that contractual provisions play in ensuring confidentiality. Then, the limitations of secrecy are examined with a view to ensuring a homogeneous interpretation within the EU after the implementation of the TSD. Ultimately, in line with the research questions that inform the dissertation, it seeks to propose a balanced solution to the secrecy-openness dichotomy. To that end, § 1 explores the two spheres of secrecy, and § 2 is devoted to the study of the limitations of secrecy. Finally, some conclusions regarding the optimal scope and duration of protection are presented in § 3.

2212 Chapter 4 § 4 B) I.
2213 Chapter 4 § 4 C) II.

A) The internal sphere of secrecy: confidentiality and employees[2214]

I. Implied duty of confidentiality during the course of the employment relationship

The survey of the three jurisdictions that has guided the comparative analysis of this dissertation reveals that in all three the relationship between an employer and their employee is premised on the observance of an implied duty of confidentiality.

In the U.S:, this principle has been construed as meaning that the employee must not use or reveal confidential information if it may be detrimental to the employer.[2215] Such a duty governs the relationship with both ordinary employees[2216] and high level employees, which nevertheless have often been considered to be subject to a higher level of fidelity due to the relevance of their position.[2217]

Similar principles are followed in England, where the employer-employee relationship is based on an implied duty of good faith and fidelity.[2218] According to the English courts, such a duty includes: (i) the obligation not to reveal information to unauthorised third parties; (ii) the obligation not to copy confidential information or use any other materials for personal use after the termination of employment; (iii) the obligation not to compete with the employer during the effective term of employment; (iv) the obligation not to work for another employer outside working hours if this

2214 For a recent in-depth analysis of trade secrets protection and departing employees see Magdalena Kolasa, *Trade Secrets and Employee Mobility* (CUP 2018).

2215 Roger M. Milgrim 2014 (n 160) § 5.02[1][a] 7.

2216 However, in some cases, it has been held that when the compensation is very low, no obligation of confidence exists, unless expressly indicated by the employer, such as in *Shatterproof Glass Corp. v. Guardian Glass Co*., 322 F. Supp. 854, 864-865 (E.D. Mich. 1970).

2217 Roger M. Milgrim 2014 (n 160) § 5.02[1][c] 14-17; William van Caenegem 2014 (n 7) 197, footnote 29; Elizabeth A. Rowe, 'When Trade Secrets become Shackles: Fairness and the Inevitable Disclosure Doctrine' [2005] 7 Tulane J of Technology & IP 167, 186; *E.I. DuPont de Nemours Powder Co. v. Masland*, 244 U.S. 100, 102 (1917).

2218 John Hull 1998 (1016) paras 6.06-6.10; Roger M. Toulson and Charles M. Phipps 2012 (n 326) paras 14-005- 14-007; the two most notable decisions in this regard are *Lamb v Evans* [1893] 1 Ch 218 (CA), 226 and *Robb v Green* [1895] 2 QB 1 (QB).

may result in a conflict of interests; and (v) the obligation to promote the best interests of the employer's business.[2219]

Likewise, in Germany, § 17(1) UWG generally proscribes the unauthorised disclosure of trade secrets entrusted to an employee during the course of the employment relationship.[2220] German courts have held that such an obligation is ultimately rooted in a general duty of loyalty towards the employer and, consequently, it does not need to be expressly included in the terms of the employment agreement to be enforced.[2221] The Federal Labour Court has resorted to the same general duty in order to infer an obligation not to compete with the trade secret holder before the end of the employment relationship, which includes the actions involved in preparing to set up a competing business that may directly affect the interests of the employer.[2222]

Crucially, the TSD does not establish whether, or under which circumstances a confidentiality duty towards the employer should arise; this is left for Member States to regulate. Notwithstanding this, the disclosure of a trade secret is deemed unlawful if it results from a "breach of a confidentiality agreement or any other duty not to disclose the trade secret" and its use is also proscribed if it arises from "a contractual or any other duty to limit the use of the trade secret". Consequently, if national legal regimes provide for the existence of such a general confidentiality duty, employees may be held liable for the unlawful use and disclosure of a trade secret (Article 4(3) TSD). More generally, liability may also arise if, during the term of employment, employees access, appropriate or copy any documents containing trade secrets without authorisation (pursuant to Article 4(2) TSD). This is typically the case of employees during the final stages of their employment relationship who are preparing for the departure.[2223]

2219 See John Hull 1998 (1016) paras 6.12- 6.32 with further references.

2220 Chapter 3 § 2 B) II. 1. a).

2221 Rudolf Kraßer 1977 (n 1327) 186; Christopher Heath, 'Employees, Trade Secrets and Restrictive Covenants in Germany' 85, 90 in Christopher Heath and Anslem Kamperman Sanders (eds), *Employees, Trade Secrets and Restrictive Covenants* (Wolters Kluwer 2017).

2222 BAG BeckRS 2013, 67444, Rdn 17.

2223 John Hull 1998 (1016) para 7.08.

II. Secrecy obligations of departing employees

One of the most contested areas of the law of trade secrets, which in practice triggers the most litigation, is the problem of concurrent interests between employers and employees after the termination of the employment relationship. There is an inherent tension between the employer's interest in protecting their confidential business information and the employee's need to use the general skills, knowledge and experience that they have accumulated in their new position.[2224] In such a context, the essential underlying problem is that departing employees will apply this information to compete with the original employer. Although at first glance this may seem unfair, it is also the lifeblood of competition in the market. Indeed, labour mobility is essential to the competitive process and a company's productivity.[2225] In the words of Laddie J in *Occular Sciences Ltd v Aspect Vision Care Ltd:*

> For public policy reasons, an employee is entitled to use and put at the disposal of new employers all his acquired skill and knowledge. That is so, no matter where he acquired that skill and knowledge and whether it is secret or was at the time he acquired it. Where the employer's right to restrain the misuse of his confidential information collides with the public policy, it is the latter which prevails.[2226]

As outlined in chapter 3,[2227] employment mobility is one of the principles that inform the TSD. However, it has also been identified as one of the main factors behind the increasing vulnerability of trade secrets.[2228] Against this backdrop, two scenarios are differentiated: post-contractual obligations and implied obligations after the termination of the employment relationship. Both of them pose a number of legal problems from a

2224 Melvin F. Jager, *Trade Secrets Law* (Thomsons Reuters 2015) § 8:6; Miles J. Feldman, 'Toward a Clearer Standard of Protectable Information: Trade Secrets and Employment Relationship' [1994] 9 Berkeley Tech LJ 151, 155; William van Caenegem 2014 (n 7) 11.

2225 William van Caenegem 2014 (n 7) 11; for an economic overview of the benefits triggered by employee mobility see Karin Hoisl, 'Tracing Mobile Inventors – The Causality between Inventor Mobility and Inventor Productivity' [2007] 36 Research Policy 619-636.

2226 *Occular Sciences Ltd v Aspect Vision Care Ltd* [1994] RPC 289, 370-371.

2227 Chapter 3 § 5 C) II. 1.

2228 Impact Assessment (n 385) 15-16.

trade secrets perspective and, in particular, with regard to the maintenance of confidentiality, as is examined in the following sections.

First, section 1 starts by analysing the existence and scope of the implied duty of confidentiality of departing employees in the United States, England and Germany. Then it examines the relevant provisions of the TSD that refer to the skills, knowledge and experience acquired honestly by employees in the performance of their duties. Drawing on the comparative analysis and in view of the harmonisation goals pursued by the TSD, a number of factors are proposed in order to aid national courts to differentiate between unprotected skills, knowledge and experience and protected trade secrets. Thereafter, section 2 presents some considerations regarding contractual provisions that attempt to limit the use of trade secrets by departing employees considering the emerging harmonised framework.

1. Employees general skills, knowledge and experience and the implied obligation of secrecy after the termination of the employment relationship

a) Comparative law analysis

aa) U.S.

In the U.S., it is generally accepted by case law that the general duty not to disclose a trade secret extends beyond the termination of the employment relationship.[2229] The finding of such an implied duty requires that the departing employee reasonably believes that the information is of a confidential nature.[2230] This will depend on a number of factors, such as: (i) the circumstances under which the trade secret was disclosed; (ii) the employee's state of mind; and (iii) the "reasonableness" of the conduct of the employer and, in particular, the measures adopted by the employer to signal its

2229 Restatement (Third) of Unfair Competition § 42 (Am. Law Inst. 1995) comment c; by way of illustration see *L.M. Rabinowitz & Co. v. Dasher*, 82 N.Y.S. 2d 431, 435 (1948): "It is implied in every contract of employment that the employee will hold sacred any trade secrets or other confidential information which he acquires in the course of his employment".

2230 James Pooley 2002 (n 66) 6-24.

secret nature, for instance limiting its access or identifying a specific piece of information as confidential.[2231]

If such a duty is established, the UTSA,[2232] the Restatement (Third) of Unfair Competition[2233] and the DTSA[2234] set out general liability for the acquisition, use and disclosure of a trade secret as a result of the breach or the inducement to breach a secrecy obligation.[2235] Consequently, the disclosure and use of a trade secret after the termination of an employment relationship may trigger liability for the former employee under both the state and federal trade secrets legal regimes. Similarly, liability may arise with respect to the new employer if they knew or had reason to know that the information was acquired as a result of such a breach.[2236]

Notwithstanding the above considerations, courts have also acknowledged the right of individuals to carry out their profession and the importance of preventing employers from privatising the skills, knowledge and experiences necessary to that end.[2237] Along this line, in the seminal article 'The legal infrastructure of high technology industrial districts: Silicon Valley, Route 128, and Covenants not to Compete,' Gilson distinguished between mere information and tacit knowledge.[2238] The former includes "easily codifiable information",[2239] while the latter refers to the "skill and expertise" of employees that is necessary for "effectively creating, developing, and implementing" innovations, which is "embedded in the human

2231 See Elisabeth A. Rowe and Sharon K. Sandeen, *Trade Secrecy and International Transactions: Law and Practice* (Edward Elgar 2015) paras 5.13-5.17 with further references.

2232 See § 1(1) and (2) UTSA.

2233 Restatement (Third) of Unfair Competition § 42 (Am. Law Inst. 1995) comment b.

2234 18 U.S.C. § 1839 (6) (A).

2235 Miles J. Feldman 1994 (n 2224) 163-164.

2236 Ronald J. Gilson, 'The Legal Infrastructure of High Technology Industrial Districts: Silicon Valley, Route 128, and Covenants Not to Compete' [1999] 74 NYULR 575, 597 highlighting the difficulties that the former employer faces in providing evidence.

2237 *CVD, Inc. v. Raytheon Co*., 769 F2d 842, 852 (1st Cir. 1985): "It is also 'well settled that an employee upon terminating his employment may carry away and use the general skill or knowledge acquired during the course of the employment.' This principle effectuates the public interest in labor mobility, promotes the employee's freedom to practice a profession, and freedom of competition".

2238 Ronald J. Gilson 1999 (n 2236) 582.

2239 Ronald J. Gilson 1999 (n 2236) 577, footnote 10.

capital" of the employer.[2240] In turn, tacit information may consist of trade secrets, the disclosure of which can be prevented by employers, and general and industry-specific knowledge, which departing employees are free to use.[2241] Following Gilson's approach, such a division allows for involuntary knowledge spill-overs, when workers move from one employer to another. These are crucial to the development of new technologies that ultimately result in new industrial life cycles, as illustrated by the success of Silicon Valley.[2242]

The most important source of law that regulates the problem of the skills, knowledge and experience that departing employees are free to use is the Restatement (Third) of Unfair Competition (and more recently the DTSA).[2243] Prior to its adoption, the legislative landscape was seemingly uncertain. The relevant provisions of the Restatement (First) of Torts and the UTSA did not address, in a clear manner, the issue of the information that departing employees could use after the termination of their employment relationship.[2244] This normative vacuum was overcome by the Restatement (Third) of Unfair Competition, which provides that information that is part of the skills, knowledge, training and experience of an employee cannot be claimed as constituting a trade secret by the former employer. Such a principle applies even if there is a direct causal link between the acquisition of information and skills by the departing worker and an investment made by the employer.[2245] Yet, in the U.S. there is no universal legal standard that allows for drawing a clear line between protected trade secrets and skills and knowledge that employees are free to use after the termination of their employment relationship. Indeed, in many fields, but particularly in the technological sector, the knowledge and experience gained by an employee in the performance of his duties are inextricably embedded in the trade secrets of the former employer.[2246] Consequently, courts have to balance a number of factors against each other in the event of litigation.

2240 Ronald J. Gilson 1999 (n 2236) 582.
2241 Ronald J. Gilson 1999 (n 2236) 599.
2242 Ronald J. Gilson 1999 (n 2236) 586.
2243 18 U.S.C. § 1836 (b)(3)(A)(i)(I)-(II).
2244 Miles J. Feldman 1994 (n 2224) 155.
2245 Restatement (Third) of Unfair Competition § 42 (Am. Law Inst. 1995) comment d.
2246 Miles J. Feldman 1994 (n 2224) 153.

The five most salient principles developed by the Restatement (Third) of Unfair Competition, legal commentators[2247] and case law to draw the dividing line are: (i) whether the information is specialised or unique to the employer or is common knowledge among a specific industry;[2248] (ii) the contribution of the employer and of the employee in generating the information; (iii) whether competitors had previously failed in developing the same product or process;[2249] (iv) if the employee, shortly before the termination of his contractual relationship, took some physical embodiment of the information such as written formulas, blueprints, plans, or lists of customers;[2250] and (v) whether preventing the employee from using the information would hinder him from finding a new job, taking into account his overall experience.[2251]

The above reproduced multifactor test operates as a default rule when the parties cannot reach an agreement. Its main advantage lies in the fact that it provides greater legal certainty to those considering litigation, since it gives notice of the elements that courts will take into account in rendering their judgement.[2252]

Although the courts in the U.S. have long acknowledged the welfare benefits of employee mobility, the doctrine of "inevitable disclosure" is still applied in a number of states.[2253] Such a doctrine allows courts to enjoin a departing employee from working for a competitor based on the assumption that he will not be able to separate the former employer's trade secrets from his own knowledge, in such a way that the acquisition, use and disclosure of the information during the new employment is unavoid-

---

2247 Miles J. Feldman 1994 (n 2224) 117 proposes a multi-factor test based on the factors mentioned in the Restatement (Third) of Unfair Competition § 42 (Am. Law Inst. 1995).

2248 *GTI Corporation v. Calhoon*; 309 F. Supp. 762, 770-772 (S.D. Ohio 1969).

2249 *Head Ski Co. v. Kam Ski Co*., 158 F. Supp. 919, 923-924 (D. Md. 1958).

2250 *AMP Inc. v. Fleischhacker*, 823 F.2d 1199, 1204-1205 (7th Cir. 1987).

2251 Restatement (Third) of Unfair Competition § 42 (Am. Law Inst. 1995) comment d.

2252 As noted by Miles J. Feldman 1994 (n 2224) 117.

2253 For an overview of the practice in each state see Ryan M. Wiesner, 'A State-By-State Analysis of Inevitable Disclosure: A Need for Uniformity and a Workable Standard' [2012] 16 Marquette IPLR 211, 217-228; Robert P. Merges, 'The Law and Economics of Employee Inventions' [1999] 13 Harvard Journal of Law & Technology 1, footnote 179; William van Caenegem 2014 (n 7) 118 (citing David W Quito and Stuart H Singer, *Trade Secrets: Law and Practice* (OUP 2009) 91-101) noting that the theory has been disregarded in six states, accepted in thirteen, and received mixed reviews in the rest.

able.[2254] This rationale was expressed in *Lumey Inc. v. Highsmith*, where the court noted that: "Even assuming the best of good faith, it is doubtful whether the defendant could completely divorce his knowledge of the trade secrets from any...work he might engage with the new employer".[2255]

Many authors have criticised this doctrine as being particularly unfair. The employee is prevented from working in his field of expertise without agreeing to such a "garden leave" (unlike the case of non-compete agreements) and without any compensation, thereby by-passing the minimum guarantees provided for under employment law.[2256] As suggested by Milgrim: "It potentially converts into a potential injunctive relief situation virtually any competitive employment taken by an individual who had held any kind of position –technological or commercial- or responsibility with plaintiff but had not entered into a restrictive covenant and accordingly not been given any consideration for restricting his post-employment obligations".[2257] In addition, from a policy perspective, the broad scope of these injunctions may hinder the positive spill-overs derived from employee mobility.[2258] The five main factors that have most often been invoked in the application of the inevitable disclosure doctrine were laid down by the

2254 Melvin F. Jager, *Trade Secrets Law* (Thomsons Reuters 2015) § 7:6; *Dayton Superior Corp. v. Yan et al*, No. 3:2012cv00380 (S.D. Ohio 2012).

2255 *Lumey Inc. v. Highsmith*, 919 F Supp. 624, 633 (E.D.N.Y. 1996).

2256 Elizabeth A. Rowe and Sharon K. Sandeen, *Trade Secrecy and International Transactions* (Edward Elgar 2015) para 5,46 further note that it is a well-established principle under employment law in the U.S. that any employee may decide to resign from his position, unless the parties have contractually agreed to the contratry, as per *McCrady v. Oklahoma Department of Public Safety*, 122 P.3d 473, 474-475 (Okla. 2005).

2257 Roger M. Milgrim 2014 (n 160) § 5.02[3][d] 74.

2258 Ronald J. Gilson 1999 (n 2236) 624; William van Caenegem 2014 (n 7) 203; similar concerns were raised by the District Court of the Southern District of New York in *EarthWeb, Inc. v Schlack*, 71 F. Supp.2d 299, 310-311 (S.D.N.Y. 1999): "While the inevitable disclosure doctrine may serve the salutary purpose of protecting a company's investment in its trade secrets, its application is fraught with hazards. Among these risks is the imperceptible shift in bargaining power that necessarily occurs upon the commencement of an employment relationship marked by the execution of a confidentiality 26 agreement. When that relationship eventually ends, the partie' confidentiality agreement may be wielded as a restrictive covenant, depending on how the employer views the new job its former employee has accepted. This can be a powerful weapon in the hands of an employer; the risk of litigation alone may have a chilling effect on the employee. Such constraints should be the product of open negotiation".

Court of Appeals of the Seventh Circuit in *PepsiCo v. Redmond*[2259] and they are: (i) the intensity of the competition between the companies; (ii) the similarities between the tasks assigned to the departing employee, (iii) the level of responsibility that the employee will take on; and (iv) the value of the secret information and (v) its time-sensitive nature.[2260]

With the above in mind and taking into consideration the sound socio-economic policies underlying employment mobility, the Federal legislator has set forth certain limitations to the doctrine of inevitable disclosure. In effect, section 18 U.S.C. § 1836 (b)(3)(A)(i) (as amended by the DTSA) stipulates that injunction shall not be granted if (i) it would prevent a person from entering into an employment relationship under conditions that result in actual or threatened misappropriation (based not only on the information that the person knows), or (ii) if it conflicts with state law that prohibits restraints on the exercise of a lawful profession, trade or business.

A literal interpretation of the DTSA allows for enjoining a departing employee from entering into a new employment relationship before the Federal Courts if, according to the employment conditions (and not just the information that he knows), he is likely to disclose a former employer's trade secret. The inclusion of this provision has been vehemently criticised by some, as it implicitly recognises the doctrine of inevitable disclosure and incorporates it into Federal Law, despite the positive spill-overs derived from employee mobility and the fact that many state laws reject it.[2261] It is for this reason that its application has been excluded when it conflicts with state law, as would be the case with California state law.[2262] However, in those states that do apply such a doctrine, the requisite that the plaintiff provides evidence of threatened misappropriation has been interpreted as limiting its applicability.[2263]

In the light of the above considerations, it seems that in the near feature a new body of federal jurisprudence regulating post-contractual obligations will emerge, thus shedding further light on the relationship between

2259 *Pepsi Co, Inc. v. Redmond*, 54 F3d 1262 (7th Cir. 1995).

2260 A more detailed account of these factors is provided by Elizabeth A. Rowe and Sharon K. Sandeen, *Trade Secrecy and International Transactions* (Edward Elgar 2015) para 5.46.

2261 Eric Godman and others, 'Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015' (November 17, 2015), 5 <https://cyberlaw.stanford.edu/files/blogs/2015%20Professors%20Letter%20in%20Opposition%20to%20DTSA%20FINAL.pdf> accessed 15 September 2018.

2262 Victoria A. Cundiff and others 2016 (n 789) 742.

2263 Sharon K. Sandeen and Christopher B. Seaman 2017 (n 673) 900-901.

trade secrets protection and the skills and knowledge that former employees are free to use, as well the applicability of the restraints of trade doctrine.

bb) England

In England, the general principle is that employees owe a duty of fidelity and good faith to their employer, which transcends the end of the employment relationship.[2264] This consideration has been criticised by recent academic work, where it is suggested that the duty of fidelity comes to an end with the termination of the employment contract.[2265] Consequently, the better view is to conceptualise the nature of the obligation between the employer and the employee as an implied contract subsisting between the two parties.[2266] Accordingly, the scope of this obligation can only extend to the information that the employee retains and that he knew (or it was obvious from the circumstances) constituted a trade secret.[2267] In a similar vein, the Law Commission Report held that in England the breach of confidence action could not be used to prevent a departing employee from using the skills, knowledge and experience "acquired at work and which is personal to the acquirer".[2268] This principle was subsequently restated in a number of decisions.[2269] However, just like in the U.S., courts have struggled to draw a dividing line between protectable trade secrets and skills,

2264 John Hull 1998 (1016) paras 7.01-7-07 however notes that the "ex-employee's duty to his employer is however narrower than the corresponding duty of good faith which was effective during employment".

2265 Tanya Aplin and others 2012 (n 22) para 12.150.

2266 Tanya Aplin and others 2012 (n 22) para 12.155 also argue that equity could also be invoked as a valid cause of action.

2267 Tanya Aplin and others 2012 (n 22) para 12.164.

2268 Law Commission 1981 (n 327) para 4.33.

2269 For instance, *Generics (UK) Ltd v Yeda Research and Development Co Ltd & Anor* [2012] EWCA Civ 726, [82]: "There is a long-established line of authority that, if an employer wishes to restrict the activities of an employee after termination of the employment, that should be done by a legally valid restrictive covenant. This is because the employee must know with certainty what it is that the employee will be able to undertake for any new employer or otherwise in furtherance of the employee's career; and any new employer will want to know the same; the *employee is entitled to deploy in furtherance of his or her career the general experience, skill and knowledge acquired in the course of it; and it may be, and probably will be, difficult to disentangle in relation to any new employment or other career activity protected confidential information, on the one hand, and other infor-*

knowledge and experience that employees are free to use in their new position.

Hitherto, the leading authority on the issue of implied obligations after the termination of an employment relationship is *Faccenda Chicken v Fowler*.[2270] The facts of the case are as follows: Faccenda Chicken's business model comprised the breeding, rearing, slaughtering and selling of chicken. The defendant, Mr Fowler, was employed by the plaintiff for more than twenty years, during which time he proposed and developed a so-called van sales operation model. In essence, the model involved offering daily fresh chickens to customers (butchers, supermarkets, etc.) using refrigerated vehicles. After resigning, Mr Fowler set up a company consisting of the same business activities and hired nine of the plaintiff's employees. Subsequently, Faccenda Chicken Ltd brought an action for an alleged breach of the implied terms of the contracts of employment of the nine departing workers.

When delivering its judgement, the Court of Appeal differentiated between protectable "trade secrets" and "mere confidential information", a distinction that has garnered substantial criticism from legal commentators[2271] and subsequent decisions.[2272] Most notably, it identified four elements that should guide the decision on whether specific information should be deemed as a trade secret or, instead, as mere confidential information that a departing employee should be free to use, which partially coincide with those followed in the U.S. They are: (i) the nature of the employment; (ii) the nature of the information; (iii) whether the employer impressed on the employee the confidentiality of the obligation; and, (iv) whether the information can be easily isolated from other information that the employee is free to use or disclose.[2273] Each of these is analysed in turn.

The first factor, the nature of the employment, was construed as referring to the circle of people to whom the information is imparted. If it is shared with employees who usually deal with confidential information, it is more likely that the courts will consider it a trade secret. By way of ex-

---

mation which it is lawful for the former employee to use or disclose, on the other hand" (emphasis added).

2270 *Faccenda Chicken Ltd v Fowler* [1987] Ch 117 (CA); Roger M. Toulson and Charles M. Phipps 2012 (n 326) [14-008].

2271 Tanya Aplin and others (n 22) para 12.175.

2272 *Lancashire Fires Limited v SA Lyons & Company Limited and Others* [1996] FSR 629 (CA), 655.

2273 *Faccenda Chicken Ltd v Fowler* [1987] Ch 117 (CA), 137-139.

ample, a member of the board is more likely to learn trade secrets in the performance of his duty than a facilities manager.[2274] As regards the nature of the information, the court was of the opinion that in order to merit protection, it is crucial that the information can be defined with some degree of precision.[2275] Next, it went on to highlight that the attitude of the employer towards the information for which protection is sought is of utmost importance, since he must signal its confidential nature to employees. Finally, it was held that it is essential that the information concerned can be separated from other information that the employee is free to use and disclose,[2276] and the skills and knowledge that he acquired during the course of the employment relationship.[2277] The latter principle is in line with the argument that a person should not be restricted from using his skills for his own benefit and that of the general public.[2278]

In *Faccenda Chicken v Fowler* the English Court of Appeal concluded that there had not been a breach of the implied terms, as neither the sales data, nor the price information could be deemed a trade secret.[2279]

cc) Germany

In Germany, the Federal Supreme Court and the Federal Labour Court have taken divergent views on the information that employees may use after the termination of a labour contract. The Federal Supreme Court is of the opinion that departing employees may use all of the information that they have acquired *honestly* during the course of their employment relationship, including trade secrets.[2280] Conversely, the Federal Labour Court holds that former employees are bound not to disclose trade secrets even after the termination of an employment relationship on the basis of a duty

2274 Tanya Aplin and others (n 22) para 12.196.
2275 Lionel Bently and Brad Sherman 2014 (n 125) 1170-1171.
2276 *Faccenda Chicken Ltd v Fowler* [1987] Ch 117 (CA), 136.
2277 Lionel Bently and Brad Sherman 2014 (n 125) 1170-1171.
2278 Roger M. Toulson and Charles M. Phipps 2012 (n 326) 14-010.
2279 *Faccenda Chicken Ltd v Fowler* [1987] Ch 117 (CA), 140 A-B; Tanya Aplin and others 2012 (n 22) para 12.172;
2280 RGZ 1907 65, 333, 337 – *Pomril*; BGH GRUR 1983, 179, 181 – *Stapel-Automat*; *Harte-Bavendamm*/Henning-Bodewig (n 376) § 17 Rdn 45; Rudolf Kraßer 1977 (n 1327) 187; Richard Schlötter 1997 (n 828) 182.

of loyalty ("*Treuepflicht*"),[2281] and there is no need to refer to them specifically in a labour agreement, in line with the interpretation followed by the courts in England and the U.S.[2282] This presumption applies irrespective of the manner (whether lawful or not) in which the trade secrets were acquired.[2283] Such conflicting views reflect the competing policies embedded in the German Constitution: on the one hand, Article 14 GG mandates the protection of immaterial property; on the other, Article 12 GG endorses employment mobility through occupational freedom.

Ultimately, the view held by the Federal Labour Court assumes that it is possible to distinguish between trade secrets and the skills, knowledge and experience lawfully acquired by employees in the normal performance of their duties (doctrine of separability or "*Trennbarkeitsthese*"), contrary to the proposition supported by the Federal Supreme Court[2284] and several German commentators,[2285] who understand that trade secrets may be intrinsically embedded within the personal experience lawfully acquired by employees (doctrine of inseparability). Considering such divergent perspectives, Ohly argues that neither position is absolute because in practice, their application is relativised by a number of legal provisions.[2286] The general view supported by the Federal Supreme Court is subject to the limitations imposed by the Law on Employee Inventions,[2287] which stipulates that an employee making a service invention must report the invention to the employer immediately (§ 5) and must keep it secret (§ 24) even after the termination of the employment relationship (§ 26). In addition, the Federal Supreme Court has held that the use of materials acquired in an unlawful manner during an employment relationship after its termination is proscribed by virtue of § 17(2)(1) and § 17(2)(2) UWG.[2288] The same

2281 Ansgar Ohly 2014 (n 100) 9; Swantje Richters and Carolina Wodtke, 'Schutz von Betriebsgeheimnissen aus Unternehmenssicht "Verhinderung von Know-how Abluss durch eigene Mitarbeiter"' [2003] NZA-RR 281, 285.

2282 Christopher Heath 2017 (n 2221) 101.

2283 Clemens Heusch and others, 'Trade secrets: overlap with restrains of trade, aspects of enforcement' [2015] GRUR Int 932, 934.

2284 BGH GRUR 1983, 179, 181 – *Stapel-Automat*; BGH IIC 2004, 449, 451 – *Spritzgießwerkzeuge.*

2285 Rudolf Kraßer 1977 (n 1327) 186.

2286 Ansgar Ohly 2014 (n 100) 9.

2287 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 (Law on Employee Inventions).

2288 Ansgar Ohly 2014 (n 100) 9.

court has also ruled that the use of a customer list that was copied into the personal computer of the employee with authorisation during the course of employment is unlawful once the contract is terminated and triggers liability under § 17(2)(2) UWG.[2289] Yet, if the departing employee memorised the information, its use in the new position should be deemed lawful.[2290] Consequently, Ohly argues that in practice the theoretical freedom of the departing employee will be limited to a large extent to the information that he can memorise.[2291] In addition, the condition that the information is acquired in an honest manner ultimately requires courts to conduct a balancing exercise considering all of the circumstances of each specific case and weighing up the competing interests.[2292] Indeed, under the doctrine of inseparability, the appraisal of "honesty" on the side of the departing employee is essential to assess his potential liability, unlike the prevailing approaches in the U.S. and England, where the enquiry is instead centred on the existence of a protectable trade secret.[2293]

By the same token, the protection of trade secrets after the termination of an employment relationship supported by the Federal Labour Court is also subject to certain limitations, in particular, with respect to the imposition of de facto non-competition covenants that do not fulfil the statutory requirements set out in §§ 74 – 74c HGB.[2294]

In view of these considerations, the cardinal problem is distinguishing between the skills, knowledge and experience that a former employee can use in his new position and a protected trade secret.[2295] In this respect, the Federal Supreme Court has noted that in the assessment of competitive conduct pursuant to § 3 UWG, deciding courts should consider, on the one hand, the interests of departing employees in their professional advancement, which are protected by constitutional law (Article 12 GG), and on the other, the interest of former employers in keeping their secrets

2289 BGH GRUR 1999, 934, 935 – *Weinberater*.

2290 Clemens Heusch and others, 'Trade secrets: overlap with restrains of trade, aspects of enforcement' GRUR Int [2015] 932, 933; BGH GRUR 1999, 934, 935 – *Weinberater*.

2291 Ansgar Ohly 2014 (n 100) 10.

2292 Ansgar Ohly 2014 (n 100) 10.

2293 Magdalena Kolasa, *Trade Secrets and Employee Mobility* (CUP 2018) 95 onwards.

2294 Handelsgesetzbuch in der im Bundesgesetzblatt Teil III, Gliederungsnummer 4100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 3 des Gesetzes vom 10. Juli 2018 (BGBl. I S. 1102) geändert worden ist (HGB or German Commercial Code); as noted by Ansgar Ohly 2014 (n 100) 10.

2295 Richard Schlötter 1997 (n 828) 179.

undisclosed (according to Article 2(1) and 14 GG). Consequently, it does not appear likely that one absolute formula would allow for drawing the boundaries between the two, because as a matter of principle "the overall balance must relate to the individual case".[2296] To that end, a number of criteria have been formulated by German courts and legal commentators.[2297]

In the first place, it has been suggested that the more relevant information is for the competitiveness of a company, the more likely it is to be treated as a trade secret.[2298] Also, it is crucial that the employee could not have acquired that knowledge if he had worked in the same or a similar position.[2299] Otherwise, it would not qualify as a trade secret. Additional criteria refer to the nature of the information and its importance for the advancement of the employee's career.[2300] Significantly, if the information is of a technical nature, it is similar to a service invention and when it is embodied in a physical support (like a written document) it will be easier to distinguish it from the skills and knowledge that every employee has acquired.[2301] Similarly, if the employee needs the information in order to be able to perform the tasks inherent to his profession, the likelihood that the information concerned will be regarded as skills, knowledge and experience that he is free to use increases. Otherwise, prohibiting the employee from using such knowledge would amount to a non-compete covenant, which under German law is only accepted under the specific conditions set forth in §§ 74- 74c HGB. Likewise, it has been purported that the position of the departing employee within the former company is also relevant. As already noted, if the information was acquired in a dishonest manner during the course of employment, departing employees should not be free to use it. Indeed, such conduct should trigger liability.[2302] As a final remark, legal scholars have held that courts should also take into consideration the

2296 BGH IIC 2004, 449, 452-453– *Spritzgießwerkzeuge*; Rudolf Kraßer 1977 (n 1327) 186.

2297 Richard Schlötter 1997 (n 828) 180.

2298 Richard Schlötter 1997 (n828) 180; Ansgar Ohly 2014 (n 100) 10 noting that the relevance of this criterion should not be overstated.

2299 Richard Schlötter 1997 (n 828) 180.

2300 BGH GRUR 1963, 367, 370 – *Industrieböden*; Ansgar Ohly 2014 (n 100) 10.

2301 Ansgar Ohly 2014 (n 100) 10.

2302 BGH GRUR 1963, 367, 370 – *Industrieböden*; BGH GRUR 1983, 179, 181 – *Stapel-Automat*; Ansgar Ohly 2014 (n 100) 10; Christopher Heath 2017 (n 2221) 102.

contribution of the employee in creating the information. If it is substantial, it is more likely that he will be free to use it.[2303]

In sum, an analysis of the German statutory provisions and case law reveals that there is no universally accepted principle that allows for drawing a clear line. It is again a matter of balancing interests.[2304] However, from the comparative analysis conducted, it seems that in Germany the assessment of the lawfulness and honesty of the conduct of a former employee acquires more relevance in the German Courts than in England and the U.S., at least under the doctrine of separability.

b) Implied secrecy obligation of departing employees under the TSD

In line with the balancing exercise that the courts and legislatures of the studied jurisdictions conduct in order to weigh up the competing interests of trade secret holders and departing employees, Recital 3 TSD states that employee mobility is essential for employment growth and improving the competitiveness of the EU economy. In this context, Article 1(3) TSD clarifies, with respect to the definition of the subject matter and the scope of application of the Directive, that:

> Nothing in this Directive shall be understood to offer any ground for restricting the mobility of employees. In particular, in relation to the exercise of such mobility, this Directive shall not offer any ground for:
> (a) limiting employees' use of information not constituting a trade secret as defined in point (1) of Article 2;
> (b) limiting employees' use of the experience and skills honestly acquired in the normal course of their employment; (…)

As is apparent from the above, firstly the Directive shall not provide a legal basis to prevent employees from using information that falls outside the scope of the definition of trade secrets. In addition, paragraph (b) specifies that the TSD should not be construed as restricting the use of the skills, experience and knowledge that an employee acquired *honestly* during the course of their employment, which furthermore, according to Recital 14, do not constitute a trade secret either.

Such a legislative technique has been criticised for a number of reasons. Firstly, it has been questioned whether including the balancing test of the

2303 Christopher Heath 2017 (n 2221) 90.
2304 Ansgar Ohly 2014 (n 100) 10.

information that employees are free to take into their new positions in the overall assessment of the subject matter protected (Article 2 TSD) rather than in the liability assessment (Article 4(3) TSD) diverts attention away from the real enquiry, i.e. whether employees are free to use the trade secret.[2305] Indeed, the establishment of additional limitations to the subject matter protected adds confusion with respect to the definition of trade secrets, as in some cases the skills, knowledge and experience acquired by an employee may constitute a trade secret according to the statutory definition established in Article 2(1) TSD.[2306] Consequently, the EU legislator should have included the prohibition to limit the use of "experience and skills honestly acquired" within the framework of the exceptions established in Article 5 TSD. This provision does not exclude liability ex ante and in all circumstances, but rather calls upon national judicial authorities to balance the competing interests at stake on a case-by-case basis. Indeed, the application of the legitimate interest exception established in Article 5(d) TSD would allow courts to weigh up whether an employee should be free to use the information acquired as part of their freedom to choose an occupation and the right to engage in work enshrined in Article 15 ChFREU and the interests of the employer in preserving secrecy.[2307] Such an approach is also more in line with the unfair competition principles that inform the appraisal of liability in the TSD and ultimately seek to proscribe only those market practices that are contrary to honest commercial practices.

Secondly, pursuant to the wording of the TSD it is unclear whether it is a matter of EU law or of national courts to establish the relevant criteria to assess whether an employee should be allowed to use a specific piece of information in his new position.[2308] While the existence of an implied duty of confidentiality that may trigger liability under Article 4(3)(b) and 4(4) TSD is left to Member States to regulate, Article 1(3) is ultimately subject to interpretation by the CJEU.[2309] Nevertheless, if the competence of the CJEU is affirmed to regulate post-contractual secrecy obligations, the complex doctrines developed by national courts will be overridden and will have to filled in by means of judicial interpretation on the basis of the

2305 Tanya Aplin 2014 (n 384) 270.
2306 Aurea Suñol, *El Secreto Empresarial* (Thomson Reuters 2009) 252.
2307 See chapter 3 § 5 C) III. 3; see Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 35 and para 38.
2308 Tanya Aplin 2014 (n 384) 271.
2309 Magdalena Kolasa, *Trade Secrets and Employee Mobility* (CUP 2018) 156.

scarce guidance provided in Article 1(3) and Recital 14 TSD. This seems an undesirable result considering that contractual obligations have been excluded from the scope of the harmonised framework established in TSD and the inherent complexity of this topic. Harmonisation should be achieved by means of a legislative proposal rather than judicial interpretation.[2310] Ultimately, such an approach may conflict with the rules that govern the ownership of employee creations, which are governed by national provisions and differ substantially on the topic of secret inventions.[2311]

c) Guiding principles

Drawing from the comparative analysis above, it appears that it is not possible to extract a normative test that allows for delineating in a precise manner when a specific piece of information constitutes a trade secret that merits protection or when it is part of the skills, knowledge and experience that employees are free to use in their new position. Indeed, the case law and legal doctrines in the three studied jurisdictions have acknowledged that the information, skills and knowledge acquired by employees may in fact also meet the standards of protection of trade secrets laws. Consequently, competent national judicial authorities will have to conduct a balancing exercise in which a number of factors will have be weighed against each other in other to find the most appropriate equilibrium between employers' right to protect their valuable information and employees' right to pursue their professional career. In the following paragraphs the eight main factors that should inform such an analysis are formulated.

In the first place, courts should start by looking into whether the information was obtained by the departing employee outside the normal performance of his duties, for instance, by entering into areas of limited access within the company or memorising and printing out documents and taking them outside the premises of the firm, or in any other dishonest manner. This is a clear indicator the information should be deemed as constituting a trade secret and ultimately reflects the requirement established in Article 1(3) TSD that the employee must have acquired the disputed information, skills and knowledge in an *honest* manner (factor 1).[2312] In particu-

2310 For a more detailed argument see Magdalena Kolasa, *Trade Secrets and Employee Mobility* (CUP 2018) 156.
2311 Tanya Aplin 2014 (n 384) 271.
2312 Tanya Aplin and others 2012 (n 22) para 12.192.

lar, due attention should be paid to whether the departing employee acquired the information pursuant to any of the types of conduct deemed unlawful under Article 4(2)(a) TSD.

Next, competent national judicial authorities should consider whether the information concerned is unique to the employer or common ground among a specific industry. In the latter case, it will not meet the secrecy requirement and, as a result, it should not be afforded protection under the trade secrets liability rules (factor 2). Similarly, courts should ponder whether the departing employee could not have acquired the information if he had not been working for the employer (factor 3). This should be construed as signalling the existence of a trade secret worthy of protection, as it provides evidence that the information was not generally known among or readily accessible to persons within the circles that normally deal with similar information. In effect, the new employer would be saving the cost of creating the information concerned.[2313]

Following the principle of employment mobility that informs the Directive, it should also be considered whether precluding the departing employee from using and (or) disclosing certain information would prevent him from working in the field in which he specialises, performing the tasks inherent to his profession or advancing in his career (factor 4). In such a case, the information should not trigger liability under the trade secrets legal regime. To hold otherwise would run counter to the freedom to choose an occupation and the right to engage in work enshrined in Article 15 ChFREU.[2314]

In a similar vein, courts should look into the nature of the information and the difficulties experienced by competitors in duplicating it.[2315] If the information provides a clear competitive advantage to its holder, or competitors have attempted to reverse engineer it (without success) or find a similar technical solution, the information concerned should merit protection (factor 5). In effect, any third party trying to find it out would have to invest time and effort in developing the secret, which in turn suggests that the information concerned is a valuable secret worthy of protection. By the same token, some commentators have suggested that information that can

2313 But see William van Caenegem (n 7) 199 noting that the importance of this principle should not be overstated becasuse its unique nature may be "coincidental", "irrelevant" and "unidentified" by the employer. Hence, the author argues that courts should not enforce trade secrets that the employers decided after the termination of the contract that constituted valuable trade secrets.

2314 See Article 15 ChFREU.

2315 Tanya Aplin and others 2012 (n 22) para 12.184.

be acquired through mechanical processes (such as Internet searches) lacks the necessary quality of secrecy.[2316] By contrast, high expenditure on the development of the information concerned (particularly Research and Development) should be viewed as a sign that it is eligible for trade secrets protection.[2317] After all, the law of trade secrets protects investment in the creation of information.[2318]

An additional factor that is taken into consideration in jurisdictions such as the U.S. and Germany and seems pertinent in the assessment of protection is whether the contribution of the employee in the development of the secret is substantial (factor 6). In such a case, it should be deemed as part of the experience and skills that he should be able to use and develop in his new position. However, defining when the contribution is in fact substantial in relation to the employer or other employees appears to be a grey area and is very difficult to assess in terms of evidence due to the high mobility and collaborative environment within companies. In addition, it also contravenes the ownership presumptions applicable under some intellectual property national laws, which provide that if an invention (patentable or not) is developed in the normal course of employment, the ownership should be vested on the employer, irrespective of the employee's contribution.[2319] As a result, this factor seems weak not only from a practical standpoint, but also taking into consideration the harmonisation goals pursued by the Directive, and should only be considered secondary evidence.

On the contrary, the attitude of the employer towards the information is essential (factor 7). In line with the third prong of the definition of trade secrets laid down in Article 2(1)(c) TSD and the prevailing doctrine in the English jurisdictions, the holder of the information must take measures to protect its secret nature. That is, the employer must impart the necessary quality of confidence and treat the information as confidential under the general standard of due diligence within the company sphere.

Finally, the more identifiable the information is, the more likely it is to be regarded as a trade secret (factor 8). In effect, information about specific products or processes, and the best way and skills necessary to implement them is acquired during the course of the employee's development and, as

2316 Tanya Aplin and others 2012 (n 22) para 12.184.
2317 Tanya Aplin and others 2012 (n 22) para 12.183.
2318 As argued in chapter 1 § 2 B) I.
2319 For instance Articles 15, 16 and 17 of the Spanish Patent Act refer to inventions in general, thereby including both trade secrets and patents.

a result, integrates the so-called "mental equipment" or "professional expertise" inherent to the position that he occupies within his company.[2320] This set of skills and knowledge is linked to his professional development and therefore he should be free to use them in any new position that he takes on. In this context, the fact that the information can be easily isolated from his professional expertise, for instance, because it is embodied in a physical support, will be a factor pointing towards the existence of a trade secret. Indeed, if the information is of a mixed nature, and includes skills and knowledge that do not qualify for trade secrets protection and valuable trade secrets that are not precisely identified, the courts will tend to deny injunctions and favour the freedom to work.[2321]

2. Some considerations regarding post contractual non-disclosure and non-competition clauses

The foregoing analysis has delved into the non-contractual secrecy obligations after the termination of an employment relationship. Nonetheless, due to the lack of uniform standards in the enforcement of the implied terms after the termination of an employment relationship, post-contractual obligations play a central role in preventing former employees from using secret information that they acquired in their previous positions.[2322] The two most important contractual devices deployed to that end are confidentiality clauses and non-compete agreements.

The former seek to "identify, clarify or extend the information classified as a trade secret, and introduce express legal obligations in relation to them during employment, but more relevantly, after the termination".[2323] Yet, the courts have long since acknowledged the shortcomings of confidentiality clauses. Indeed, it is very difficult to monitor the use and disclosure of information by a departing employee in his new position; the employer will only learn ex post facto about it and, thus, will not be able to prevent it. In addition, the enforcement of confidentiality clauses is seemingly problematic, as it requires that the alleged secret information is precisely

2320 Tanya Aplin and others 2012 (n 22) para 12.186.
2321 William van Caenegem (n 7) 199.
2322 Charlotte Sander, 'Schutz nicht offenbarter betrieblicher Informationen nach der Beendigung des Arbeitsverhältnisses im deutschen und amerikanishcen Rect' [2013] GRUR Int 217, 225.
2323 William van Caenegem (n 7) 202.

defined and usually courts tend to take into account specific aspects on a case-by-case basis.[2324]

In view of the hurdles posed by NDAs, non-competes are usually perceived as a more efficient tool to prevent the dissemination of confidential information.[2325] As such, these preclude the departing employee from working in a specific field, subject to geographical and time limitations.[2326] In this context, it is much easier for the former employer to identify the field in which the employee will work and to seek ex ante remedies to prevent disclosure. Notwithstanding this, the effects of such contractual devices on employee mobility and competition have been the object of extensive scholarly debate and have given rise to substantial economic literature on the potential negative impact on innovation.[2327]

a) Comparative law analysis

aa) U.S.

Under U.S. law, the validity of non-disclosure agreements is assessed according to the applicable state law. In general, these types of agreements seem to be accepted in all states and they are not subject to additional consideration, as it is regarded that they expressly establish an obligation that is implicitly provided for by law.[2328] They mostly take two forms: they can be regulated in a separate confidentiality agreement (also known as a non-disclosure agreement or NDA) or they can be included as a contractual

2324 Tanya Aplin and others 2012 (n 22) para 12.04.

2325 Yuval Feldman, 'Behavioral And Social Mechanisms that Undermine Legality in The Workplace: Examining The Efficacy of Trade-Secrets Laws Among Knowledge Workers in Silicon Valley' (2005) Bar Ilan University Public: Law Working Paper No. 1-05, 24 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=714481> accessed 15 September 2018.

2326 Tanya Aplin and others 2012 (n 22) para 12.04.

2327 William van Caenegem 2014 (n 7) 203; White House, 'Non-Compete Agreements: Analysis of the Usage, Potential Issues, and State Responses' (2016); Elisabeth A. Rowe. 'When Trade Secrets become Shackles: Fairness and the Inevitable Dis- closure Doctrine' [2005] 7 Tulane J of Technology & IP 167.<https://obamawhitehouse.archives.gov/sites/default/files/non-competes_report_final2.pdf> accessed 15 September 2018.

2328 Elizabeth A. Rowe 2005 (n 2327) 189; James Pooley 2002 (n 66) 8-4.

clause within the employment contract.[2329] From a practical perspective, the inclusion of these types of clauses is important in order to define the obligations regarding secrecy of the employee and to show the adoption of reasonable measures to protect the secret nature of information by the trade secret holder.[2330]

Unlike in the case of non-competes, the employee can move on to work for a competitor, but he cannot disclose (or use) the information that he acquired while working for the former employee.[2331] However, in the event that a specific NDA may have a negative impact on the career development of departing employees, courts will proceed to examine the reasonability of its terms in their assessment of its enforceability.[2332] In effect, most state courts require that NDAs are reasonable in scope and protect a legitimate business interest, such as a trade secret.[2333] Accordingly, an NDA covering an obligation not to disclose or use information that is part of the skills, knowledge, training and experience of an employee will generally be considered null and void.[2334] By the same token, non-disclosure agreements that cover information that is publicly available will also be considered non-enforceable.[2335] Consequently, courts have stated that it is of utmost importance that the employer identifies the information in a precise manner. Indeed, some courts in the U.S. have rejected the enforcement of NDAs drafted in a very general and vague manner.[2336] As a final note, it should be stressed that courts have given divergent interpretations in regard to the question of whether NDAs need to be geographically and temporally limited.[2337] While some take a very strict approach, others seem

2329 Elizabeth A. Rowe and Sharon K. Sandeen, 'Trade Secrecy and International Transactions: Law and Practice' (Edward Elgar 2015) para 5.19.
2330 Elizabeth A. Rowe 2005 (n 2327) 190.
2331 Norman D. Bishara, Kenneth J. Martin, Randall S. Thomas, 'An Empirical Analysis of Noncompetition Clauses and Other Restrictive Postemployment Covenants' [2015] 68 Vandervilt LR 1, 20.
2332 Elizabeth A. Rowe and Sharon K. Sandeen, 'Trade Secrecy and International Transactions: Law and Practice' (Edward Elgar 2015) para 5.18.
2333 Norman D. Bishara, Kenneth J. Martin, Randall S. Thomas, 'An Empirical Analysis of Noncompetition Clauses and Other Restrictive Postemployment Covenants' [2015] 68 Vandervilt LR 1, 21.
2334 Jodi L. Short, 'Killing the Messenger The Use of Nondisclosure Agreements to Silence Whistleblowers' [1999] 60 University of Pittsburgh LR 1207, 1226.
2335 Jodi L. Short 1999 (n 2334) 1227.
2336 *Disher v. Fulgoni*, 464 N.E.2d 639, 643 -644(Ill. App. Ct. 1984).
2337 Jodi L. Short 1999 (n 2334) 1223.

more flexible in their assessment of the "reasonableness" of the terms of a contract.[2338]

With respect to non-competition agreements, it should be noted that the assessment of their validity should also be conducted according to the applicable state law.[2339] In some of them, these types of covenants are considered non-enforceable, while others only accept them under very limited circumstances.[2340] Most notably, the California Business and Professions Code stipulates that "every contract by which anyone is restrained from engaging in a lawful profession, trade, or business" is void.[2341] This provision aims at fostering open competition and employees' right to pursue employment and enterprise and has been interpreted in a very restrictive manner by the California Supreme Court.[2342] In effect, in *Edwards v Arthur Andersen*, the court concluded that any restriction on the employee's ability to work in his profession (even if limited or narrow) was void under § 16600 of the California Business and Professions Code.[2343] With time, the Californian approach has become increasingly popular among a minority of States, such as Hawaii, North Dakota, and Oklahoma, where non-competes are also considered generally non-enforceable.[2344] Similarly, in Colorado and Oregon, non-competes are not enforceable against managers and professional workers.[2345] Some commentators have suggested that this tendency results from the establishment of a causality link between the economic success of Silicon Valley and the invalidity of non-competes under California law, which other state legislatures are trying to replicate by proscribing the enforcement of non-competes.[2346] In this respect, it should

2338 *Papa John's International, Inc. v. Pizza Magia International, LLC*, No. 00-10071 (5th Cir. 2001).

2339 Viva R. Moffat, 'Making Non-Competes Unenforceable' [2012] 54 Arizona LR 939, 943.

2340 Elizabeth A. Rowe 2005 (n 2327) 190.

2341 Cal. Bus. & Prof. Code § 16600 (West. 2010).

2342 On Amir and Orly Lobel, 'Driving Performance: A Growth Theory on Noncompete Law' [2013] 16 Stanford Technology LR 833, 842.

2343 *Edwards v. Arthur Andersen LLP*, 189 P.3d 285, 296 (Cal. 2008).

2344 Robert W. Gomulkiewicz, 'Leaky Covenants-Not-to-Compete' [2015] 49 University of California Davis LR 251, 265.

2345 On Amir and Orly Lobel, 'Driving Performance: A Growth Theory on Noncompete Law' [2013] 16 Stanford Technology LR 833, 843.

2346 Robert W. Gomulkiewicz, 'Leaky Covenants-Not-to-Compete' [2015] 49 University of California Davis LR 251, 255 referring to the impact of Ronald J. Gilson 1999 (n 2236) 575.

be noted that the Congress has recently proposed a bill to prohibit employers from entering into covenants not to compete.[2347]

Notwithstanding the aforementioned, according to the prevailing legal doctrine, in most states where non-competes are deemed enforceable, courts examine their validity through strict lenses and on a case-by-case basis. Generally, the employer is required to provide evidence that the agreement is *reasonably* ("rule of reason"): (i) necessary to protect a trade legitimate interest of the employer (for example, trade secrets and goodwill); (ii) limited in duration (according to the prevailing views, two years seems to be the maximum allowed);[2348] (iii) limited in geographical scope; and (iv) limited in the scope of the proscribed activity.[2349] In addition, their validity is subject to receiving adequate compensation, which is usually considered to be satisfied by the salary agreed. However, in the event that the non-compete is executed after the employment relationship has commenced, states' case law is divided among those states that require additional compensation (in the form of a salary increase or a mere lump sum) and those that consider that no increase is required.[2350] In sum, it appears that different states have developed different tests to apply the rule of reason, which has led to a general lack of uniformity and predictability with regard to the enforceability of non-competes.[2351]

bb) England

In England, post-contractual non-disclosure and non-competition agreements are assessed under the general contractual restraints of trade doctrine. According to Diplock LJ:

> A contract in restraint of trade is one in which a party (the covenantor) agrees with another party (the covenantee) to restrict his liberty in the

2347 See H. R. 5631 To prohibit employers from requiring employees to enter into covenants not to compete, and for other purposes <https://www.congress.gov/115/bills/hr5631/BILLS-115hr5631ih.pdf> accessed 15 September 2018.

2348 James Pooley 2002 (n 66) 8-36.

2349 Elizabeth A. Rowe 2005 (n 2327) 190; Roger M. Milgrim 2014 (n 160) § 6.01[3][d] 12; Viva R. Moffat, 'Making Non-Competes Unenforceable' [2012] 54 Arizona LR 939, 948.

2350 Elizabeth A. Rowe and Sharon K. Sandeen, 'Trade Secrecy and International Transactions: Law and Practice' (Edward Elgar 2015) para 5.39.

2351 Viva R. Moffat, 'Making Non-Competes Unenforceable' [2012] 54 Arizona LR 939, 948.

> future to carry on trade with other persons not parties to the contract in such a manner as he chooses.[2352]

As is apparent from the above, the restraint of trade doctrine applies when a person is contractually "bound for the future, and with respect to third parties".[2353] From the outset it should be noted that its applicability is not limited to employment contracts; it also applies to agreements between suppliers of goods and services that restrict competition; exclusive dealing agreements; and also covenants affecting the use of land, to name some.[2354] However, it is generally accepted that post-employment agreements are scrutinised under more strict lenses than other types of covenants.[2355]

The foundation of the modern restraints of trade doctrine was formulated by the House of Lords in *Nordenfelt v Maxim Nordenfelt Guns and Ammunition Co Ltd*[2356] and it essentially provides that contracts that result in a restraint of trade are void, unless such a restraint is reasonable in the interests of the parties and the general public. This doctrine is ultimately built on the public interest in allowing citizens to use their skills to develop the means to make a living and the right of individuals to work,[2357] which collide with the principle of freedom of contract and the right of corporations to protect their secrets.[2358] Recent academic work has identified five sequential steps to be used in order to assess whether an agreement affecting a departing employee is void under the restraint of trade doctrine, which will guide the present discussion.[2359]

First, the competent court should delineate with precision the obligations imposed upon the departing employee by the agreement. Secondly, it should be established whether the contractual provisions restrain the

2352 *Petrofina (Great Britain) Ltd v Martin* [1966] Ch 146, 180 (CA).
2353 John D. Heydon, *The restraint of trade doctrine* (2nd edn, Butterworths 1999) 43.
2354 Edwin Peel, *The Law of Contract* (14th edn, Sweet&Maxwell 2015) para 11-065.
2355 John D. Heydon, *The restraint of trade doctrine* (2nd edn, Butterworths 1999) 66-67.
2356 *Nordenfelt v Maxim Nordenfelt Guns and Ammunition Co Ltd* [1984] AC 535 (HL).
2357 Tanya Aplin and others 2012 (n 22) 12.09
2358 Guy Tritton, 'Employees, Trade Secrets and Restrictive Covenants in the United Kingdom' 61, 69 in Christopher Heath and Anselm Kamperman Sanders (eds), *Employees Trade Secrets and Restrictive Covenants* (Wolters Kluwer 2017).
2359 Tanya Aplin and others 2012 (n 22) para 12.12.

employee, for instance, by preventing him from working in a particular field.[2360]

Thirdly, courts should interrogate whether the restraint falls within one of the interests that case law has identified as *legitimate*. The imposition of a restraint of trade may only be justified if it protects a proprietary interest of the employer.[2361] In particular, the House of Lords identified as legitimate interests that may justify a restraint: (i) trade secrets and confidential information, and (ii) customer connections and goodwill.[2362] The scope of the former category was famously addressed in *Faccenda Chicken v Fowler*,[2363] where the Court of Appeal held that a departing employee's implied obligations were confined to "trade secrets, or the equivalent of trade secrets", which was a distinctly narrower notion than that of confidential information.[2364] In addition, it was held that restrictive covenants would only be enforceable if they protected a trade secret as opposed to confidential information in general.[2365] Such a limited interpretation of trade secrets with respect to restrictive covenants has been the object of vehement criticism.[2366] Consequently, more recent decisions have ruled that a legitimate interest may include both trade secrets and confidential information.[2367]

Fourthly, after identifying the concurrence of a legitimate interest, courts must assess if the restraint is reasonable considering the employer's and the employee's interests and the temporal, geographic, and material scope of the covenant. In particular, in one of the leading decisions on the subject, *Herbert Morris Ltd v Saxelby*, it was noted that the restraint "must afford no more than adequate protection to the benefit of the party in whose favour it is imposed".[2368] In effect, the assessment of reasonableness is usually conducted from the perspective of the employer and the protec-

2360 Tanya Aplin and others 2012 (n 22) para 12.20.
2361 John Hull 1998 (1016) para 8.13
2362 *Herbert Morris Ltd v Saxelby* [1916] AC 688 (HL), 702.
2363 *Faccenda Chicken Ltd v Fowler* [1987] Ch 117 (CA); a summary of the facts of the case is provided in chapter 6 § 1 A) II. 1. a) bb).
2364 *Faccenda Chicken Ltd v Fowler* [1987] Ch 117 (CA), 127.
2365 *Faccenda Chicken Ltd v Fowler* [1987] Ch 117 (CA), 127.
2366 John Hull 1998 (1016) para 8.79; Tanya Aplin and others 2012 (n 22) paras 12.72 -12.76.
2367 Guy Tritton 2017 (n 2358) 76 72; *Lancashire Fires Limited v S.A. Lyons & Company Limited and Others* [1996] FSR 629 (CA), 666.
2368 *Herbert Morris Ltd v Saxelby* [1916] AC 688 (HL), 707.

tion of his legitimate interests, rather than that of the employee.[2369] Ultimately, the assessment of reasonableness will depend on the specific circumstances of the case and the specific industry practices.[2370] Additional factors that courts have taken into consideration are the amount of time during which the employee worked for the employer, the negotiation process of the contract or how the employment relationship was terminated.[2371] Interestingly, in England, the compensation received by the employee is not taken into consideration in the assessment of the reasonableness of the restraint.[2372] This contrasts with the prevailing view in most U.S. states and Germany, where adequate consideration is a precondition of validity for non-competition agreements. Finally, if a court considers that a contract imposes an unreasonable restraint, it will strike out the void parts by application of the doctrine of severance.[2373]

Having regard to the above, a number of considerations should be presented with respect to the applicability of the restraints of trade doctrine to non-disclosure and non-competition agreements.

Firstly, considering NDAs, it should be noted that courts seem inclined to enforce them provided that they do not include information that is in the public domain or that constitutes part of the skills, knowledge and experience that employees should be free to use.[2374] This mostly favourable tendency results from the fact that the scope of these agreements mostly coincides with the scope of the implied obligation not to disclose trade secrets. However, limitations regarding use (non-use clauses) are typically assessed under more strict parameters and courts usually proceed to evaluate whether the time, scope and geographical limitations are reasonable.[2375]

Secondly, in the assessment of the reasonableness of non-compete clauses, English courts are especially strict due to the inherent anticompetitive effects triggered by these kinds of provisions. In particular, their duration must be short. There are several cases where restrictions that extended beyond twelve months after the termination of the employment relationship

2369 Dan Prentice, 'Illegality and Public Policy' para 16-106 in Hugh Beale (ed) *Chitty on contracts* (32th edn, Sweet&Maxwell 2017).
2370 John Hull 1998 (1016) para 8.57.
2371 Tanya Aplin and others 2012 (n 22) para 12.95.
2372 Tanya Aplin and others 2012 (n 22) para 12.46.
2373 Guy Tritton 2017 (n 2358) 76 ; Tanya Aplin and others 2012 (n 22) para 12.135
2374 Tanya Aplin and others 2012 (n 22) para 12.99.
2375 Tanya Aplin and others 2012 (n 22) para 12.101.

were declared unreasonable.[2376] Another crucial aspect is the establishment of the scope of the restricted field of activity. English courts tend to demand that the sector and the role that the departing employee is prevented from taking are defined in a very specific manner. Otherwise, it is regarded that the covenant extends beyond the mere prohibition of competition with another business, thereby unreasonably affecting the ability of the employee to develop his professional career.[2377] With respect to the geographical scope, recent decisions seem to support a flexible approach when the legitimate interest invoked is the protection of a trade secret. In such cases, due to the inherently perishable nature of trade secrets, courts seem more inclined to enforce covenants that include a world-wide non-competition clause.[2378] However, if the legitimate interest aims at protecting customer connections, the geographical scope should be limited to the area in which the company had customers on the date on which the employment contract was entered into.[2379]

As a whole, it appears that the restraints of trade doctrine provides great flexibility to courts in their assessment of the validity of NDAs and non-competes, which furthermore are not subject to additional consideration. Notwithstanding this flexibility, the negative effect of non-competes on innovation was acknowledged by the UK Government in 2016 in the context of a consultation regarding the assessment of the need to pass a specific regulation on this subject. However, due to the fact that the vast majority of the respondents argued that non-competes were useful tools to protect their business interests, the consultation was dropped.[2380]

2376 In *Polymasc Pharmaceuticals plc v Charles* [1999] FSR 711 (Pat), 720 and *Dyson Technoloy Ltd v Strutt* [2005] EWHC 2814 (Ch), [66] a one year restrain was not considered problematic.

2377 Tanya Aplin and others 2012 (n 22) paras 12.116 - 12.121.

2378 *Dyson Technology Ltd v Strutt* [2005] EWHC 2814 (Ch), [66].

2379 *Spencer v Marchington* [1988] IRLR 392 (Ch), 395.

2380 Department for Business Innovation & Skills, 'Non-compete clauses – Call for Evidence' (2016) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/525293/bis-16-270-non-compete-clause-call-for-evidence.pdf> accessed 15 September 2018.

cc) Germany

In German law, NDAs are usually considered permissible under §§ 134[2381] and 138[2382] BGB and are not subject to additional consideration and time limitations.[2383] These types of agreements can include trade secrets and information that does not constitute a trade secret but that was expressly identified as confidential by the employer.[2384] However, pursuant to § 138 BGB, an NDA that provides that the employer must keep secret all the information related to the business will be considered void.[2385] The cardinal problem in the assessment of the validity of NDAs is differentiating them from non-competition agreements that are subject to the fulfilment of the statutory requirements set out in §§ 74- 74c HGB.[2386]

By way of illustration, the Federal Labour Court held that an NDA that prevented the manager of a laboratory from disclosing a specific secret formula developed by the employer after the termination of the contract was enforceable, because the development of his professional career would not be hindered by such a prohibition and, furthermore, it did not affect the possibility of the departing employee competing with the former employer.[2387] In contrast, in a later decision, the same court concluded that an NDA that precluded a sales representative from using the names and addresses of clients that the employee had learned during the course of his employment relation for his own benefit (or a third party) was not enforceable because it would prevent him from working in his field of specialisation. Such a non-disclosure agreement would amount to a non-competition covenant that did not meet the statutory requirements.[2388] However, the Federal Labour Court did affirm that the sale of the customers' data would contravene the terms of the NDA.[2389] This position was clari-

2381 § 134 BGB: "A legal transaction that violates a statutory prohibition is void, unless the statute leads to a different conclusion".
2382 § 138 (1) BGB: "A legal transaction which is contrary to public policy is void".
2383 Charlotte Sander 2013 (n 2322) 225.
2384 Martin Brock, 'Know-how im Arbeitsrecht' Rdn 56 in Christop Ann, Michael Loschelder and Markus Grosch (eds), *Praxishandbuch Know-how-Schutz* (Carl Heymanns Verlag 2011).
2385 Martin Brock 2011 (n 2384) Rdn 56; Swantje Richters and Carolina Wodtke 2003 (n 2281) 281.
2386 Wolf Hunold, 'Rechtsprechung zum nachvertraglichen Wettbewerbsverbot' [2007] NZA-RR 617, 619.
2387 BAG NJW 1983, 134, 135 – *Thrombosol*.
2388 BAG NZA 1988, 502, 503 – *Weinhändler*.
2389 BAG NZA 1988, 502, 504 – *Weinhändler*.

fied in a ruling in 1993, regarding the validity of a post-contractual non-disclosure clause of an employee that had been working for forty years for a company in the chemical sector that manufactured a chemical compound known as titandioxid. After the termination of his contract he went on to work for a competitor that also manufactured titandioxid, and consequently, the former employer sought to enforce the NDA in court. The Federal Labour Court generally ruled that an NDA could not prevent a departing employee from using the experience-based knowledge ("*Erfahrungswissens*") that he had acquired while working for the former employer.[2390] It further noted that the use of such information could only be prevented through the conclusion of a valid non-competition agreement.[2391]

The principle that emerges from the analysis of the decisions referred to above is that according to the case law from the Federal Labour Court, in practice NDAs do not provide solid ground to protect trade secrets against use and disclosure by departing employees when such information is embedded in the general skills, knowledge and experience acquired during the course of service.[2392] Ultimately, courts should assess this on a case-by-case basis considering the particularities of the case at hand and whether the NDA concerned in fact covers *Erfahrungswissens* or whether such a provision can de facto be equated to a non-competition agreement.[2393]

Under German law, once the employee has terminated his employment relationship with the principal, he is free to compete with his former employer either by joining a competitor or by setting up his own business.[2394] Such a general principle may only be limited by the conclusion of an express non-competition agreement, which is subject to the fulfilment of the statuary requirements set out in §§ 74-74c HGB, unlike the common law jurisdictions studied, where no statutory provisions in this regard have been enacted. As a preliminary remark, it should be noted that until 2003, these requirements were only applicable to shop clerks. However, by virtue

2390 BAG NZA 1994, 502, 505 – *Titandioxid*.
2391 BAG NZA 1994, 502, 504 – *Titandioxid*.
2392 Martin Brock 2011 (n 2384) Rdn 60-62.
2393 Swantje Richters and Carolina Wodtke 2003 (n 2281) 285.
2394 Wolf Hunold 2007 (n 2386) 617; Dirk Helge Laskawy, 'Die Tücken des nachvertraglichen Wettbewerbsverbots im Arbeitsrecht' [2012] NZA 1011, 1012.

of § 110 of the Industry Regulation Act,[2395] their scope of application was extended to all types of employees.[2396] To be enforceable, non-competition covenants (i) must be in writing and (ii) must be executed by the employee in a separate agreement where the exact terms are specified; (iii) must be subject to the appropriate consideration, which shall be at least 50% of the last gross salary of the employee; and (iv) must not extend beyond two years. Furthermore, pursuant to § 74a HGB, a non-competition agreement is unenforceable if, considering the subject matter, geographical and time scope, it constitutes an unreasonable obstacle to the employee's career development.[2397]

Additionally, just like in the U.S. and England, the validity of non-competes is subject to the protection of the *legitimate interest* of the principal (§ 74a HGB).[2398] The Federal Labour Court has interpreted such a requirement in a rather restrictive manner; it does not suffice that the former employer imposes such a clause with the intention of restraining competition. Consequently, there must be a causal relationship between the activities developed by the former employer and the prohibited act of competition.[2399] In particular, the Federal Labour Court has identified two legitimate interests: (i) the safeguarding of trade secrets (so long as the requirements for protection are still met), and (ii) the protection of a customer base,[2400] which partially coincide with the legitimate interest identified in England under the restraints of trade doctrine. Regarding the question of whether the advancement of an employee's career is unduly affected, the Federal Labour Court has stated that this must be decided on a case-by-case basis taking into consideration a number of factors, such as the age of the employee, the consideration received, the actual scope of the covenant and the mobility within the specific industry.[2401]

2395 See Gewerbeordnung in der Fassung der Bekanntmachung vom 22. Februar 1999 (BGBl. I S. 202), die zuletzt durch Artikel 1 des Gesetzes vom 17. Oktober 2017 (BGBl. I S. 3562) geändert worden ist (Industry Regulation Act).

2396 Martin Brock 2011 (n 2384) Rdn 77.

2397 William van Caenegem (n 7) 191; Wolf Hunold 2007 (n 2386) 617; Charlotte Sander 2013 (n 2322) 225.

2398 Martin Brock 2011 (n 2384) Rdn 87.

2399 Dirk Helge Laskawy, 'Die Tücken des nachvertraglichen Wettbewerbsverbots im Arbeitsrecht' [2012] NZA 1011, 1013.

2400 BAG NZA 1996, 310, 310 – *Nachvertragliches Wettbewerbsverbot.*

2401 BAG NZA 2010, 1175, 1176 – *Anspruch auf KarenzentschÄdigung nur bei verbindlichem Wettbewerbsverbot.*

In sum, it appears that in Germany the conclusion of NDAs after the termination of an employment agreement does not protect the employer against the use and disclosure of the skills, knowledge and experience acquired by the departing employee, which may inextricably include trade secrets. This can only be limited by a non-competition agreement, the validity of which is subject to the fulfilment of the conditions set out in the HGB. In particular, appropriate consideration should be paid and a maximum duration of two years is established. Crucially, this includes the assessment of whether a legitimate interest exists and whether, in view of its territorial, temporal and material scope, it will unduly affect the employee's professional advancement. Hence, the assessment of reasonableness of NDAs and non-competes is ultimately carried out by means of judicial interpretation considering all of the circumstances at stake.[2402]

b) Post-contractual obligations under the TSD

Following a systematic interpretation of the TSD, it can be concluded that the establishment of post-employment contractual obligations is excluded from its scope of application. Pursuant to Recital 13, the possibility of concluding non-compete agreements is governed by the relevant statues of EU and national law. Similarly, Recital 39 sets forth that contract law should not be affected by the norms enshrined in the Directive, which clearly indicates that the regulation of NDAs is also governed by national law. This rationale has further crystallised in Article 1(3)(c) TSD, which lays down that the validity of any contractual restrictions on employee mobility should be assessed in accordance with the relevant national or EU provisions in force.[2403]

However, it is likely that when interpreting the validity of these clauses, national courts across the EU will take into consideration the policy advantages triggered by employee mobility, as one of the principles that inform the TSD and which is therefore part of the acquis communataire, along with the freedom of movement principle. Indeed, in all of the jurisdictions

2402 William van Caenegem (n 7) 191-192.

2403 Article 1(3) TSD: "Nothing in this Directive shall be understood to offer any ground for restricting the mobility of employees. In particular, in relation to the exercise of such mobility, this Directive shall not offer any ground for (c) imposing any additional restrictions on employees in their employment contracts other than in accordance with Union or national law".

studied, the enforcement of NDAs and non-competes is ultimately based on the assessment of the reasonableness of their terms, considering, among other factors, the impact on the career prospects of the employee. Without doubt, post-contractual secrecy obligations are central to preverseving the secret nature of the innovations created intracompany. Yet, they are also subject to a number of limitations to foster competition and safeguard the right of employees to advance in the development of their career.

B) The external sphere of secrecy

The external sphere of secrecy refers to the preservation of confidentiality against the unlawful use and disclosure of trade secrets by third parties that may have accessed the information with authorisation from the holder but only for a limited time, or in order to achieve a specific purpose. This is typically the case for licensing agreements, where the trade secret holder grants the licensee the right to use the secret information in exchange for the payment of an agreed fee. In effect, in order to exploit trade secrets, their holders are required to carefully balance a number of competing interests. On the one hand, they should attempt to share the information with as few people as possible in order to limit the risk of disclosure and the resulting loss of the competitive advantage conferred by its secrecy. Indeed, once the information has left the internal sphere of the company, it cannot be reintroduced due to the inherently irreversible nature of cognitive processes: what has been learnt cannot be unlearnt.[2404]

On the other, to maximise the economic potential of trade secrets, their holder may have to share the information with a substantial number of parties, particularly in the absence of funding resources or manufacturing capabilities that allow for developing the final product.[2405] Similar considerations apply in the conclusion of R&D agreements, by virtue of which a number of parties (including both private and public entities) may decide to cooperate in the generation of technical innovations. Against this background, in order to minimise unauthorised disclosures that may result in the loss of secrecy, it is of utmost importance that the contractual clauses

2404 Stefan Maaßen and Tobias Wuttke, 'Know-how-Verwertung (Veräußerung und Lizenz)' Rdn 38-40 in Christoph Ann, Michael Loschelder and Marcus Grosch (eds), *Praxishandbuch Know-how-Schutz* (Carl Heymanns Verlag 2011).

2405 Stefan Maaßen and Tobias Wuttke 2011 (n 2404) Rdn 40.

that regulate the use and subsequent revelation of secret information are carefully drafted.

More generally, the external sphere of secrecy also refers to the adoption of measures to prevent the unlawful acquisition of trade secrets by any third parties through industrial espionage, as mandated by Article 2(1)(c) TSD. The standard of "reasonableness" has already been examined in previous chapters,[2406] and some examples of the types of measures adopted have been mentioned during the study of the perfume industry.[2407] Consequently, no further reference will be made to the need for companies to implement physical and IT measures.[2408] Instead, the following sections will delve into the study of the regulation of confidentiality obligations in two types of contracts entered into between trade secret holders and third parties in order to maximise the returns from their valuable secret information: licensing agreements (section I) and R&D agreements (section II).

I. Licensing agreements

1. Object and legal nature

Licensing agreements are often conceptualised in contrast to the rights conferred by assignment agreements. Licences, as opposed to assignment agreements, convey no "proprietary interest" in the IPRs that are the object of the contract.[2409] By virtue of such a covenant, the licensee is essentially authorised by the licensor to carry out acts that would otherwise amount to an infringement of IPRs, which would usually be subject to the payment of an agreed consideration.[2410] Consequently, it has been suggested that the licence is "a contractual right rather than an interest in property".[2411]

2406 See chapter 4 § 3 E).
2407 See chapter 5 § 4 B) V.
2408 For an overview of potential measures see Victoria A. Cundiff 2009 (n 739) 364-377.
2409 Noel Byrne and Amanda McBratney, *Licensing Technology* (3rd edn, Jordans 2005) 20-21.
2410 John Hull 2013 (n 934) 170.
2411 Mark Anderson, *Technology Transfer* (3rd edn, Haywards Heath 2010) para 13.5.

In the context of trade secrets,[2412] despite the fact that licensing is one of the main paths by which technology is transferred and commercially exploited, in England and Germany there has been a longstanding debate regarding the legal nature of know-how licences.[2413] This mostly stems from the uncertainty surrounding the legal nature of trade secrets and the fact that they do not confer erga omnes exclusivity on their holders.[2414] In England, case law and commentators have argued that these types of contracts do not confer the right to carry out acts that otherwise are exclusively vested in the owners, as in the case of formal IPR licences. Their essence lies in the disclosure of information between the parties to the contract under specific conditions.[2415]

Similar considerations have been raised in Germany, where, unlike the English jurisdiction, it is generally accepted that know-how licences do confer the licensee the right to use the information imparted.[2416] However, unlike patent or trade mark licences, their existence is not statutorily foreseen. Nevertheless, their validity is inferred from the freedom of contract principle (§§ 134 and 138 BGB), the right to claim the performance of an obligation (§ 241(2) BGB) and the need to conclude a contract in order to create valid contractual obligations (§ 311(1) BGB).[2417] According to the prevailing view, know-how licences are considered to be a sui generis type of contract that should be governed by the rules of legal usufruct ("*Rechtspacht*") as per §§ 581 to 584b BGB for as long as a licensing fee is

2412 Hereafter the term "know-how" will be used in accordance with the definition provided in Article 1(1)(i) TTBER. While this provision requires information to be secret, some German commentators have noted that know-how licences do not require that the information object of the contract is secret, see for instance Kurt Bartenbach, *Patentlizenz-und Know-how-Vertrag* (Verlag Dr. Otto Schmidt 2013) Rdn 2548: "Das nicht geheime Erfahrungswissen ist dagegen das in der jeweiligen Branche bekannte (Grund-) Wissen, das sich jeder Interessent unter Aufwand vo Zeit und Geld auch selbst erarbeitetn könnte"

2413 Recital 4 TTBER highlights the pro-competitive effects of licensing agreements concerning technology because they avoid the duplication of research efforts and spur incremental innovation.

2414 Tanya Aplin and others 2012 (n 22) paras 8.120-8.121.

2415 This was the position supported by the House of Lords in *Rolls-Royce Ltd v Jeffrey (Inspector of Taxes)* [1962] 1 WLR 425 (HL) and Aplin and others 2012 (n) para 8.121.

2416 Kurt Bartenbach 2013 (n 2412) Rdn 2655.

2417 Stefan Maaßen and Tobias Wuttke 2011 (n 2404) Rdn 41-43.

paid.[2418] Notwithstanding this consideration, some commentators have suggested that when the licensor conveys the information without further secrecy or assistance obligations and in exchange for the payment of a lump sum, the rules regulating purchase agreements should apply.[2419]

Likewise, in the U.S., where trade secrets have predominantly been considered a type of IPR by the courts[2420] and know-how licenses are generally accepted, some judicial decisions have also differentiated between the legal nature of formal IPR licences and know-how licences because the latter only bind the licensee, whereas all other competitors are entitled to reverse engineer the product and use it in a lawful manner.[2421]

Finally, it is important to note that based on the object of the contract, know-how licences are generally divided into two categories: (i) pure trade secrets licences, and (ii) technical assistance licences.[2422] The former provide for the use of know-how,[2423] while the latter include the impartment of the secret information along with the supply of technical assistance by the licensor.[2424] Some commentators also distinguish between licences that only provide for the use of know-how and those that foresee a hybrid licence, which includes the conveyance of know-how along with the right to use other IPRs, typically patent rights.[2425] Similarly, a distinction is drawn between exclusive and non-exclusive licences, considering whether the terms of the agreement provide that the licensor undertakes not to share the know-how with any third party (sometimes limited within a specific territory) and not to exploit it himself (exclusive licence) or whether the possibility of granting multiple licences is established (non-exclusive licences).[2426]

2418 Michael Groß, *Der Lizenzvertrag* (Deutsche Fachverlag 2015) Rdn 24; Stefan Maaßen and Tobias Wuttke 2011 (n 2404) Rdn 45; Kurt Bartenbach 2013 (n 2412) Rdn 2660.

2419 Eike Ullman and Hermann Deichfuß, '§ 15 Übertragbarkeit des Rechts; Lizenzen' Rdn 241 in Georg Benkard (ed), *Patentgesetz* (11th edn, C.H. Beck 2015).

2420 See chapter 1 § 3 B) I. 2. b).

2421 See for instance *Painton Company v. Bourns Inc.*, 442 F2d 216, 223 (2d. Cir. 1971).

2422 John Hull 2013 (n 934) 175.

2423 Stefan Maaßen and Tobias Wuttke 2011 (n 2404) Rdn 51

2424 John Hull 2013 (n 934) 175.

2425 Wolfgang Winzer, *Der Lizenzvertrag* (C.H. Beck 2014) Kap. 4, Rdn 17.

2426 Noel Byrne and Amanda McBraty, *Licensing Technology* (3rd edn, 2005 Jordans) 22-24.

2. Secrecy obligations

The legal issues raised by know-how licensing agreements are manifold. However, providing an in-depth analysis of all of them exceeds the scope of the present investigation. In line with the research questions that inform the dissertation, the following sections are devoted to the study of the secrecy obligations of the parties to a licensing agreement in three scenarios: during the pre-contractual negotiations, during the term of the licence, and after its termination. In particular, this thesis does not look into the competition law issues raised by licensing practices and the application of the TTBER, which are only considered insofar as they affect the confidentiality obligations of the parties.

a) Pre-contractual obligations of secrecy

As argued in chapter 1, one of the utilitarian rationales that justifies trade secrets protection is that it provides a legal solution to Arrow's Information Paradox, whereby licensors are wary of disclosing their secret information to potential licensees before concluding an agreement because it puts their information at risk[2427] and, most importantly, the potential licensee may gain knowledge of the information without the need to effectively conclude the agreement and pay any consideration in return.[2428] At the same time, licensors may be sceptical about executing a licensing agreement that binds them for the future without knowledge of the licensed information, because the information may in fact be known to them or it may already be part of the public domain.[2429]

Against this background, it appears that building a relationship of trust with licensees to minimise the risk inherent to such negotiations is of paramount importance, in line with the arguments suggested by the representatives of the perfume industry.[2430] For legal certainty purposes, the conclusion of NDAs also appears particularly advisable,[2431] even though in some jurisdictions an implied duty of secrecy may be established and trig-

2427 Stefan Maaßen and Tobias Wuttke 2011 (n 2404) Rdn 48.
2428 See chapter 1 § 2 B) II.
2429 Robert G. Bone 1998 (n 15) 280.
2430 See chapter 5 § 4 B) V.
2431 John Hull 2013 (n 934) 174.

ger liability in the event of a breach.[2432] In any case, the entering into of such a pre-contractual agreement provides solid evidence that an obligation of secrecy existed. In order to effectively protect the licensor, its scope should be confined to the regulation of the conditions under which the information is disclosed for the sole purpose of allowing the licensee to assess his interest in taking a full licence, without granting the right to make use of the information concerned.[2433] Consequently, such a contract should identify in a precise manner the secret materials and delineate the pre-acquired knowledge of the potential licensee and the knowledge submitted for consideration. Furthermore, in order to ensure the enforceability of secrecy against departing employees, a clause should be included, whereby the licensee undertakes to obtain an express confidentiality obligation from its employees.[2434]

b) During the term of the contract

One of the main objectives of licensing agreements is to regulate the obligations of the parties during the term of the contract. In the context of know-how agreements, confidentiality obligations play a central role both for the licensor and the licensee, as examined in the following sections.

aa) Secrecy obligations of the licensor

The main obligation of the licensor is to supply the licensee with the information that constitutes the know-how object of the contract,[2435] along with the necessary documents to provide the necessary technical assistance and support to the licensee.[2436] In addition, know-how licences frequently include clauses regulating the warranties and representations of the licensor, in particular regarding the transmission of the know-how, the accura-

2432 If such a duty is established, it triggers liability according to Article 4(3)(b) TSD.

2433 John Hull 2013 (n 934) 174-175; *Pagenberg*/Beier, *License Agreements* (Carl Heymanns Verlag 2008) Sample 3, Rdn 4.

2434 *Pagenberg*/Beier (n 2433) Sample 3, Rdn 5-6.

2435 Kurt Bartenbach 2013 (n 2412) Rdn 2776.

2436 Stefan Maaßen and Tobias Wuttke 2011 (n 2404) Rdn 54 highlighting that the scope of this obligation should be assessed on a case-by-case basis considering the specifc circumstances of each case.

cy and completeness of the documents, and even the instruction of the licensee (and his employees).[2437] The obligation to share any further developments and improvements over the licensed information is also usually included in these types of agreements, although in the absence of any specific provision, such an obligation should not be implied, at least under German law.[2438]

As regards secrecy, the licensor is obliged to keep the information secret during the term of the agreement. Otherwise, the information would become generally known and the contract would be deprived of its object. Ultimately, the licensee would not be able to recover the investment made in the preparations for the exploitation of the technology.[2439] Consequently, under German law, if the secret nature of the information is lost for reasons attributable to the licensor, the licensee is entitled to claim damages.[2440]

bb) Secrecy obligations of the licensee

The main obligations of the licensee include, among others, the payment of the agreed licensing fee and keeping the licensed information secret.[2441] The observance of the secrecy obligation is essential to maintain the competitive advantage conferred by the information. Hence, if a breach occurs as a result of a disclosure to a third party by the licensee, liability may arise and accordingly the licensor may claim damages, at least under German law.[2442] Therefore, in the interest of legal certainty, it is highly advisable to specify the terms that will govern such an obligation in the body of the agreement.

Express confidentiality clauses should first identify in a precise manner the information that is the subject of the licensing agreement that should be kept secret. Secondly, the parties should regulate the content and scope of the secrecy obligation and in particular the possibility of disclosing the licensed information to third parties. Specifically, it should be established

2437 Stefan Maaßen and Tobias Wuttke 2011 (n 2404) Rdn 58.
2438 Stefan Maaßen and Tobias Wuttke 2011 (n 2404) Rdn 60.
2439 Stefan Maaßen and Tobias Wuttke 2011 (n 2404) Rdn 60.
2440 According to § 581(1) BGB and §§ 535 and 536a BGB; see further Stefan Maaßen and Tobias Wuttke 2011 (n 2404) Rdn 61.
2441 Kurt Bartenbach 2013 (n 2412) Rdn 2800; Michael Groß, *Der Lizenzvertrag* (Deutsche Fachverlag 2015) Rdn 98-99.
2442 Stefan Maaßen and Tobias Wuttke 2011 (n 2404) 64.

under which conditions the information can be imparted to third parties in order to allow for its commercial exploitation. These obligations should be equally demanding as those imposed upon the licensee, considering that once the information is generally known, the subject of the contract is lost.[2443] Similarly, it is also advisable that the licensing agreement regulates the possibility of taking copies (in electronic, paper or any other form) and the number of copies that can be made, which furthermore should always be labelled as confidential.[2444] Another aspect that should be included in the agreement is the duration of the confidentiality obligation, particularly after the termination of the contract, and the exceptions thereto. Crucially, the prohibition of disclosing information that constitutes a trade secret but does not meet all of the requirements of the definition of know-how established in the TTBER may not benefit from the block exemption and may be enforceable as a restraint of competition, pursuant to Article 101 TFEU.[2445] In addition, the block exemption will only apply for as long as the information is secret.[2446] Consequently, the exceptions to the obligation of confidentiality should exclude the information that was already known to the licensee at the time that the agreement was concluded; the information that was acquired in a lawful manner from third parties; the information that was developed independently by the licensee; and the information that it is generally known or readily accessible.[2447] Finally, it is advisable that the licensing agreement includes a clause that establishes that the licensed information can only be used for the purpose agreed in the contract,[2448] along with a penal clause in the event that the licensee breaches the secrecy obligation.[2449]

2443 Stefan Maaßen and Tobias Wuttke 2011 (n 2404) 70.
2444 *Pagenberg*/Beier (n 2433) Sample 3, Rdn 10.
2445 Hinrich Mummenthey, 'Vertraulichkeitsvereinbarungen' [1999] CR 651, 655.
2446 See Article 2(2) TTBER.
2447 Stefan Maaßen and Tobias Wuttke 2011 (n 2404) Rdn 73; the legal questions raised by the interplay between know-how licensing agreements and competition are manifold. However, providing a more detailed analysis falls outside the scope of the present analysis.
2448 Kurt Bartenbach 2013 (n 2412) Rdn 2237; Hinrich Mummenthey 1999 (n 2445) 656.
2449 For an overview of the scope and limits of penal clauses under German law see Stefan Maaßen and Tobias Wuttke 2011 (n 2404) Rdn 75-77.

c) After the termination of the contract

A comparative analysis reveals that the existence of an implied post-contractual secrecy obligation is a highly controversial issue. In Germany, the non-disclosure obligation continues after the termination of the contract on the basis of a post-contractual duty of loyalty ("*Treuepflicht*").[2450] However, in the interest of legal certainty, it is suggested that the licensing agreement should establish such a possibility in an express manner, in particular with regard to the duration of the non-disclosure obligation.[2451] Some German commentators have suggested that the duration of the post-contractual obligation should be between three and five years, even though a clause that provides that the obligation should remain in force for as long as the information remains secret should also be considered valid.[2452] Similarly, the German competition authority considers that the imposition of a fixed term (of 15 years) is questionable and that confidentiality obligations should rather extend for as long as the information remains secret, in accordance with Article 2(2) TTBER.[2453] From a practical perspective, it is extremely difficult to assess whether the licensee has disclosed or used the information concerned. Hence, due to the difficulty in monitoring the return of the documents and the use of the licensed information, it is recommended that the contract foresees the possibility of establishing penalty clauses in the event of early termination of the contract by the licensee.[2454]

In England, the courts have mostly addressed the existence of post-contractual secrecy obligations from the perspective of the information that the licensee is entitled to use after the termination of the contract, which has to be assessed pursuant to the specific terms of the agreement. A review of the main decisions on this topic reveals that once the contract is terminated, the right of the licensee to use the information also comes to an end.[2455] However, there are a number of decisions where such a principle

2450 Kurt Bartenbach 2013 (n 2412) Rdn 2871.
2451 Kurt Bartenbach 2013 (n 2412) Rdn 2871.
2452 Stefan Maaßen and Tobias Wuttke 2011 (n 2404) Rdn 72; Hinrich Mummenthey 1999 (n 2445) 656.
2453 *Pagenberg*/Beier (n 2433) Sample 1, Rdn 128, Rudolf Kraßer 1970 (n 831) 590; BKartA 1977 TB 94.
2454 Michael Groß, *Der Lizenzvertrag* (Deutsche Fachverlag 2015) Rdn 490; Kurt Bartenbach 2013 (n 2412) Rdn 2873.
2455 John Hull 2013 (n 934) 176-177 with further references.

is not followed.[2456] For instance, in *Regina Glass Fibre v Werner Schuller*, the Court of Appeal interpreted that the licensee was entitled to use the licensed confidential information, which concerned the manufacture of glass fibre, along with any improvements thereto, after the termination of the contract.[2457] Most commentators understand that this is an isolated decision and that the rationale for such an interpretation is that in the absence of such a use right, the viability of the licensee's business would have been dubious.[2458] Ultimately, the outcome of *Regina Glass Fibre v Werner Schuller* highlights that in the assessment of the possibility of using licensed secret information after the termination of the agreement, the English Courts will decide considering the terms of the licensing agreement.[2459]

In sum, from a comparative law perspective, it appears that there is no uniform interpretation regarding the admissibility of implied post-contractual secrecy obligations on the licensee and their duration. This issue will be addressed further in § 3 B) in the context of the study of the legal application of the Nordhaus Model.

II. R&D agreements

1. Object and legal nature

The EU legislature in the Preamble of the TSD underscored the importance of collaborative research and development activities in order to foster employment and innovation growth within the single market in the context of the TSD.[2460] Indeed, R&D agreements are central to allowing for the exchange of information between companies (both in the public and private sectors) particularly in innovative environments. A number of definitions have been proposed by lawmakers and commentators to conceptualise these types of agreements.[2461] For the purpose of the current analysis,

2456 Tanya Aplin and others 2012 (n 22) para 8.140 noting that "there is no general principle that governs this situation, rather it is a matter of interpretation of the licence agreement".
2457 *Regina Glass Fibre v Werner Schuller* [1972] RPC 229 (CA), 235.
2458 John Hull 2013 (n 934) 177.
2459 Tanya Aplin and others 2012 (n 22) paras 8.146 - 8.147.
2460 Recital 3 TSD.
2461 See Commission Regulation (EU) No 1217/2010 of 14 December 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European

the following working definition will be referenced: by virtue of R&D agreements two or more parties "agree to conduct research activities as a service (contract research) or in collaboration (research cooperation) to gain new scientific know-how or related IP".[2462] Under the first category, one party undertakes to provide specific research and development activities for the other. In contrast, in research cooperations, all of the parties share their knowledge and competences and agree on an R&D plan.[2463] As regards the object of the agreement, it can comprise anything that is developed, manufactured and distributed and that requires a production method or any device to that end, such as individual products, systems, software and any kind of procedures.[2464]

In general, R&D agreements can be divided into three stages.[2465] First, in the initial phase, the parties examine their pre-existing IP and trade secrets under strict confidentiality obligations and establish the objectives of the cooperation.[2466] In the second stage (the development phase), the parties collaborate to achieve the joint goals established in the initial phase. Finally, in the third stage (the utilization phase), the parties exploit the results of the research on an individual basis or jointly, in accordance with the terms of the R&D agreement.[2467]

In order to cooperate effectively, it is essential that the parties expressly specify the terms that govern the transfer of background IP (i.e. the pre-existing formal IPRs and trade secrets owned by each party).[2468] In contract research agreements, usually the background IP is licensed to the execut-

---

Union to certain categories of research and development agreements [2010] OJ L335/36 (R&DBER), Article 1(1)(a); Wolfgang Winzer, *Forschungs- und Entwicklungsverträge* (2nd edn, C.H. Beck 2011) Rdn 3-18.

2462 Melanie Graf and Herbert Zech, 'IP in Research and Development Agreements: object and legal qualification' 293, 293 in Duncan Matthews and Herbert Zech (eds), *Research Handbook on Intellectual Property and the Life Sciences* (Edward Elgar 2017).

2463 Claudia Milbradt and Marco Stief, 'Forschungs- und Entwicklungsvertrag'126, 126 in Marco Stief and Boris Bromm (eds), *Vertragshandbuch Pharma und Life Sciences* (C.H. Beck 2015).

2464 Wolfgang Winzer 2011 (n 2461) Rdn 1-3.

2465 Philipp Maume,'Know-how in Kooperationen (Entwicklung und Outsourcing)' Rdn 12 in Christoph Ann, Michael Loschelder and Marcus Grosch (eds), *Praxishandbuch Know-how-Schutz* (Carl Heymanns Verlag 2011).

2466 Melanie Graf and Herbert Zech 2017 (n 2462) 293.

2467 Philipp Maume 2011 (n 2465) Rdn 12.

2468 Christoph Bertsch,'Research Agreement' 38, 55-56 in Wolfgang Weitnauer and others (eds), *Life Sciences Agreements in Germany* (C.H. Beck 2014).

ing parties, while in research cooperation agreements, the parties establish a cross license for their respective background IP.[2469]

From the above considerations it follows that the crucial provisions of R&D agreements concern the regulation of the assignment and the licensing of the resulting R&D efforts, the so-called "foreground IP"[2470] or "project technology",[2471] which includes all of the formal IPR developed as a result of the implementation of the R&D plan, as well as trade secrets.[2472] The parties are free to regulate the assignment and licensing of the trade secrets created as a result of the execution of the R&D plan, provided that the competition law limitations imposed by the R&DBER and the applicable national law on employee creations are complied with.

As regards their legal nature, contract research agreements are usually entered into between a private entity and a public entity, such as universities and basic research centres. The latter party usually carries out the research activities according to the research plan designed by the financing party. Consequently, the agreement takes the form of a service contract or an agency contract depending on the certainty of the research outcome.[2473] Indeed, it has been suggested that the more certain the result is, the more likely it is to be qualified as a service contract. In contrast, in research cooperation agreements, the parties may create a partnership to exploit the foreground IP.[2474] Furthermore, in some instances, if the exploitation of the project technology requires the creation of new distribution or manufacturing structures, it may even be advisable to establish a joint venture.[2475]

2. Secrecy obligations

In the context of R&D agreements, secrecy plays a central role in ensuring the success of the common efforts of the parties. However, confidentiality obligations cannot be inferred from the nature of these types of contracts

2469 Claudia Milbradt and Marco Stief, 'Forschungs- und Entwicklungsvertrag' 126, 145 in Marco Stief and Boris Bromm (eds), *Vertragshandbuch Pharma und Life Sciences* (C.H. Beck 2015).
2470 Melanie Graf and Herbert Zech 2017 (n 2462) 293.
2471 Christoph Bertsch 2014 (n 2468) 55-56.
2472 Melanie Graf and Herbert Zech 2017 (n 2462) 293.
2473 Melanie Graf and Herbert Zech 2017 (n 2462) 293.
2474 In Germany it is governed by §§ 705-740 BGB.
2475 Philipp Maume 2011 (n 2465) Rdn 13-14.

and, therefore, it is of utmost importance that the content and scope of such obligations is expressly regulated in the body of the agreement, particularly after the termination of the contract.[2476] From a competition law perspective, it should be noted that the admissibility of confidentiality clauses is not expressly addressed in the R&DBER, even though they are generally considered valid if they are necessary for the implementation of the R&D agreements, to the extent that such clauses do not circumvent the safeguards established in Article 3 R&DBER.[2477] In addition, in order to ensure the adequacy of secrecy obligations in regard to the limitations imposed by competition law, most agreements include so-called "escape clauses", whereby it is established that the duty of secrecy terminates once the information becomes generally known.[2478] Indeed, if one of the parties to the agreement obtains the information lawfully from a third party, confidentiality obligations persist until the information becomes generally known among the relevant circles, because in such a case the common interest in keeping the information from other market participants also continues.[2479]

In pre-contractual negotiations, it is of utmost importance that confidentiality clauses are agreed upon before the R&D agreement is concluded, to ensure that the information disclosed during the negotiations is only used for the purposes of assessing the background IP and the viability of the R&D agreement. As argued in the context of licensing agreements, such a clause should include a prohibition on taking copies and the obligation to return the documents if the negotiations break off, or after the agreement is terminated.[2480]

Most importantly, the implementation of an R&D research plan can lead to the development of numerous trade secrets, such as data and labbooks, that are included in the foreground IP. In contract research agreements, usually the financing party acquires the resulting trade secrets, whereas in research collaboration agreements, this will depend on the national rules governing partnerships.[2481] Ultimately, in both instances, the

2476 Philipp Maume 2011 (n 2465) Rdn 5.
2477 Philipp Maume 2011 (n 2465) Rdn 53.
2478 Lorenz Kaiser, 'Vetragsmanagement' 257, 268 Alexander Wurzer and Lorenz Kaiser (eds), *Handbuch Internationaler Know-how-Schutz* (Bundesanzeiger Verlag 2011); *Pagenberg*/Beier (n 2433) Sample 8, Rdn 33; Wolfgang Winzer 2011 (n 2461) Rdn 199.
2479 Philipp Maume 2011 (n 2465) Rdn 55.
2480 Melanie Graf and Herbert Zech 2017 (n 2462) 295
2481 Melanie Graf and Herbert Zech 2017 (n 2462) 295.

national provisions regulating employee creation will have to be observed. Against this background, secrecy obligations concerning the foreground IP and the necessary background IP to exploit the results of the R&D Agreement are desirable for both parties during the term of the agreement and do not give rise to competition law concerns.[2482] However, in post-contractual scenarios, from a competition law perspective, they will only be admissible to the extent that they do not preclude disclosure to third parties during the exploitation of the foreground technology or have a negative impact on the ability of any of the parties to conduct further research.[2483]

In line with the above, several commentators submit that post-contractual secrecy obligations should be limited to a specific term to be able to benefit from the R&DBER. In effect, a duration of two to five years has been suggested by some authors,[2484] even though most commentators indicate that a general clause that provides that confidentiality obligations persist until the information becomes generally known should also be considered admissible, because the common interest of the parties in keeping the information undisclosed persists.[2485]

The foregoing analysis underscores that confidentiality clauses are key to safeguarding the exploitation of the trade secrets developed in the context of R&D agreements to allow for a return on joint innovative efforts. Notwithstanding this consideration, they are also subject to a number of limitations regarding their scope and duration to avoid restraints of competition law.

§ 2 *The limitations of secrecy*

The legal regime for the protection of trade secrets must strike a delicate balance between, on the one hand, the interest of the holder in concealing his valuable information from competitors, in order to recoup the cost of its development, and on the other, the access of third parties, which is necessary to foster competition and follow-on innovation. Much of this debate has been channelled through the discussion of whether trade secrets should be protected as a form of IPRs or under the unfair competition

2482 Christoph Bertsch 2014 (n 2468) 63-64.
2483 Philipp Maume 2011 (n 2465) Rdn 62.
2484 Wolfgang Winzer 2011 (n 2461) Rdn 197.
2485 *Pagenberg*/Beier (n 2433) Sample 8, Rdn 3; Wolfgang Winzer 2011 (n 2461) Rdn 197.

regime. As examined in the first chapter of this dissertation, many commentators and judicial decisions understand that in order to prevent a trade secret holder from being able to reap the fruits of his endeavours indefinitely, thus circumventing the trade-off imposed by the IPRs system, it is crucial that the property approach is abandoned in connection to trade secrets.[2486] However, this dissertation posits that trade secrets have an inherently hybrid nature and that even if formally they are regarded as a species of IPRs, this should not necessarily entail enhancing the level of protection, but rather allows for focusing on the limitations to the rights conferred.[2487]

In line with the latter argument, the TSD has adopted an open-ended approach to the legal nature issue and has expressly included a number of limitations in order to ensure the complementarity between trade secrets and formal IPRs and to safeguard the fundamental freedoms enshrined in the ChFREU. Consequently, Article 3 TSD refers to lawful means of acquiring, using and disclosing a trade secret and Article 5 TSD spells out a number of exceptions to the rights conferred on the trade secret holder. From a legislative technique perspective, the types of lawful conduct specified under Article 3 exclude liability ex ante by limiting the scope of application of the TSD, whereas the exceptions mentioned in Article 5 call upon national judicial authorities to conduct a balancing exercise to determine whether liability arises.

The present analysis looks into the most important statutory limitations that may lead to a disclosure of information in order to understand the optimal scope of secrecy. These are independent discovery (section A), reverse engineering (section B), and competition law (section C), and they are examined in the following sections.

A) Independent discovery and creation

The protection of trade secrets is premised on the fact that any competitor can, in an independent manner, come up with the same information as that covered by an already existing secret. Such a limitation is essential to prevent a trade secret holder from having an exclusive absolute right over the unrevealed information. This is also of paramount importance to en-

2486 Josef Drexl 2009 (n 369) 449; Gintare Surblyte 2011 (n 182) 90.

2487 Mark A. Lemley 2008 (n 15) 352; Lionel Bently 2013 (n 307) 91-92 and chapter 1 § 3 B).

sure the complementarity between the legal regime for the protection of trade secrets and the IPRs system in place, particularly regarding patents.[2488] Otherwise, if protection were accorded even in the case of independent discovery, the rationale underlying the protection of IPRs would be by-passed. Inventors would opt for informal means of protection, as this would allow them to benefit from their innovative endeavours (potentially) indefinitely without disclosing the information to competitors and without bearing the costs of the patent system.[2489] This would hinder the information function pursued by the publication of patent specifications. As a whole, if trade secret holders were protected against independent discovery or creation, the incentives to apply for patent protection would practically disappear. Consequently, the secrecy requirement compels inventors to choose the form of IP protection that better serves the objectives of society.[2490]

The importance of independent discovery has crystallised in Article 3(1)(a) TSD as a lawful form of acquiring a trade secret and mirrors a well-established practice among EU jurisdictions.[2491] It constitutes a defence against misappropriation claims, and should be construed as meaning that certain information that the plaintiff regards as his own trade secret has not been derived either directly or indirectly from knowledge gained in confidence from the holder or as a result of espionage activities.[2492] In sum, there cannot be a causal link between the information acquired from the trade secret holder and the information independently generated.[2493]

Against this background, it is noteworthy that innovations rarely occur in isolation.[2494] Areas of technology such as biotechnology and computer

2488 See chapter 1 § 3 A).

2489 *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 476 (1974) "a trade secret law, however, does not offer protection against discovery by fair and honest means, such as by independent invention, accidental disclosure, or by so-called reverse engineering".

2490 Mark A. Lemley 2008 (n 15) 339-341 arguing that the secrecy requirement compels inventors to choose the form of IP protection that better serves the objectives of society.

2491 For instance, in England see Law Commission 1981 (n 327) para 4.71-4.72; in Germany see Rudolf Kraßer 1977 (n 1327) 191.

2492 James Pooley 2002 (n 66) § 5.01[1] 5-3.

2493 Lionel Bently 2012 (n 114) para 3.23; see also *Seager Limited v Copydex Limited* [1967] 2 All ER 415 (CA).

2494 Vincent Chiappetta 1999 (n 24) 88 arguing that such a restriction on the trade secret holder's right to exclude third parties offers the right counterbalance to the incentives to invest in secrecy.

software are to a large extent cumulative. In those fields, inventions are mostly based on prior innovations.[2495] Thus, it is likely that a large percentage of the trade secrets end up being independently created by competitors working in the same industry.[2496] Indeed, "the original owner's risk is another's opportunity.[2497]

In view of this consideration, if a second inventor generates the information independently and applies for a patent covering such information, the grant process will inevitably lead to the publication of the application, and consequently the information will no longer be regarded as secret.[2498] In this particular scenario, under the EPC, the first inventor will not be able to destroy the novelty of the patent on the basis of its use, unless it is proved that the prior use made the information available to the public.[2499] In addition, if the patent is granted, except if the specific national regime provides for a "prior user's right", the trade secret holder will have to enter into a licensing agreement with the patentee in order to avoid the risk of patent infringement.[2500]

B) Reverse engineering

I. Conceptual introductory remarks

In the design of every trade secrets legal regime, the legislature should consider whether reverse engineering practices should be regarded as a lawful (or unlawful) form of acquiring undisclosed information and under which conditions, in order to strike the most appropriate balance between the conflicting interests of trade secret holders and their competitors, as well as the general public. Reverse engineering is central to the assessment of se-

2495 Suzanne Scotchmer 2004 (n 41) 125-126.

2496 Samson Vermont, 'Independent Invention as a Defense to Patent Infringement' [2006] 105 Michigan LR 475, 478-479.

2497 James Pooley 2002 (n 66) § 5.01[1] 5-3; this principle was famously acknowledged by the U.S. Supreme Court in *Kewanee Oil Co. v. Bicron Corp*., 416 U.S. 470, 490 (1974), where it was noted that an invention is likely to be discovered by competitors and that therefore, what was once secret may become common knowledge within a given industry.

2498 Lionel Bently 2012 (n 114) para 3.37.

2499 According to consistent case law from the Boards of Appeal of the EPO, such as G 1/95 [2006] OJ EPO 615.

2500 Lionel Bently 2012 (n 114) para 3.38; on the prior user's right defence, see chapter 1 § 3 A) I. 2. c).

crecy, because the need to undergo such a process to obtain a specific piece of information signals that it is secret and that therefore, a priori, it is eligible for protection. In addition, it is also essential to ensure the erosion of concealed information so that with time it eventually enters the public domain. However, the subsequent use and disclosure of information obtained from the said process and its interplay with other areas of law, in particular contract law, formal IPRs and unfair competition, remains controversial. Consequently, the inclusion of reverse engineering as a lawful form of obtaining information, subject to certain limitations, constitutes one of the milestones of the TSD.[2501]

It is the first time that such an overarching provision has been included within the acquis communautaire, thus bringing greater legal certainty to one of the pillars upon which the regime for the protection of trade secrets and its limitations is articulated. In effect, as surprising as it may seem, no right to reverse engineering (a so-called "reverse engineering defence") has been positively codified into patent law, even though it is a well-established practice among competitors across all industries.[2502] Before the adoption of the TSD, only Article 6 of the Software Directive allowed for "decompilation", a specific form of reverse engineering used in computer programming, but only for the purposes of achieving interoperability of independently created programs,[2503] along with Article 5(3) of the same directive, which enshrined the right to observe, study or test the functioning of a program in order to determine the underlying ideas and principles.[2504] Similarly, Article 5 of the Directive on the protection of topographies of semiconductor products provided that reproduction for private purposes or for the purposes of evaluation, analysis, research or teaching is permitted, but the sale of identical chips is proscribed.[2505]

2501 See Article 3(1)(b) TSD.

2502 Pamela Samuelson and Suzanne Scotchmer 2002 (n 226) 1582; but note that Article 27 of the Agreement on a Unified Patent Court [2013] OJ C–175/01 stipulates that the effects of a patent do not extend to (a) acts done privately and for non-commercial purposes, and (b) acts done for experimental purposes, which to a certain extent preserves the right to reverse engineer.

2503 See Article 6 Software Directive, which is examined below in chapter 6 § 2 B) IV. 2).

2504 Thomas Dreier, 'The Council Directive of 14 May 1991 on the Legal Protection of Computer Programs' [1991] 13 EIPR 319, 322.

2505 Council Directive 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products [1987] OJ L24/36.

From a conceptual perspective, the TSD defines reverse engineering as the "observation, study, disassembly or testing 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".[2506] A similar interpretation has been followed by the courts in the U.S., where the Supreme Court in *Kewanee Oil Co. v. Bicron Corp* defined it as "starting with the known product and working backward to divine the process which aided in its development or manufacture".[2507] Both explanations reveal that ultimately reverse engineering is an intellectual process that aims at "extracting know-how or knowledge from a human-made artifact".[2508] It can be applied in every field of technology, even though the amount of time, effort and costs required will largely depend on the specific characteristics of the product.[2509]

The reasons that may lead someone to engage in reverse engineering activities beyond the manufacturing of a replacement (or a clone) of a competitor's product are manifold. These include learning, repairing a product, providing related services, creating a compatible product or improving an existing one, to name some.[2510] Thus, from a dogmatic perspective, reverse engineering comprises the act of discovering the concealed information and, more extensively, the use of the resulting knowledge, even if it leads to the dissemination of information and the loss of secrecy.[2511] The root of the discrepancies with regard to the permissibility of reverse engineering in EU jurisdictions lies in the multiple ends to which it is applied. While innovative activities seem to provide legitimate grounds, creating replacements (or clones) has raised fairness concerns in some jurisdic-

2506 Recital 16 TSD: "Reverse engineering of a lawfully acquired product should be considered as a lawful means of acquiring information, except when otherwise contractually agreed. The freedom to enter into such contractual arrangements can, however, be limited by law".

2507 *Kewanee Oil Co. v. Bicron Co*., 416 U.S. 470, 476 (1974).

2508 Pamela Samuelson and Suzanne Scotchmer 2002 (n 226) 1577; in the same vein, Henning Harte-Bavendamm 1990 (n1502) 658 has defined it as "any process by which a product manufactured by a third party is analysed in detail with the aim of gaining actual knowledge of the underlying structure and function" (translation by the author).

2509 Pamela Samuelson and Suzanne Scotchmer 2002 (n 226) 1587.

2510 James Pooley 2002 (n 66) § 5.02[2] 17; see more generaly Ansgar Ohly 2009 (n 98) 537 distinguising between (i) "the innovative analyst"; (ii) "the copycat analyst" and (iii) "the right-owner analyst"; further reasons for engaging in reverse engineering practices are examined by Henning Harte-Bavendamm 1990 (n1502) 659-660.

2511 Tanya Aplin 2013 (n1600) 343.

tions.[2512] In the latter instance, drawing the boundaries between the simplest act of reverse engineering and copying activities appears to be a grey area.[2513] As a result, Member States' practices in this field have differed greatly.

In the light of the above considerations, the following section looks into the rationales underlying reverse engineering (section II). Next, the thesis goes on to examine the regulation of reverse engineering from a comparative law perspective (section III). First, it starts by analysing the legal framework of these practices (or its absence) in the TRIPs Agreement. Then, it compares the approach adopted with regard to this specific subject in the U.S., where it has long been accepted as a lawful way of acquiring a trade secret, with the one followed in England and Germany before the implementation of the TSD. Drawing on this comparative analysis, some interpretative considerations with respect to secrecy and the optimal scope of protection are presented in the light of Article 3(1)(b) TSD (section IV).

II. Rationales underlying reverse engineering

The deontological and utilitarian justifications for trade secrets protection examined in chapter 1 do not appear suitable to justify a limitation on the right to extract secret information from a marketed product in all instances.[2514] These inconsistencies can be best explained by two factors. First, the finished product has left the internal sphere of the company and therefore there is no need to deter an over-investment in self-help measures (the limit to the arms race doctrine) and protect the trial and error process inherent to its development (the privacy doctrine).[2515] In addition, a limitation on reverse engineering does not help to lower transaction costs because the contract that regulates the transaction has already been concluded before the item is placed on the market or delivered to the counterparty (incentives to disclose doctrine). In fact, agreeing on a limitation on reverse engineering seems most appropriate during pre-contractual negotia-

2512 Ansgar Ohly 2009 (n 98) 537; see in this regard the analysis in chapter 1 § 2 A).

2513 William Landes and Richard Posner 2003 (n 38) 370; Ansgar Ohly 2009 (n 98) 538 "it emerges that there is a wide range of possible motives for reverse engineering. In some cases reverse engineering is a necessary or at least useful step in the process of further innovation, in other cases it may only enable imitation".

2514 Chapter 1 § 2.

2515 Ansgar Ohly 2009 (n 98) 548.

tions, for instance in the exchange of prototypes before concluding the final agreement. Second, there is no universal commercial morality standard that allows for establishing whether devising secret information should be considered contrary to "honest commercial practices".[2516]

In contrast, the most intuitive justification for reverse engineering is that such a right stems from the ownership of the product in which the secret is embedded.[2517] In the words of Jacob J in *Mars UK Ltd v Teknowledge Ltd*: "what the owner has is the full right of ownership. With that goes an *entitlement to dismantle the machine* and tell anyone he pleases" (emphasis added).[2518]

From a legal perspective, reverse engineering is regarded as an essential element in maintaining the equilibrium with the IPRs system and particularly with respect to patent rights.[2519] Ultimately, it is also central to find a balanced solution to the secrecy-openness dichotomy: if secret innovations could not be subject to reverse engineering activities, the incentives to apply for patents and participate in the trade-off imposed by the patent system would disappear, along with the knowledge externalities derived from it.[2520] The fact that competitors may take apart a product to find out the underlying functioning and principles imposes a factual time limitation on the exclusivity conferred by secrecy. As a result, when informal means of protection are the preferred option to appropriate returns from innovation, it is likely that the duration of the exclusivity will be limited until the product is reverse engineered. To avoid such a risk, the innovator will apply for a patent in order to secure exclusivity for a finite period (the patent term).[2521]

From an economic perspective, Samuelson and Scotchmer, in their seminal article, "The Law and Economics of Reverse Engineering", conclude that a general prohibition on reverse engineering would amount to granting perpetual rights without publicising the knowledge of the invention. In this context, they suggest that in traditional manufacturing industries the *cost* and *time* necessary to reverse engineer a product allow innovators to recoup the investment made in its generation through the lead-time

2516 Ansgar Ohly 2009 (n 98) 548.
2517 Tanya Aplin 2013 (n 2511) 341-377.
2518 *Mars UK Ltd v Teknowledge Ltd* [2000] FSR 138 (Pat), 149.
2519 Ansgar Ohly 2009 (n 98) 546-547.
2520 Chapter 1 § 3 A); Pamela Samuelson and Suzanne Scotchmer 2002 (n 226) 1583.
2521 Pamela Samuelson and Suzanne Scotchmer 2002 (n 226) 1583-1584.

conferred by secrecy.[2522] Therefore, the innovator is sufficiently protected against the reverse engineer.[2523] Indeed, the investment of *time* and *cost* strikes the balance between the interests of the trade secret holder, and those of their competitors.[2524] In sum, reverse engineering practices foster market competition, decrease prices and enhance follow-on innovation.[2525] In the same vein, Landes, Posner and Friedman suggest that one of the most important aspects of reverse engineering practices is that they allow competitors to gain knowledge of inventions and creations, thus fostering follow-on innovation.[2526] Consequently, the cost of subsequent innovations is shared between the originator's initial research and development expenditure and the second-comer's investment in reverse engineering the product and developing the improvements.[2527]

Notwithstanding this consideration, reverse engineering is not always costly and time consuming.[2528] As examined in the context of perfumes, finding out the composition of a fragrance can be carried out fast and at a low price. It only requires that a small portion of a perfume is introduced into a gas-chromatograph. In a matter of minutes, the composition of the formula will be revealed to the skilled chemist, who may produce an identical product.[2529] In this regard, it has been argued that when reverse engi-

2522 Pamela Samuelson and Suzanne Scotchmer 2002 (n 226) 1590; a similar view is expressed by Jerome H. Reichman 1994 (n 102) 2521 where the author notes that "reverse engineering provides originators with an indispensable period of lead time in which to recoup their initial investment and to establish footholds in the market".

2523 Tanya Aplin 2013 (n 2511) 372.

2524 Pamela Samuelson and Suzanne Scotchmer 2002 (n 226) 1590; see comment to § 1 UTSA, which provides that: "Often, the nature of a product lends itself to being readily copied as soon as it is available on the market. On the other hand, if reverse engineering is lengthy and expensive, a person who discovers the trade secret through reverse engineering can have a trade secret in the information obtained from reverse engineering";; similarly Gintare Surblyte, 'Enhancing TRIPS: Trade Secrets and Reverse Engineering' 725, 742-743 in Hanns Ullrich and others (eds), *TRIPS plus 20 – From Trade Rules to Market Principles* (Springer 2016).

2525 Pamela Samuelson and Suzanne Scotchmer 2002 (n 226) 1590.

2526 David D. Friedman, William M. Landes and Richard A. Posner, 'Some Economics of Trade Secret Law' [1991] 5 JEP 61, 70 noting that "Reverse engineering will often generate knowledge about the product being reverse engineered that will make it possible to improve on it".

2527 Jerome H. Reichman 1994 (n 102) 2521.

2528 Jerome H. Reichman 1994 (n 102) 2527.

2529 See chapter 5 § 4 B) 1.

neering practices are "cheap" and "rapid" and allow for creating identical copies, they may ultimately have "*market destructive consequences*" as innovators will not be able to recoup the investment in their creation, which in turn may lead to a market failure.[2530] In such a context, and in line with the incentives to innovate doctrine previously analysed,[2531] an intervention by the legislator to prevent such market destroying practices by limiting reverse engineering may be justified.[2532] In fact, this is the justification underpinning the limitations on reverse engineering in the semiconductor industry and Article 6 of the Software Directive, which provides that acts of decompilation shall only be permissible to the extent that they are necessary to achieve interoperability.[2533]

Furthermore, this rationale has also crystallised in Recital 17 TSD, in which the EU legislature has acknowledged that in those industries where creators and innovators cannot resort to IPRs protection and reverse engineering can be carried out at a very low cost, these activities may amount to parasitic copying or slavish imitation that free ride on the reputation and innovation efforts of the trade secret holder. Against this background, the TSD indicates that this specific area may be the object of harmonisation in the near future.[2534] Yet, such an approach does not take into consideration the different practices among EU Member States regarding parasitic competition and that market economies operate under the principle of freedom to imitate.

With the above arguments in mind, the following section delves into the regulation of reverse engineering from a comparative law perspective. First, it starts by analysing the regulation of this conduct (or rather its absence) in the TRIPs Agreement. Next, it compares the regulatory approach adopted on this specific practice in the U.S., where it has long been accepted as a lawful form of acquiring a trade secret, with the ones followed in England and Germany before the implementation of the TSD. Finally,

---

2530 Pamela Samuelson and Suzanne Scotchmer 2002 (n 226) 1594.

2531 Chapter 1 § 2 B) I.

2532 Pamela Samuelson and Suzanne Scotchmer 2002 (n 226) identify five potential options to regulate reverse engineering: (i) restricting destructive means of reverse engineering; (ii) introducing a breadth requirement for products obtained through reverse engineering; (iii) establishing purpose-and necessity-based criteria for determining the legitimacy of reverse engineering; (iv) regulating the use of reverse engineering tools; and (v) restricting the publication of information discovered by a reverse engineer.

2533 Thomas Dreier 1991 (n 2504) 324.

2534 See Recital 17 TSD.

some policy considerations regarding the interplay between secrecy and reverse engineered products are presented in the light of Article 3(1)(b) TSD.

III. Comparative law analysis

1. TRIPs

Article 39 TRIPs is silent on the permissibility of reverse engineering.[2535] Even though the wording of this provision to a large extent mirrors § 1(2) UTSA, the drafters of TRIPs failed to establish a reverse engineering defence and define its contours vis-à-vis misappropriation.[2536] Therefore, the approaches adopted by the WTO Member States on this specific issue differ greatly, as no minimum standards of protection are laid down in this regard. In essence, the root of the discrepancies is whether information that can be acquired through reverse engineering is to be deemed readily ascertainable and whether such a practice may be considered contrary to honest commercial practices according to Article 10bis PC.[2537]

2535 Pamela Samuelson and Suzanne Scotchmer 2002 (n 226) 1577: "It neither requires nor sanctions a reverse engineering privilege".

2536 Jerome Reichman, 'How trade secrecy law generates a natural semicommons of innovative know-how' 185, 186 in Rochelle C. Dreyfuss and Katherine J. Strandburg (eds), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research* (Edward Elgar 2011); in this regard, François Dessemontet 2008 (n 601) 275 uses this argument to note that "The function of Article 39 TRIPs is to protect trade secrets, not to allow reverse engineering - which may be allowed under some legal orders, but might also have been outlawed by Article 39 TRIPs – since, as Professor Reichman points out, the definition of trade secrets embedded in Article 39 TRIPs closely follows Sec . 38 et seq. of the Restatement (Third) of Unfair Competition §39 (Am. Law Inst. 1995), but does not mention reverse engineering contrary to the restatement"; it is submitted here that this interpretation of the wording of Article 39 TRIPs is too simplistic.

2537 Markus Peter and Andreas Wiebe 2007 (n 304) Art. 39 Rdn 21.

2. U.S.

In the U.S., reverse engineering has long been accepted as a lawful form of acquiring a trade secret.[2538] This is statutorily recognised in the four most relevant sources of law that regulate trade secrets, namely the Restatement (First) of Torts,[2539] the Restatement (Third) of Unfair Competition,[2540] the UTSA[2541] and, more recently, the DTSA.[2542] Crucially, the UTSA subjects the lawfulness of reverse engineering to the acquisition of the product in which the trade secret is embodied by lawful and fair means, such as purchasing it on the open market.[2543] Accordingly, if the access to the item was gained in an illegal way, for instance, by resorting to trespass or theft, the acquisition of the information embodied therein will be considered illegal.[2544] For the same reason, information that is obtained through reverse engineering because of the breach of an explicit or implicit agreement is also deemed to have been obtained through improper means.[2545]

The policy justifications underlying the right to reverse engineer were examined by the U.S. Supreme Court in the famous case *Kewanee Oil Co. v. Bicron Corp*.[2546] This ruling concerned a classic case of trade secrets misappropriation in the chemical industry by departing employees who went on to work for a competing firm after the termination of their contracts. This decision is particularly notable because the Supreme Court clearly stated for the first time after the *Sears, Roebuck & Co. v. Stiffel Co*. judgement[2547] that there is no conflict between the objectives pursued by federal patent law and the goals of state trade secrecy law and that therefore the law of trade secrecy is not pre-empted by federal patent law.[2548]

In particular, the court argued that if a trade secret did not meet the patentability requirements, according trade secret protection would not have an adverse impact on the disclosure of information, one of the main

---

2538 *Kewanee Oil Co. v. Bicron Corp*., 416 U.S. 470, 476 (1974); similarly, *Sinclair v. Aquarius Electronics, Inc.,* 42 Cal. App.3d 216, 226 (Cal. Ct. App.1974).
2539 Restatement (First) of Torts § 757 (Am. Law Inst. 1939).
2540 Restatement (Third) of Unfair Competition §43 (Am. Law Inst. 1995) comment b.
2541 Comment to § 1 UTSA.
2542 18 U.S.C. § 1839 (6)(B).
2543 Comment to § 1 UTSA.
2544 Gale R. Peterson 1995 (n 1602) 451.
2545 Pamela Samuelson and Suzanne Scotchmer 2002 (n 226) 1582.
2546 *Kewanee Oil Co. v. Bicron Corp*., 416 U.S. 470 (1974).
2547 *Sears, Roebuck & Co. v. Stiffel Co.,* 376 U.S. 225 (1964).
2548 *Kewanee Oil Co. v. Bicron Corp*., 416 U.S. 470, 485 (1974).

objectives pursued by the patent system. Under such circumstances, the trade secret holder would not risk disseminating his valuable information (inter alia in a licensing context) if he could not protect it against unlawful acquisition, use and disclosure.[2549]

More notably, as regards trade secrets where there is doubt about their compliance with the standards of patentability, the Supreme Court held that the holder of information would most likely opt for patent protection because of its "superior benefits" compared to trade secrecy law. Along the same lines, it was argued that even if the invention were clearly patentable, no tension would arise as to the protection of undisclosed information. The Supreme Court strikingly held that the holder would always apply for a patent, given that trade secrets law provides weaker protection than patent law. In this context, the court enshrined reverse engineering (together with independent discovery) as a fair means of discovering a trade secret.[2550] Consequently, a specific state law prohibiting reverse engineering would be pre-empted by federal law.[2551] Yet, this reasoning seems to disregard the fact that, in many industries, secrecy is the preferred means of appropriating returns from innovation, particularly when the patent system is too costly considering the value of the invention, or it is envisaged that the returns obtained will be higher than if a patent were applied for.[2552]

This consideration was restated in another landmark case decided by the U.S. Supreme Court some years later: *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*[2553] This case dealt with the lawfulness of manufacturing fiber-

---

2549 *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 485 (1974).

2550 See *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 476 (1974) "trade secret law, however, does not offer protection against discovery by fair and honest means, such as by independent invention, accidental disclosure, or by so-called reverse engineering"; this was later emphasised in *Chicago Lock Co. v. Fanberg,* 676 F.2d 400 (9th Cir. 1982).

2551 *Chicago Lock Co. v. Fanberg,* 676 F.2d 400, 405 (9th Cir. 1982) noting that "such an implied obligation upon the lock owner (obligation not to reverse engineer) in this case would, in effect, convert the Company's trade secret into a state-conferred monopoly akin to the absolute protection that a federal patent affords. Such an extension of California trade secrets law would certainly be preempted by the federal scheme of patent regulation"; see also Ansgar Ohly 2009 (n 98) 539.

2552 As explored in chapter 1 § 3 A) I. 2. a); see in particular David D. Friedman, William M. Landes and Richard A. Posner, 'Some Economics of Trade Secret Law' [1991] 5 JEP 61, 63-64.

2553 *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141 (1989).

glass hulls through a direct moulding process, for which no patent had been applied, in order to produce imitations of the boat hulls produced by the plaintiff, Bonito Boats. The petitioner sought an injunction on the basis of a state law enacted in Florida, which prohibited the use of a direct melding process to duplicate the vessel hull made by a third party without the consent of the original manufacturer. The fact pattern reveals that this case falls between a reverse engineering case and a mere copying case.[2554]

In its legal reasoning, the Supreme Court started by noting that reverse engineering forms an essential part of innovation and that variations in the original product may in fact result in progress in the specific field.[2555] Furthermore, it argued that, "the competitive reality of reverse engineering may act as a spur to the inventor, creating incentives to develop inventions that meet the rigorous requirements of patentability".[2556] While highlighting the importance of reverse engineering for market competition, the court also emphasised the significance of imitation for innovation by stating that:

> From their inception, the federal patent laws have embodied a careful balance between the need to promote innovation and the recognition that imitation and refinement through imitation are both necessary to invention itself and the very lifeblood of a competitive economy.[2557]

As is apparent from the above, allowing for reverse engineering was deemed an essential element not only to spur innovative practices, but also to ensure complementarity with the patent system.[2558] In view of these arguments, the Supreme Court concluded that the Florida Statute was preempted by federal patent law.[2559]

2554 Ansgar Ohly 2009 (n 98) 537.

2555 *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141, 160 (1989); Pamela Samuelson and Suzanne Scotchmer 2002 (n 226) 1583.

2556 *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141, 160 (1989).

2557 *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141, 160 (1989).

2558 *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141, 142 (1989) noting that: "(…), the threat of reverse engineering of unpatented articles creates a significant spur to the achievement of the rigorous standards of patentability established by Congress. By substantially altering this competitive reality, the Florida statute and similar state laws may erect themselves as substantial competitors to the federal patent scheme".

2559 *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141, 168 (1989).

3. England before the implementation of the TSD

The reverse engineering exception in England has been underexplored both by case law and by legal commentators.[2560] So far, only one appellate decision has expressly recognised the freedom to reverse engineer, and only in a very succinct manner, without analysing the actual scope of this defence.[2561] However, the proposal to implement the TSD in the UK noted that such a principle has in fact been implemented by UK common law.[2562] Indeed, several rulings from lower courts have accepted it as the necessary corollary to the patent system.

The starting point of the analysis of the legal framework that governs reverse engineering in England draws from the principles spelt out in chapter 4 in the context of placing an item on the open market in which a trade secret is embodied.[2563] In a nutshell, when a product is marketed in a manner that discloses the commercial secret so that little or no intellectual skill is necessary to obtain it, such information loses its confidential nature and can be freely used by anyone.[2564] This is in line with the first of the five principles articulated by Aplin after reviewing the limited English case law that addresses the issue of reverse engineering.[2565]

The second principle suggested by the author considers that "*commercial secrets that may be ascertained by reverse engineering retain limited confidentiality*".[2566] This is particularly relevant when the trade secret embodied in a

---

2560 Tanya Aplin 2013 (n1600) 346.

2561 *Force India Formula One Team Ltd v 1 Malaysia Racing Team SDN BHD* [2013] EWCA civ 780 (CA), [72] commenting on the fact pattern of *Saltman Engineering v Campell Engineering* [1948] 65 RPC 203 (CA): "In that case, the plaintiffs instructed the defendant to make tools for the manufacture of leather punches in accordance with drawings which the plaintiffs provided to the defendant for this purpose. The defendant used the drawings to make tools, and the tools to make leather punches, on their own account. The finished product (i.e. the leather punches) were readily available to buy in the shops; and the defendants could have bought one and reverse engineered it".

2562 See United Kingdom Intellectual Property Office, 'Consultation on draft regulations concerning trade secrets' (18 February 2018) 28 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/682184/Consultation_Trade_Secrets_Directive.pdf> accessed 15 September 2018.

2563 Chapter 4 § 4 C) II. 3.b)

2564 See for instance *Force India Formula One Team Limited v 1 Malaysia Racing Team SDN BHD* [2012] EWHC 616 (Pat), [222].

2565 The principles proposed by Tanya Aplin 2013 (n 2511) 346-363 will guide the present discussion.

2566 Tanya Aplin 2013 (n 2511) 349-355.

marketed product is not readily apparent, but it is possible to acquire it through reverse engineering i.e. with the investment of time, labour and particularly cost and intellectual skill. Under such circumstances, the Chancery division in *Terrapin Ltd v. Builders' Supply Co (Hayes) Ltd*[2567] suggested that the mere marketing of the good does not necessarily imply that the commercial secrets embodied therein lose their confidential nature. Instead, this should be determined on the basis of (i) whether the good was reverse engineered, and (ii) the use of the information ascertained via reverse engineering, in line with the arguments already suggested.[2568]

In *Terrapin Ltd v. Builder's Supply Co (Hayes) Ltd*, the plaintiff, a producer of prefabricated portable buildings, had concluded a manufacturing agreement with the defendant. To that end, drawings, technical information and know-how were conveyed in confidence to the respondent. Several months after the termination of the contract, the defendant started to sell portable buildings with essentially the same features as the buildings produced during the manufacturing agreements. In the ratio decidendi, the Court of Chancery held that: "springboard it remains even when all the features have been published or can be ascertained by actual inspection by any member of the public". According to Aplin, this should be understood as meaning that the "information obtained via reverse engineering retains limited confidentiality".[2569] In other words, the information is not deprived of its confidential nature because the amount of time and intellectual skill necessary to obtain it prevents it from being generally known or easily accessible to the relevant circles and the general public.[2570] In addition, associated secrets that cannot be obtained through reverse engineering also remain concealed.[2571] In *Terrapin Ltd v Builders' Supply Co (Hayes) Ltd* the information was considered confidential because the defendants had by-passed the trial and error process inherent to reverse engineering practices and instead had developed the improved model on the basis of information conveyed in confidence.

In line with the second principle, the third principle states that "*commercial secrets that have been obtained via reverse engineering do not necessary lose their confidentiality*".[2572] The assessment of whether reverse engineering de-

2567 *Terrapin Ltd v Builders' Supply Co (Hayes) Ltd* [1962] RPC 375 (Ch).
2568 Chapter 4 § 4 C) II. 3. b).
2569 Tanya Aplin 2013 (n 2511) 352.
2570 Chapter 4 § 4 C) II. 3. b); Jacob J holds the opposite view in in *Mars UK Ltd v Teknowledge Ltd* [2000] FSR 138 (Pat), 149.
2571 Tanya Aplin 2013 (n 2511) 354.
2572 Tanya Aplin 2013 (n 2511) 355-356.

stroys secrecy will depend on two factors, namely (i) whether the information acquired through reverse engineering has been further disseminated, and (ii) the number of people that have succeeded in reverse engineering the secret. If the number is substantial, the information will be deemed to fall into the public domain,[2573] consistent with the doctrine of relevant circles examined above.[2574] Indeed, with time, most trade secrets erode because more competitors are able to reverse engineer them. Consequently, the secret progressively loses its commercial value (it no longer provides a competitive advantage) and also its concealed nature.

The fourth principle provides that "*a person seeking to reverse engineer will not usually come under an obligation of confidence*".[2575] Several cases have drawn attention to this point, but it was most notably elaborated by Jacob J in *Mars UK v Teknowledge Ltd*,[2576] the leading authority to date on reverse engineering.[2577]

Mars UK Ltd was a British manufacturer of coin receiving and changing mechanisms. Their machines incorporated discriminators whose function was to control the authenticity and value of the coins introduced into the machine. Modern discriminators operate through sensors that take a series of electrical measurements. The disputed discriminator was known as the "Cashflow" and its main feature, as opposed to the existing models, was that it could be reprogrammed for new coin data. The recalibration function of the Cashflow was protected through several mechanisms, and in particular, the encryption of information. Furthermore, the re-programmation function was outsourced by Mars to several independent authorised companies. The defendant succeeded in reverse engineering the Cashflow discriminator and consequently Mars launched proceedings for copyright and database rights infringement, as well as breach of confidence.

2573 By way of illustration Lionel Bently 2012 (n 114) para 3.44 suggests that: "it is conceivable that someone (Z) who reverse engineered "E" and thereby worked out how to make it may simply take advantage of that knowledge himself. If that occurred, X could not object to Z's activities, but X might retain an enforceable secret itself. This is because confidentiality only requires that information remain relatively secret. Thus, X might continue to be able to enforce of confidentiality against those to whom he disclosed the information about the process of making "E" in confidence (such as its employees); " Jacob J holds the opposite view in *Mars UK Ltd v Teknowledge Ltd* [2000] FSR 138 (Pat), 149.

2574 See chapter 4 § 4 D) II. and IV.

2575 Tanya Aplin 2013(n 2511) 356-362.

2576 *Mars UK Ltd v Teknowledge Ltd* [2000] FSR 138 (Pat).

2577 Tanya Aplin and others 2012 (n 22) para 671.

With respect to the breach of confidence claim, in the legal arguments Jacob J started by noting that "encrypted information is to be regarded in law as a trade secret and treated as such".[2578] Next, he went on to analyse whether the three requirements set forth in *Coco v A.N. Clark* had been met. With regard to the first requirement, whether the information possessed the "necessary quality of confidence", it was held that the owner of encrypted information was entitled to take apart the machine by virtue of its ownership right. In this particular aspect, the decision seemed to indicate that whenever a piece of information has been acquired through reverse engineering it automatically loses its quality of confidence.[2579] This proposition has been the object of vehement criticism by some commentators, because the information had only been reverse engineered by the defendant and had not been circulated further. By holding that the information was no longer secret, Jacob J was equating the confidence requirement with the objective novelty test under patent law, and disregarding the factual nature of such a condition.[2580]

With respect to the second and third liability requirements, by virtue of which the information must have been communicated in circumstances importing an obligation of confidence and subsequently misused, Jacob J held that the mere fact of receiving encrypted information does not give rise to a duty of confidence and that "there is nothing surreptitious in taking a thing apart to find out how it is made". .[2581] Thus, it was concluded that the information incorporated in the machine was obviously not confidential and that finding out information from a product purchased on the

2578 *Mars UK Ltd v Teknowledge Ltd* [2000] FSR 138 (Pat), 150, [29]; later on he further notes that "mere difficulty in doing the job is not enough - there must be some element of deliberate difficulty put in the way. Mars make no bones about the far-reaching nature of their case. In the words of their closing submissions "the issue is whether it is possible to impose confidentiality upon someone who receives information by purchasing an article in the open market".

2579 *Mars UK Ltd v Teknowledge Ltd* [2000] FSR 138 (Pat), 149 "(…) starting with the first requirement, does the encrypted information in the Cashflow, have the "necessary quality of confidence"? I think the answer is clearly "no". The Cashflow is on the market. Anyone can buy it. And anyone with the skills to de-encrypt has access to the information. The fact that only a few have those skills is, as it seems to me, neither here nor there. Anyone can acquire the skills and anyway, a buyer is free to go to a man who has them. Mars suggest that the owner, although he owns the machine, does not own the information within it. That is too glib".

2580 Tanya Aplin 2013 (n 2511) 355.

2581 *Mars UK Ltd v Teknowledge Ltd* [2000] FSR 138 (Pat), 149 [33].

open market was part of the fair game for competitors.[2582] In sum, the legal reasoning in *Mars v. Teknowledge* underscores that under the breach of confidence action the general principle is the freedom to reverse engineer, which can be limited by contractual provisions and IPRs, but not based on an implied equitable duty of confidence. In particular, the inclusion of technical measures in the product to prevent the acquisition of the information does not give rise to a duty of confidence.[2583]

Finally, the fifth principle suggested by Aplin states that, "*it is no defence to a breach of confidence claim to say that a product could have been –or has been– reverse engineered*.[2584] In essence, this should be construed as meaning that even if it had been possible to reverse engineer the disputed product, if the defendants did not do so and instead used confidential information they would still be liable for a breach of confidence. This was clarified, among others, in *Saltman*[2585] and *Force India*,[2586] where the deciding courts held that by-passing independent research and using confidential information instead should amount to a breach of confidence. In essence, this principle purports that whoever wants to benefit from the reverse engineering defence must show that he has gone through the trial and error process necessary to devise the secret information.

The previous analysis reveals that despite the absence of an express reverse engineering defence, in England courts mostly understand that the acquisition of a trade secret through reverse engineering constitutes a lawful form of acquiring secret information and therefore it cannot give rise to liability under the breach of confidence action provided that the item is acquired on the open market and unless a limitation on these types of practices is agreed upon contractually.

2582 Lionel Bently 2012 (n 114) para 3.42.

2583 Tanya Aplin 2013(n 2511) 357.

2584 Tanya Aplin 2013 (n 2511) 362-363.

2585 *Saltman Engineering v Campell Engineering* [1948] 65 RPC 203 (CA) 215: "What the Defendants did in this case was to dispense in certain material respects with the necessity of going through the process which had been gone through in compiling these drawing, and thereby to save themselves a great deal of labour and calculation and careful draughtsmanship. (…) They have saved themselves that trouble by obtaining the necessary information either from the original drawings or from the tools made in accordance with them. That, in my opinion, was a breach of confidence".

2586 *Force India Formula One Team Limited v 1 Malaysia Racing Team SDN BHD* [2012] EWHC 616 (Pat), [22].

4. Germany before the implementation of the TSD

In Germany, reverse engineering is predominantly regarded as unfair, as opposed to in the U.S. and England, where it is considered as a lawful form of acquiring a trade secret. Under German law, such practices may be captured under paragraph 1 of § 17(2) UWG and, in particular, by litera (a), which proscribes the acquisition or securement of a trade secret through any technical means that enable it, and by litera (b), which renders unlawful the physical reproduction of the secret information.[2587] The general test of fairness that governs the UWG is not applicable to §§ 17 and 18 UWG and, therefore, it is irrelevant whether the trade secret is effectively used or disclosed because the mere acquisition or securement of the information triggers both criminal and civil liability.[2588] Accordingly, a person that engages in reverse engineering practices will be held liable unless a specific ground of justification exists, such as consent, a statutory duty or contractual claim to disclose, or a state of emergency.[2589]

The cornerstone of the reverse engineering doctrine followed by the German courts was first developed in 1935 by the Supreme Court of the German Reich ("*Reichsgericht*") in the *Stiefeleisenpresse* decision.[2590] In essence, the facts of the case are as follows: the plaintiff was the sole producer of a complex machine used to manufacture metal fittings ("*Spiefeleisen*"), which were necessary in order to strengthen the soles of boots and shoes. A Polish manufacturer of metal fittings ("*Stiefeleisen*"), which in the past had purchased one of the plaintiff's machines, sought to acquire a second unit after some time, but at a lower price. In view of their refusal to negotiate the price, the Polish company contacted the defendant, an undertaking which also produced metal fittings machines ("*Stiefeleisenpresse*"), but using a different technology. Following the Polish company's

2587 Andreas Wiebe, 'Reverse Engineering und Geheimnisschutz von Computerprogrammen' [1992] CR 134, 135; Gintare Surblyte, 'Enhancing TRIPS: Trade Secrets and Reverse Engineering' 725, 750-753 in Hanns Ullrich and others (eds), *TRIPS plus 20 – From Trade Rules to Market Principles* (Springer 2016); Henning Harte-Bavendamm 1990 (n1502) 662 noting that in the context of reverse engineering the acquisition of the physical support in which a trade secret is embodied may trigger liability according to litera (c) of paragraph 1 of § 17(2) UWG as a preparatory means of acquiring the secret prior to conducting reverse engineering.

2588 Henning Harte-Bavendamm 1990 (n1502) 662.

2589 Ansgar Ohly 2009 (n 98) 541.

2590 RGZ 1935 149, 329 – *Stiefeleisenpresse*.

request, the defendant agreed to manufacture and deliver a machine that fitted the tools used for the machine that they already owned, which had been purchased from the plaintiff some time before. Accordingly, one of the defendant's experts disassembled the machine, took measurements and made drawings of the different parts and finally copied the tools used to repair it. As a result, the defendant ended up supplying a replica of the plaintiff's machine to the Polish company. When the plaintiff learnt about this fact he brought an action for a violation of § 17(2) of the UWG, under the doctrine of slavish imitation, despite the fact that a patent covering the invention had expired thirty years before. Both claims were upheld by the Supreme Court of the German Reich. With respect to the trade secrets claim, in the legal reasoning the court first assessed whether the requirements for protection were met.[2591] Secondly, the ruling deemed that in order to dissemble the *Stiefeleisenpresse* machine, substantial effort (in the sense of great difficulty and cost) was required to devise the secret and, in view of that, the defendant's conduct was unfair and violated § 17(2) UWG. In particular, the court specifically noted that tearing apart the machine was not the normal way of acquiring information.[2592]

The "great difficulty and cost" ("*große Schwierigkeit und Opfer*") benchmark has been adopted in subsequent judicial decisions as the prevailing criteria to assess whether the acquisition of confidential information through reverse engineering is lawful.[2593] If substantial effort is required in order to devise secret information, its acquisition will be deemed an act of unfair competition. However, this has not been without criticism. Some commentators consider that this doctrine is inherently vague and leads to much legal uncertainty, because it poses the additional question of elucidating from a quantitative perspective when the degree of difficulty and cost is such that triggers liability.[2594] Most notably, it has been questioned because by protecting the investment made, the trade secret holder is conferred a type of exclusivity akin to that granted by formal IPRs, thereby disregarding the salutary effects of reverse engineering on price competition

2591 Chapter 4 § 2 A).

2592 Andreas Wiebe, 'Reverse Engineering und Geheimnisschutz von Computerprogrammen' [1992] CR 134, 135.

2593 Ansgar Ohly 2009 (n 98) 542 noting that most subsequent cases have followed this decision and only a minority have deviated from it, based on the argument that the information seems to be available without substantial effort, in this regard see for instance OLG Hamburg GRUR-RR 2001, 137, 139 – *Nachbau einer technischen Vorrichtung nach Ablauf des Patentschutzes.*

2594 Florian Schweyer 2012 (n 99) 466.

and follow-on innovation.[2595] In addition, such an approach overlooks the relative nature of secrecy, which is necessary to reconcile the interests protected, on the one hand, by the law of trade secrets and, on the other, under formal IPRs and patents in particular. Devising the internal structure or composition of a product purchased on the open market is a well-established practice in most industries and is considered an important part of the competitive process. Thus it should not be considered an unlawful form of acquiring information. In this regard, Ohly states that not enough attention has been paid to the policy arguments that speak in favour of the allowance of reverse engineering and against the establishment of such a high threshold for trade secrets protection.[2596]

Notwithstanding this restrictive interpretation, with the implementation of the TSD the reverse engineering doctrine will have to be reconsidered in Germany, as is examined in the following section.

IV. Reverse engineering under the TSD

1) Scope of the reverse engineering pursuant to Article 3(1)(b) TSD

One of the critical aspects of the TSD is the inclusion of a general reverse engineering defence (Article 3(1)(b) TSD), which constitutes a maximum standard of protection.[2597] The provision reads as follows:

> The observation, study, disassembly or testing 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 legal valid duty to limit the acquisition of the trade secret.

Further clarification is provided in Recital 16, which states:

> (…) Reverse engineering of a lawfully acquired product should be considered as a lawful means of acquiring information, except when otherwise contractually agreed. The freedom to enter into such contractual arrangements can, however, be limited by law.

2595 Ansgar Ohly 2009 (n 98) 542 noting that "The court point out that thedefendant by taking apart a machine'which was not meant to be taken aprt,' had strengthened its own competitive position at the plaintiff's cost. In other words: the defendant had reaped where it had not sown".

2596 Ansgar Ohly 2009 (n 98) 543.

2597 Article 1 TSD.

Pursuant to Article 3(1)(b) TSD, reverse engineering will be deemed a lawful form of acquiring a trade secret as long as either of the two following alternative pre-conditions is met: (i) the product or object in which the trade secret is embodied has been made available to the public, or (ii) the product or object in which the trade secret is embodied is possessed lawfully by someone under no legal obligation to limit the acquisition of the information. In this regard, the relevant provision also foresees the possibility of limiting by contract reverse engineering practices, which allows the holder to keep the information secret for a longer period and thereby prolong the exclusivity conferred by secrecy. Yet, pursuant to the wording of Recital 16, such a possibility may be excluded by law.[2598]

The first condition stipulates that the product or object must have been *made available to the public*. By analogy with patent law, a product will be regarded as available if it can be accessed or acquired on the open market free from any legal duty of confidence or non-disclosure.[2599] This includes the production, offering, marketing or otherwise exploiting of the product or object concerned.[2600]

The second condition provides that the product has to be *lawfully* possessed by someone "who is free from any legal valid duty to limit the acquisition of the trade secret". This wording seems more problematic insofar as it raises a number of interpretative questions. First, uncertainty arises regarding how to assess when a good is possessed *lawfully*. From a systematic perspective, it seems that lawfulness should be evaluated by reference to the types of conduct listed in Article 4(2)(a) TSD, which spells out a number of examples of when the acquisition of trade secrets is to be considered contrary to honest commercial practices, such as the unauthorised appropriation of objects, materials, substances or electronic files. However, the latter provision refers to the acquisition of the information as such and not the item in which it is embodied, which may include a broader spectrum of behaviours. The protection of possession has not been harmonised

2598 Gintare Surblyte, 'Enhancing TRIPS: Trade Secrets and Reverse Engineering' 725, 742 in Hanns Ullrich and others (eds), *TRIPS plus 20 – From Trade Rules to Market Principles* (Springer 2016).

2599 Guidelines for Examination in the EPO, Part G, Patentability, Chapter IV. Section 7.2.1: "Subject-matter should be regarded as made available to the public by use or in any other way if, at the relevant date, it was possible for members of the public to gain knowledge of the subject-matter and there was *no bar of confidentiality restricting the use or dissemination of such knowledge*"(citation omitted, emphasis added).

2600 Guidelines for examination in the EPO, Part G, Chapter IV. Section 7.1.

across the EU and therefore the relevant national civil provisions in each jurisdiction should govern the assessment of lawfulness. Consequently, in line with the escape clause included in Article 4(2)(b) TSD, national courts may also consider unfair other forms of obtaining the products subject to a reverse engineering proceedings, such as theft, misrepresentation, bribery or espionage, despite the fact that these were excluded from the scope of the TSD due to their criminal law nature. Similarly, in those borderline cases where it may be unclear whether the item has been acquired in an unlawful manner, for instance, if the seller concealed its identity at the time of purchase, national rules apply.[2601]

Second, an additional interpretative question refers to whether the *acquirer of the information* refers only to the purchaser (the owner) or also to those that have hired or licensed the object. From the wording of the provision, it seems that if the product is lawfully under the sphere of control of the acquirer (factual possession), either because it has been sold, licensed or hired, it should be possible to conduct reverse engineering activities, even if this leads to the revelation of the secret and the production of a competing product, unless agreed otherwise contractually or proscribed by law.[2602]

Furthermore, Article 3(1)(b) TSD provides that the acquirer must be "free from any *legal valid duty* to limit the acquisition of the trade secret". Pursuant to Recital 16, the expression "legal valid duty" refers to the possibility of limiting reverse engineering practices by contract.[2603] However, the inclusion of contractual clauses appears problematic because it upsets the equilibrium between the trade secrets legal regime and formal IPRs, particularly in the case of software licences. This is analysed in the following section.

2601 Tanya Aplin 2013 (n 2511) 375.

2602 Tanya Aplin 2013 (n 2511) 372.

2603 Article 3(1)(b) TSD refers to "any legal valid duty to limit the acquisition of the trade secret", whereas Recital 16 TSD refers to contractual provisions. Hence, the term "legal valid duty" is understood to refer to contractual provisions. However, one could also argue that it includes statutory limitations that restrict the possibility of conducting reverse engineering practices, such as the prohibition of decompilation enshrined in Article 6 of the Software Directive. In addition, by virtue of the principle of primacy law of EU law, it may be debatable whether national statutory limitations on reverse engineering should be effective.

2) Contractual limitations on the possibility of reverse engineering and in particular the interplay with the Software Directive

Contractual relationships between private parties are governed by the freedom of contract principle, which may nevertheless stand as an obstacle to the safeguards established by law. This problem is particularly acute in the context of trade secrets because if the parties agree not to reverse engineer a licensed product, the balance struck by the EU legislator may tip in favour of the trade secret holder.[2604] To be sure, contractual clauses proscribing reverse engineering enhance secrecy because they defer the entrance of information into the public domain. An illustrative example of this is mass-distribution software licensing agreements that include clauses preventing the licensee from reverse engineering the licensed program. This type of provisions raises concerns not only from a trade secrets perspective, but also in terms of a conflict with the safeguards enshrined in the Software Directive. Before turning to them, it is important to introduce a number of considerations regarding the protection of software and its interface with the law of trade secrets.

Both the object code and the source code of a computer program can be protected under copyright rules.[2605] However, in order to capture the market, frequently software manufacturers resort to trade secrets protection for the source code, which is in human-readable programming language, and to copyright protection for the object code, which needs to undergo a process of decompilation in order to be translated into source code. Thereby, competitors are prevented from copying the program or creating compatible or even competing programs because the object code prevents access to the principles and ideas and its translation into source code amounts to an act of reproduction, which is subject to the right holder's authorisation under Article 4 of the Software Directive.[2606]

In view of such a broad scope of protection, the EU legislature included a number of safeguards in the Software Directive that allow for reverse engineering a computer program, subject to several conditions, in order to foster competition and follow-on innovation within the software market.[2607] First, Article 5(3) of the Software Directive provides that the li-

2604 Mark A. Lemley 1995 (n 1617) 1246.
2605 See chapter 1 § 3 A) II.
2606 Thomas Dreier 1991 (n 2504) 323-324.
2607 See Commision, 'Proposal for a Council Directive on the legal protection of computer programs' COM (88) 816 final, paras 3.10-3.15; Robert J. Hart, 'In-

censee is entitled without prior authorisation from the licensor "to observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program if he does so while performing any of the acts of loading, displaying, running, transmitting or storing the program which he is entitled to do".[2608] This purpose-based safeguard allows for the analysis of a computer program to devise the underlying ideas and principles, but only in the performance of the acts inherent to its use.[2609] Hence, such practices fall within the definition of reverse engineering laid down in Article 3(1)(b) TSD, which also includes the observance, testing and analysis of products.

Second, Article 6 of the Software Directive lays down that the restricted acts established in Articles 4(1)(a) and 4(1)(b) of the Software Directive do not require prior authorisation if they are necessary to achieve the interoperability of an independently created computer program with other programs, provided that: (i) they are carried out by the licensee or any third party entitled to use a copy of the program; (ii) the information has not been previously readily available to them; and (iii) the acts of decompilation are limited to those parts that are indispensable to achieve interoperability.[2610] Therefore, Article 6 permits a specific form of reverse engineering known as decompilation, but only for the purposes of achieving interoperability (purpose-based norm).[2611]

---

teroperability information and the Microsoft decision' [2006] 28 EIPR 361, 363.

2608 Article 5(3) Software Directive.

2609 Gintare Surblyte, 'Enhancing TRIPS: Trade Secrets and Reverse Engineering' 725, 743 in Hanns Ullrich and others (eds), *TRIPS plus 20 – From Trade Rules to Market Principles* (Springer 2016).

2610 Thomas Dreier 1991 (n 2504) 324; furthermore, pursuant to Article 4 the use of information acquired through decompilation activities is also restricted to (i) any uses other than achieving interoperability; (ii) sharing it with others except for the purposes of achieving interoperability; and (iii) for the creation of a computer program substantially similar in its expression; on the importance of interoperability for innovation see Urs Gasser and John Palfrey, 'Breaking Down Digital Barriers: How and When Interoperability Leads to Innovation, plus three companion case studies on DRM, Digital Identity, and Web Services' (2007) Berkman Center Publications Series <http://nrs.harvard.edu/urn-3:HUL.InstRepos:2710237> accessed 15 September 2018.

2611 Julie E. Cohen, 'Reverse Engineering and the Rise of Electronic Vigilantism: Intellectual Property Implications of "Lock-Out" Programs' [1995] 68 Southern California LR 1091, 1094 defines decompilation as a specific form of reverse engineering that "parses the binary object code in which computer programs are distributed into higher-level, human-readable commands".

As regards the interplay between the two provisions, a systematic analysis reveals that the acts of decompilation (Article 6 Software Directive) constitute a specific form of reverse engineering and that therefore they do not fall within the scope of the acts of analysis laid down in Article 5(3) of the Software Directive. Consequently, if a party performs an act of decompilation that does not meet the statutory requirements set out in Article 6 (such as achieving interoperability), it will not be possible to claim that the conduct falls under the exception set out in Article 5(3) of the Software Directive.[2612]

Most importantly, in order to ensure that parties do not circumvent these exceptions by means of a contract, the second paragraph of Article 8 of the Software Directive stipulates that contractual provisions that contravene the safeguard established in Article 5(3) and Article 6 will be null and void. At first glance, the application of this principle appears rather straightforward. However, upon closer examination, a number of questions arise regarding the actual scope of such a prohibition and its intersection with the law of trade secrets.

The correlation between the exception established in Article 5(3) and Article 8 of the Software Directive was examined by CJEU in the highly contested decision, *SAS Institute Inc. v World Programming Ltd*.[2613] Among other questions, the CJEU was asked whether, pursuant to Article 5(3) of the Software Directive, the licensee of a computer program is entitled to observe, study or test the functioning of that program in order to determine the underlying ideas and principles with a purpose that goes *beyond* the framework established by the licence. According to the decision, the terms of the disputed licence provided that the defendant, World Programming Ltd, was only allowed to carry out acts for non-commercial purposes, but in fact had performed the said acts for purposes that fell outside the scope of the licence.[2614] In the judgement the court came to two apparently conflicting conclusions. First, it held that the software holder could not ban a licensee from determining the ideas and principles underlying the program provided that: (i) the licensee had carried out *acts that the licence had permitted him to perform*; (ii) the said acts were necessary to conduct loading and running acts to use the program; and, (iii) the licensee had not

2612 Ansgar Ohly 2009 (n 98) 545; Thomas Dreier 1991 (n 2504) 323.
2613 Case C–406/10 *SAS Institute Inc. v World Programming Ltd* (CJEU, 2 May 2012).
2614 Case C–406/10 *SAS Institute Inc. v World Programming Ltd* (CJEU, 2 May 2012), para 47.

infringed the rights of the software holder.[2615] This general statement was later qualified by the CJEU in the same decision, where it was noted that "*copyright* in a computer program *cannot be infringed* where, as in the present case, the lawful acquirer of the licence did *not have access to the source code of the computer program* to which that licence relates, but merely studied, observed and tested that program in order to reproduce its functionality in a second program". (emphasis added).[2616] Hence, the first statement indicates that acts of study are lawful as long as they do not exceed the terms of licence, whereas the second statement suggests that the discovery of the ideas and principles of a program should be deemed lawful because there is no copyright infringement if the lawful acquirer did not access the source code, regardless of the purpose indicated in the terms of the licence.

The ambiguity of this conclusion has been highlighted by several commentators[2617] and also by the referring judge,[2618] who interpreted the acts "permitted by the licence" as "the acts of loading, displaying, running, transmitting or storing" the program.[2619] Consequently, the defendant was still entitled to invoke the protection conferred by Article 5(3) of the Software Directive to extract the underlying principles and ideas through the said acts, irrespective of whether or not these were for a licensed purpose. The interpretation followed by the English Court of Appeal seems to be the most pertinent one, particularly in the light of the confusing reasoning followed by the CJEU in the decision. It prevents the software holder from availing himself of rights that were expressly excluded from the scope of application by the EU legislator and it is also in line with the expression-idea dichotomy enshrined in Recital 11 of the Software Directive. Otherwise, the safeguards established in the second paragraph of Article 8 would be devoid of meaning and purpose.

2615 Case C–406/10 *SAS Institute Inc. v World Programming Ltd* (CJEU, 2 May 2012), para 59.

2616 Case C–406/10 *SAS Institute Inc. v World Programming Ltd* (CJEU, 2 May 2012), para 61.

2617 Daniel Gervais and Estelle Derclaye, 'The scope of computer program protection after SAS: are we closer to answers?' [2012] 34 EIPR 562, 571; Gintare Surblyte, 'Enhancing TRIPS: Trade Secrets and Reverse Engineering' 725, 746 in Hanns Ullrich and others (eds), *TRIPS plus 20 - From Trade Rules to Market Principles* (Springer 2016).

2618 *SAS Institute Inc. v World Programming Limited* [2013] RPC 17 (Ch), [64].

2619 *SAS Institute Inc. v World Programming Limited* [2013] RPC 17 (Ch), [68]-[69].

In line with the previous argument, the interplay between the contractual limitations and the trade secrets legal regime has been questioned on the basis of the first paragraph of Article 8 of the Software Directive, which stipulates that the scope of application of the said Directive shall not affect other legal provisions that regulate "patent rights, trade-marks, unfair competition, *trade secrets*, protection of semi-conductor products or the law of contract". Thus, this leads to the question of whether contractual provisions that ban decompilation or the analysis of the ideas and principles underlying a computer program may be deemed null and void under the Software Directive but enforceable under Article 3(1)(b) TSD and thereby trigger liability as a breach of contract leading to the unauthorised use or disclosure of a trade secret (Article 4(3)(c) TSD).[2620]

A combined reading of Article 6 and Article 8 (second paragraph) of the Software Directive reveals that if a licensing agreement stipulates that the licensee is proscribed from decompiling a program for the purposes of achieving interoperability, such a clause will not be considered enforceable by courts under copyright rules. Therefore, considering that such a clause may nonetheless be valid and trigger liability under Article 3(1)(b) TSD if it is breached does not seem sound because it would circumvent one of the main goals of the Software Directive: to allow access to interfaces in order to ensure interoperability and avoid consumers being locked-in with a specific software manufacturer.[2621] The same is true for clauses that contract out the possibility of observing, studying or testing the functioning of the program to extract the underlying ideas or principles during the acts of loading, displaying, running, transmitting or storing the program (Article 5(3) of the Software Directive). As a result, the second paragraph of Article 8 of the Software Directive should be considered to take percent as lex specialis because it specifically regulates software contracts and the rights of the parties and, therefore, any contractual provision that would undermine the objectives pursued by the said Article should be considered null and void.[2622] This proposition is reinforced by Recital 39 TSD, which provides that the scope of application of the TSD shall not affect other regimes in

2620 Gintare Surblyte, 'Enhancing TRIPS: Trade Secrets and Reverse Engineering' 725, 750-753 in Hanns Ullrich and others (eds), *TRIPS plus 20 - From Trade Rules to Market Principles* (Springer 2016).

2621 Case T–201/04 *Microsoft v Commission* [2007] ECR II-03601, para 650.

2622 This is also the view supported by Tanya Aplin 2013 (n 2511) 373; Pamela Samuelson and Suzanne Scotchmer 2002 (n 226) 1660 and Thomas Dreier 1991 (n 2504) 325, who notes with respect to Article 6 of the Software Directive that "such a conclusion, which in essence would mean that a legitimate

place, and in particular IPRs. Notwithstanding this consideration, ultimately the interplay between the TSD and the Software Directive will be subject to the interpretation of the CJEU.

Having regard to the above legal framework, from a policy perspective, it should be noted that, in general, contractual restrictions may have an adverse effect on competition and innovation.[2623] In essence, one of the policy rationales that justifies trade secrets protection is that it is the necessary counterbalance to the patent system. In the words of the U.S. Supreme Court in *Kewanee Oil Co. v. Bicron Corp.*: "where patent law acts as a barrier, trade secret law functions relatively as a sieve.[2624] Reverse engineering promotes follow-on innovation by disseminating knowledge, even if not as directly as a patent specification, and gradually diminishes the market power of the first-comer. Thus, if customers contract out reverse engineering, information may never enter the public domain.[2625] In turn, this enhances the position of the trade secret holder, who may retain exclusivity in the market, to the detriment of their competitors. As noted by Samuelson and Scotchmer, the possibility of excluding reverse engineering is particularly problematic in markets that depend on IPRs, as these were established in order to regulate the scope of exclusive rights and their limitations and provide for the most adequate balance.[2626]

Consequently, the possibility that the legislator is allowed to establish that contractual clauses that offset this balance shall be null and void (Recital 16) appears sound from a policy perspective. It ensures that secrecy progressively erodes and that new competitors can enter the market, con-

---

program user could obtain information within the limits prescribed by the directive but that he could not use it, would run counter to the directive's very purpose of guaranteeing a certain minimum access to interface information in order to ensure interoperability. Therefore, Article 9(1) (now 8(1)) must be understood as meaning that the interface information which may mandatorily be obtained without infringement of exclusives right, may not be retained by contractual restrictions based on trade-secret protection".

2623 Gintare Surblyte, 'Enhancing TRIPS: Trade Secrets and Reverse Engineering' 725, 750-753 in Hanns Ullrich and others (eds), *TRIPS plus 20 - From Trade Rules to Market Principles* (Springer 2016).
Case T–201/04 *Microsoft v Commission* [2007] ECR II-03601, para 650.

2624 *Kewanee Oil Co.v. Bicron Corp*, 416 U.S. 470, 490 (1974).

2625 However, Michael Risch, 'Hidden in Plain Sight' [2017] 31 Berkeley Technology LJ 1635, 1652 argues in favour of applying such clauses to non-visible aspects of software, as well as to visible aspects regardless of whether they constitute trade secrets.

2626 Pamela Samuelson and Suzanne Scotchmer 2002 (n 226) 1660.

sidering its specific characteristics.[2627] Indeed, an absolute bar on such clauses without considering the specific circumstances of each market seems too far reaching and disregards their importance in pre-contractual negotiations. However, the validity of such clauses will have to be assessed in accordance with national civil law and, in particular, the provisions that regulate standard business terms.[2628]

3) Guiding principles

The analysis conducted reveals that the reverse engineering limitation is central to striking the optimal balance between the interests of trade secrets holders, competitors and third parties because it allows for the erosion of secrecy, which leads to the incorporation of information in the public domain. Therefore, to ensure that such a limitation is construed in a uniform manner across the EU the following interpretive remarks are presented.

First, drawing from the principles presented in chapter 4, and in order to delineate the boundaries of secrecy, the mere placing on the market of a product in which a trade secret is embodied does not automatically reveal all of the trade secrets associated with it. To hold otherwise would substantially limit the subject matter protected by the law of trade secrets.[2629] Instead, only those features (i) that are readily apparent upon inspection of the product, or (ii) that can be devised with little time and cost shall be deemed to have been made available. Secrecy remains with regard to the intrinsic features or processes that can only be devised after the investment of substantial time, effort and, in particular, cost and intellectual skill. In addition, if a secret is unveiled after a costly process of reverse engineering it shall not be automatically regarded as publicly available for the purposes of trade secrets law. The deciding factor is whether the information has been so widely disseminated within an industry that the competitive advantage conferred by it has disappeared.

Second, it should be noted that the wording of Article 3(1)(b) TSD does not allude to the actions of *use* and *disclosure*. Indeed, during the negotiation process, representatives from certain sectors (such as the perfume in-

2627 Pamela Samuelson and Suzanne Scotchmer 2002 (n 226) 1653.
2628 Christian Alexander 2017 (n 1091) 1041 referring to the test of reasonableness of content enshrined in § 307 BGB.
2629 Tanya Aplin 2014 (n 384) 271.

dustry) raised concerns as to the lawfulness of the subsequent use and disclosure of information acquired through reverse engineering, as well as regulatory disclosure. They claimed that allowing any subsequent use or disclosure would affect the "the functioning of the internal market and the commercial interests of the trade secret holder if it occurs without his permission and/or in a way contrary to fair commercial practices".[2630] Notwithstanding this consideration, following a systematic interpretation of the Directive, the subsequent use and disclosure of confidential information lawfully acquired through a process of reverse engineering should be a priori be permitted, unless contracted out. From a practical point of view, it does not always seem feasible to differentiate between the acquisition and subsequent use or disclosure of a trade secret.[2631] Also, from a policymaking perspective, it seems unsound to allow for the acquisition of secret information through reverse engineering and to prevent its subsequent use and disclosure: the economic justifications that apply to the acquisition of reverse engineered products also apply to any use and disclosure that follow, even if competing products are created.[2632] This fosters knowledge dissemination and ultimately strengthens competition in the market.[2633] Otherwise, the trade secret holder would be in a position similar to the patent holder, where the relevant technology is disclosed in the patent specification but competitors are not allowed to use it for commercial purposes.

However, when reverse engineering is so cheap, easy and rapid that it may have market destructive consequences, because it could undermine the incentive to invest in the creation of new products, there may be a case for prohibiting specific forms of reverse engineering or limiting the use of the products manufactured with the information obtained, for instance, by introducing a breath requirement with respect to the products obtained through a process of reverse engineering .[2634] Consequently, the products created as a result of the said process should meet a certain threshold of in-

2630 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.

2631 This is the view expressed by Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) para 35, who note that it is not always possible to differentiate between acquisition and use.

2632 Tanya Aplin 2013 (n 2511) 373.

2633 Tanya Aplin 2013 (n 2511) 372-373.

2634 Pamela Samuelson and Suzanne Scotchmer 2002 (n 226) 1653; Ansgar Ohly 2009 (n 98) 550.

novation; they cannot be mere replicas. This was the approach followed by the EU legislator with respect to semiconductor chip layout. Ultimately, by virtue of the principle of precedence of EU law over national legal regimes and considering that Article 3(1)(b) TSD constitutes a maximum standard of protection,[2635] the introduction of limitations that ban specific forms of reverse engineering or demand forward programming should be assessed and proposed by the EU legislator (not national lawmakers).[2636]

As a final note, it should not be overlooked that reverse engineering practices are also subject to the limitations imposed by IPRs and unfair competition regimes. If in the process of reverse engineering an IPR is infringed, the said act will trigger liability under the specific IPR regime, unless an exception is expressly included to that end, such as in the case of the reproduction right under copyright law to achieve the interoperability of a computer program. It should not constitute a defence to argue that the product has been reverse engineered.[2637] The admissibility of creating identical products is also subject to the scrutiny of national unfair competition rules and doctrines that regulate unfair copying.[2638] The scope of the freedom to imitate principle runs as a common threat in all jurisdictions, and the limitations to such a doctrine are applicable not only vis-à-vis formal IPRs, but also trade secrets.[2639]

C) Competition law as an inherent limitation to the protection conferred by a trade secret

Competition law operates as the third limitation to the rights conferred by a trade secret, even though it is not expressly set out in the body of the TSD, only in Recital 38.[2640] In this regard, it should be noted that the relationship between trade secrets and competition law is of a two-fold nature. On the one hand, secrecy is essential to ensuring competition in the market. If every market participant had access to competitors' information, no

2635 This principle is enshrined in Case 6/64 *Flaminio Costa v ENEL* [1964] ECR 585, 593-594.
2636 Pamela Samuelson and Suzanne Scotchmer 2002 (n 226) 1653.
2637 Tanya Aplin 2013(n 2511) 376.
2638 Ansgar Ohly 2009 (n 98) 550; see § 4(3) UWG and Article 11 of the Spanish Unfair Competition Act.
2639 See chapter 1 § 3 B) III.
2640 See Recital 38 TSD.

competitive pressure in innovation would exist.[2641] Such a rationale is embedded within the policy goals that inform the TSD. In the Impact Assessment prepared by the Commission, it was noted that restrictions on the use of misappropriated secret information are justified "in order to promote an economically efficient and competitive process".[2642] Indeed, as argued in chapter 1, secrecy provides incentives to innovate, as it allows its holders to internalise the benefits of innovations. Yet, this should not be viewed as an absolute statement.[2643] An array of factors should be weighed up to assess whether trade secrets protection will in fact lead to innovation within the market, namely the degree of market power or the specific features of the industry.[2644] To be sure, as already noted, "in the case of trade secrets the law does not guarantee that the protected information contains innovation".[2645]

On the other hand, secrecy may lead to de facto exclusivity, even if trade secrets are not exclusive absolute rights by nature like other formal IPRs, such as patents or copyright.[2646] Indeed, the fact that a market participant is able to withhold information from the rest of his competitors may confer on him exclusivity, which may ultimately result in an abuse of market dominance pursuant to Article 102 TFEU. This is best illustrated by refer-

2641 Gordon L. Doerfer, 'The Limits on Trade Secret Law Imposed by Federal Patent and Antitrust Supremacy' [1967] 80 Harvard LR 1432, 1462: "Trade secret law serves a positive function in the promotion of competition by providing a needed lead time within which development costs can be at least partially recovered. On balance, because of the relatively small and speculative harm to competition and because the of the probable benefits to competition through the basic incentive of lead time, trade secret law does not seem inimical to free competition".

2642 See in this regard the Explanatory Memorandum attached to the 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, 2.

2643 See chapter 1 § 2 B) I.

2644 Gintare Surblyte, 'Enhancing TRIPS: Trade Secrets and Reverse Engineering' 725, 735 in Hanns Ullrich and others (eds), *TRIPS plus 20 – From Trade Rules to Market Principles* (Springer 2016).

2645 See also Josef Drexl 2011 (n 50) 182.

2646 See Recital 16 TSD: "In the interest of innovation and to foster competition, the provisions of this Directive should not create any exclusive right on the know-how or information protected as trade secrets"; see further Gintare Surblyte, 'Enhancing TRIPS: Trade Secrets and Reverse Engineering' 725, 735 in Hanns Ullrich and others (eds), *TRIPS plus 20 – From Trade Rules to Market Principles* (Springer 2016).

ence to the *Microsoft* case decided in 2007 by the GCEU (then CFI), following an appeal from a previous decision rendered by the Commission.[2647] The main facts and legal reasoning are summarised below.

In the 1990s, Microsoft was dominant in the EU market for PC operating systems through its Windows platform.[2648] In 1998, Sun Microsystems, Inc., a competing firm that supplies servers and server operating systems, lodged a complaint before the Commission, arguing that Microsoft's refusal to disclose information necessary to achieve interoperability amounted to an abuse of market dominance pursuant to Article 102 TFEU, as it prevented the plaintiff and other competitors from working as a group server operating system supplier.[2649] At this point, it should be recalled that both the Commission and the GCEU held that it was not commercially viable to reverse engineer Microsoft's interoperability information owing to its high cost and the fast moving nature of the software market.[2650] In its response, *Microsoft* argued that "the Interoperability information requested by Sun constitutes valuable intellectual property protected by copyright, trade secret laws and patents".[2651]

Against this factual pattern, the Commission and the GCEU applied the "exceptional facilities" test developed in connection with the refusal to license IPRs (*Volvo*,[2652] *Magill*,[2653] *IMS Health*)[2654] and deemed that Microsoft's conduct amounted to an abuse of market dominance. Notwithstanding this, the GCEU reshaped the test, considering the fast-moving na-

2647 *Microsoft* (Case COMP/C-3/37.792) Commission Decision 2007/53/EC [2007] OJ L32/23 and Case T–201/04 *Microsoft v Commission* [2007] ECR II-03601; for an in-depth analysis of trade secrets and their impact on competition law see: Gintare Surblyte 2011 (n 182); see also Josef Drexl 2011 (n 50) 185.

2648 *Microsoft* (Case COMP/C-3/37.792) Commission Decision 2007/53/EC [2007] OJ L32/23, para 15.

2649 At that time Article 82 EC Treaty.

2650 *Microsoft* (Case COMP/C-3/37.792) Commission Decision 2007/53/EC [2007] OJ L32/23, paras 685-687; see Case T–201/04 *Microsoft v Commission* [2007] ECR II-03601 para 362.

2651 *Microsoft* (Case COMP/C-3/37.792) Commission Decision 2007/53/EC [2007] OJ L32/23, footnote 249.

2652 Case 238/87 *AB Volvo v Erik Veng (UK) Ltd* [1988] ECR I- 6211.

2653 Joined Cases C-241/91 P and C-242/91 *Radio Telefis Eireann (RTE) and Independent Television Publications (ITP) v Commission of the European Communities* [1995] ECR I-00743.

2654 Case C–418/01 *IMS Health v NDC* [2004] ECR I-5039.

ture of the software industry and the legal nature of trade secrets.[2655] The latter are not formally IPRs, but may in fact confer exclusivity in the market on their holders.[2656] The test, as envisaged by the CJEU in *IMS Health*, takes into account four cumulative elements.[2657] In the first place, the supply of the product must be indispensable for conducting the specific business. Secondly, the refusal to license must prevent the emergence of a new product. Thirdly, such a refusal cannot be justified on objective grounds. Finally, it excludes competition in a secondary market.[2658]

In *Microsoft* the cardinal question was whether the new product requirement, as laid down in *IMS Health,* would mean that Sun could develop a new product other than a group serving operating system, which was already offered by Microsoft. It was against this specific background that the Commission and the GCEU departed from the CJEU's case law and turned to the wording of Article 102(b) TFEU.[2659] The GCEU noted that the appearance of a new product should not be the only criterion:[2660]

> The circumstances relating to the appearance of a new product, as envisaged in Magill and IMS Health, cited in paragraph 107 above, cannot be the only parameter which determines whether a refusal to license an intellectual property right is capable of causing prejudice to consumers within the meaning of Article 82(b) EC. As that provision states, such prejudice may arise where there is a limitation only of production or markets, but also of technical development.

In the case of *Microsoft*, the value of the information did not lie in its technological superiority but rather in its secret nature, which prevented other

---

2655 Gintare Surblyte 2011 (n 182) 129; *Microsoft* (Case COMP/C-3/37.792) Commission Decision 2007/53/EC [2007] OJ L32/23, para 118 and Case T–201/04 *Microsoft v Commission* [2007] ECR II-03601, para 635.

2656 A new standard of intervention is proposed by Surblyte Gintare Surblyte 2011 (n 182) 213-217, who argues that owing to the fundamental differences in the legal nature of trade screts and formal IPRs, the legal test applied should be a different one.

2657 As clarified by the CJEU in Case C–418/01 *IMS Health v NDC* [2004] ECR I-5039, para 38.

2658 Beatriz Conde Gallego, 'Unilateral refusal to license indispensable intellectual property rights – US and EU approaches'215-238 in Josef Drexl (ed), *Research Handbook on Intellectual Property and Competition Law* (Edward Elgar, 2008).

2659 See Gintare Surblyte 2011 (n 182) 128-133, T-201/04 *Microsoft v Commission* [2007] ECR II-03601, para 128-133.

2660 Case T–201/04 *Microsoft v Commission* [2007] ECR II-03601, para 647.

potential competitors from entering the market.[2661] This poses a number of questions vis-à-vis the complementarity theory that governs the relationship between IPRs and competition law. In effect, the prevailing approach is that IPRs and competition law strive to achieve the same objective, namely, to foster competition and innovation.[2662] [2663] However, in the case of trade secrets, protection is afforded without taking into consideration whether the information covered is in fact innovative.[2664] Furthermore, where access to information is key to enter a specific market, the likelihood of monopolisation is high if the law affords protection to trade secrets (or access to information in general).[2665]

In addition, as already noted,[2666] contractual agreements between the parties that limit the use of trade secrets may result in a restrain of competition and therefore are also subject to the scrutiny of competition law under Article 101 TFEU and the corresponding block exemption regulations approved to improve the production or distribution of goods and to promote technical or economic progress, such as the TTBER and the R&DBER.

In sum, it seems that secrecy is necessary to foster competition in the market. Yet, as seen in the example of *Microsoft*, under certain circumstances it may lead to an abuse of dominant position prohibited under to Article 102 TFEU or a restrain of competition proscribed under Article 101 TFEU. In such a context, competition law may arise as a necessary limitation to secrecy. Such a rationale has been incorporated as part of the TSD in Recital 38, which lays down the prevalence of Articles 101 and 102

2661 Josef Drexl 2011 (n 50) 182-183.

2662 Josef Drexl, 'Intellectual Property and Antitrust Law – IMS Health and Trinko – Antitrust Placebo for Consumers Instead of Sound Economics in Refusal-to-Deal Cases' [2004] IIC 788, 792.

2663 Commission, 'Guidelines on the application of Article 81 of the EC Treaty to technology transfer agreements' [2004] OJ C101/2, para 7: "Indeed, both bodies of law share the same basic objective of promoting consumer welfare and an efficient allocation of resources. Innovation constitutes an essential and dynamic component of an open and competitive market economy. Intellectual property rights promote dynamic competition by encouraging undertakings to invest in developing new or improved products and processes. So does competition by putting pressure on undertakings to innovate. Therefore, both intellectual property rights and competition are necessary to promote innovation and ensure a competitive exploitation thereof".

2664 Josef Drexl 2011 (n 50) 181.

2665 Josef Drexl 2011 (n 50) 183.

2666 Chapter 6 § 1 B).

TFEU and sets out that the provisions of the Directive should not provide legal grounds to restrict competition in a manner contrary to the TFEU.

§ 3 *The optimal scope of secrecy: a balanced approach in the light of the TSD*

Trade secrets play a central role in many industries, where they are deemed essential assets to appropriate returns from innovation, particularly when no formal IPR protection applies, such as in the perfume industry. Their strategic importance for economic growth and competitiveness prompted the Commission to harmonise this area of law among the EU Member States. Yet, during the negotiation process concerns were raised regarding the optimal scope of secrecy and its effect on creative and innovative industries. In fact, the analysis conducted throughout this thesis underscores the difficulties in finding the appropriate strength of trade secrets protection. To be sure, if the scope is too broad, follow-on innovation and free speech may be hindered. Conversely, if the protection of secret information is tailored in a manner that is too narrow, the incentives to create valuable information will be substantially diminished, which in turn may lead to market failure in certain industries where formal intellectual property protection falls short, such as the cosmetics industry. Considering the above, this section explores potential solutions to define the optimal scope of secrecy.

A) The Nordhaus model and trade secrets protection

First, it should be recalled that trade secrets may last for as long as the information that they cover remains undisclosed. This is a well-established principle among EU jurisdictions as well as in the U.S., and results from the interplay between the patent system and the trade secrets legal framework.[2667] In fact, the duration of trade secrets may exceed that of patents or copyright.[2668] Pursuant to TRIPs, the patent term of protection is twenty years from filing.[2669] Similarly, copyright protection lasts for at least fifty

2667 Accordingly, the TSD does not set forth any term of protection.
2668 But note that for trade marks the term of protection extends for as long as the mark is used in commerce and the appropriate fees are paid.
2669 See Article 33 TRIPs.

years after the death of the author.[2670] It is generally regarded that misappropriation, reverse engineering and independent creation limit the duration of secrets and make them more vulnerable than any other IPR.[2671] However, in some instances this may not be possible and the holders of undisclosed information may be able to exploit it in an exclusive manner with no end in sight, which may ultimately affect the possibility of competitors to innovate.

A prime example of the potentially perpetual duration of trade secrets is the Coca-Cola formula, which was developed over one hundred and twenty-five years ago and remains one of the most valuable secrets of all time.[2672] In the same vein, in the software industry, the practical difficulties of reverse engineering Microsoft's interoperability information were one of the main hurdles that competitors faced in entering the operating systems market. As highlighted both by the Commission and the GCEU (then CFI), it was not commercially viable to reverse engineer Microsoft's interoperability information owing to its high cost and the fast moving nature of the software market.[2673] In this regard, Scotchmer noted that, "unlike other forms of intellectual property, trade secret allow owners to supress knowledge".[2674] Such a statement is at odds with the need to reconcile the need to provide incentives to innovate for trade secret holders and the interests of the public at large in using such information.[2675]

When reverse engineering is too costly and lengthy, the holder of the secret will be able to reap the fruits of his innovation perpetually (or after the patent term) without complying with the disclosure obligations imposed by the patent system and the knowledge spill-over derived from it.

From a law and economics perspective, the optimal strength of trade secrets protection has been analysed from four different, yet not necessarily

2670 See Article 12 TRIPs; but note that in many jursidictions, such as the EU and the U.S., the term has been extended to seventy years.

2671 Mark A Lemley 2008 (n 15) 352-353.

2672 See 'Coca-Cola Moves Its Secret Formula to The World of Coca-Cola' (The Coca-Cola Company, 8 December 2011) <http://www.coca-colacompany.com/press-center/press-releases/coca-cola-moves-its-secret-formula-to-the-world-of-coca-cola/> accessed 15 September 2018.

2673 *Microsoft* (Case COMP/C-3/37.792) Commission Decision 2007/53/EC [2007] OJ L32/23, paras 685-687; Case T–201/04 *Microsoft v Commission* [2007] ECR II-03601, para 362.

2674 Suzanne Scotchmer 2004 (n 41) 81. However, the author further notes that "the law encourages the sharing and sale of ideas"; see also Robert G. Bone 1998 (n 15) 281.

2675 Mark A. Lemley 2008 (n 15) 353.

mutually exclusive, angles. The most prominent theory, purported by Friedman, Landes and Posner, is that the optimal scope of secrecy should be determined by reference to the liable conduct i.e. the lawful ways of acquiring, using and disclosing secret information and the costs and benefits associated with it.[2676] For instance, as has already been examined, allowing competitors to obtain a secret through reverse engineering off-sets the cost of preventing such conduct, due to the benefits triggered by follow-on innovation. However, if no trade secrets protection were afforded against theft, the expenditure on self-help measures by trade secrets owners would be very high, which in turn would increase the expenditure of competitors and consequently lead to a wasteful arms race.[2677] This approach seems to be the one followed by the EU legislator in view of the broad array of exceptions and lawful conducts laid down in the TSD. Other scholars propose that the optimal scope of protection should be modulated during the enforcement phase, i.e. through establishing the amount of damages.[2678] In a similar vein, it would be possible to limit the subject matter eligible for trade secrets protection.[2679] This seems to be one of the principles applied to foster employee mobility: the skills and knowledge acquired during the normal course of the employee's work do not constitute a protectable trade secret.[2680] Finally, a fourth possibility would be to limit the duration of protection, which is a major theme of discussion in the field of patent law, but has garnered little attention with regard to trade secrets.

To study the optimal scope of trade secrecy, this thesis focuses on duration as a key parameter and looks into the inherent trade-off between static and dynamic efficiency, particularly in the context of technical inventions. To do so, it applies the Nordhaus model, which was developed to analyse the optimal length of patent rights.[2681] Nordhaus' concept has been at the centre of the patent policy discussion for the last fifty years, not least be-

2676 David D. Friedman, William M. Landes and Richard A. Posner, 'Some Economics of Trade S–et Law' [1991] 5 J Econ Perspectives 61, 67-70.

2677 David D. Friedman, William M. Landes and Richard A. Posner, 'Some Economics of Trade Secret Law' [1991] 5 JEP 61, 69; see more generally chapter 1 § 2 B) III.

2678 Thomas Rønde, 'Trade secrets and information sharing' [2001] 10 J of Economics & Management Strategy 391-417.

2679 Luigi A. Franzoni and Arun Kaushik, 'The optimal scope of trade secrets law' [2016] 45 International Review of Law and Economics 45, 45.

2680 This issue has been analysed under chapter 6 § 1 A) II.

2681 William D. Nordhaus, *Invention Growth, and Welfare: A Theoretical Treatment of Technological Change* (The MIT Press 1969) 10.

cause duration arguably represents the most direct way in which legislators can control the scope of rights.[2682]

As examined in chapter 1, patents equip the innovator with exclusionary rights so that he can reap the benefits of his invention.[2683] These benefits are necessary to incentivise the inventor to conduct costly and uncertain R&D investments. However, the innovator's monopoly rents come at a cost for society, because the profit maximising product price in a monopoly is higher than in a competitive environment. This excludes some consumers who are not able pay the monopoly price. This so-called "deadweight loss" reduces the benefits for society coming from the invention. Limiting the exclusionary rights to a specific duration, such as is the case for patents with a maximum length of twenty years, seeks to achieve a compromise between the costs in static efficiency,[2684] due to the exclusion of consumers, and the costs in dynamic efficiency,[2685] due to insufficient incentives for innovators.

In sum, there is a social cost in extending IPR induced monopolies beyond the duration necessary to incentivise the innovator. This is also true in the case of secrecy induced monopolies. However, the investment necessary for invention differs greatly between industries. For instance, pharmaceutical inventions are particularly investment-intensive, but also come with potentially large benefits for society.[2686] By setting the duration of protection to a very long period or even making it infinite, these kinds of investment-intensive inventions become worthwhile; however, inventors in other fields are provided with unnecessarily long monopolies. Nordhaus, for the first time, analysed this trade-off and argued for a finite duration of patents. He theoretically concluded that after a certain patent duration, the social benefits generated by more costly new innovations no longer compensated for the dead-weight loss from the prolongation of monopolies.[2687] Hence, a socially optimal patent duration cannot be infinite.

In the light of the above argument, this thesis posits that following the Nordhaus Model by analogy, trade secrets protection should also be finite. Yet, it does not seem advisable to impose a fixed term duration as it exists

2682 François Lévêque and Yann Ménière, *The Economics of Patents and Copyright* (The Berkeley Electronic Press 2004) 25.
2683 The following arguments draw from the synthesis of the Nordhaus model provided in Lévêque and Ménière 2004 (n 2682).
2684 François Lévêque and Yann Ménière 2004 (n 2682) 26.
2685 François Lévêque and Yann Ménière 2004 (n 2682) 19.
2686 François Lévêque and Yann Ménière 2004 (n 2682) 46.
2687 François Lévêque and Yann Ménière 2004 (n 2682) 32.

for formal IPRs.[2688] Protection should cease when the additional incentive from the prospect of secrecy is marginal, while the social costs of maintaining an artificial monopoly rather remain constant. In such a case, the social benefits generated by the innovation would no longer compensate for the dead-weight loss from the prolongation of a monopoly.[2689] Consequently, from a legal perspective the duration of trade secrets would be best modulated by the inclusion of an exception to infringement claims. Here, the alleged infringer could counterclaim that trade secrets protection should not be enforceable if the dead-weight loss prevails in the above mentioned welfare trade-off. The problem, however, is that the information necessary to conduct such an assessment is, if at all, only in the possession of the trade secret holder. Third parties hence cannot evaluate in a reliable manner the point in time when the investment devoted to the development of the secret has been recouped and ultimately, from a welfare perspective, when they should be free to use the information.

Notwithstanding this, the final chapter of the dissertation has highlighted the relevance of contractual agreements in maintaining secrecy intra companies (with employees), but also extra companies (with regards to suppliers, licensees or R&D partners). Consequently, a manner of modulating the finite duration of secrecy protection would be to introduce a general presumption in the context of business-to-business agreements, by virtue of which the duration of secrecy and non-use obligations is limited to four years after the termination of the contract, unless the parties expressly agree otherwise. The contours of such a presumption are analysed in the following section.

B) Legal application of the Nordhaus model to trade secrets protection: introduction of a presumption regarding post-contractual duration in business-to-business relationships

Contractual provisions that regulate non-disclosure obligations play a central role in deferring the entrance of information into the public domain both with regard to the internal and external spheres of secrecy of a company. Therefore, a potential legal application of the Nordhaus model

2688 Mark A. Lemley 2008 (n 15); Michael P. Simpson, 'The Future of Innovation: Trade Secrets, Property Rights, and Protectionism—An Age-Old Tale' [2005] 70 Brooklyn LR 1121, 1156-1158.

2689 Mark A. Lemley 2008 (n 15) 353.

would be to introduce a general presumption within the TSD that limits the duration of non-disclosure and non-use obligations in business-to-business contracts (including non-business entities, such as universities and research institutions) to four years after the termination of the agreement, unless the parties expressly agree for another term of duration. The wording of the proposed clause reads as follows:

> *In business-to-business agreements (including non-business entities) that regulate the acquisition, use and disclosure of trade secrets by virtue of which the parties undertake not to disclose and not to use the information that constitutes the object of the agreement after its termination, failure to mention the term of such obligations shall limit their duration to four years after the termination of the contract. In any case, these obligations will cease to exist once the information no longer meets the requirements for protection established in Article 2(1) of the present Directive for reasons not attributed directly or indirectly to the parties to the agreement to which the trade secrets have been disclosed.*

The introduction of the above reproduced contractual presumption is in line with the principle supported in many civil law jurisdictions by virtue of which obligations of an indefinite duration are considered non-enforceable by courts,[2690] which has also been questioned by the German competition authority in the context of licensing agreements that establish long post-contractual obligations of confidentiality (15 years).[2691] Consequently, the introduction of such a limited duration presumption in the absence of an express agreement between the parties would enhance legal certainty in post-contractual scenarios across the EU and would allow to strike a balance between the conflicting interests of trade secret holders and their commercial partners.

In effect, on the one hand, trade secret holders would be protected against unauthorised disclosure and use for four years after the termination of the contract. This would allow them to recoup the investment made in the creation of the information while ensuring that the recipient is prevented from taking advantage of the knowledge gained on the basis

2690 In Spain the invalidity of obligatons without a finite term is enshrined in Article 1583 of the Civil Code and has been the object of numeros judicial decisions such as STS de 14 de marzo de 2013. It has also been acknowledged by the most relevant civil law commentaries, such as Luis Díez-Picazo, *Fundamentos del derecho civil patrimonial*, vol II (5th edn, Tecnos 1996) 323.

2691 See BKartA 1977 TB 94.

of an extinct contractual relationship. On the other hand, the applicability of this presumption would ensure that the recipient of the information is not unreasonably burdened with secrecy and non-use obligations, the duration and scope of which were not clearly identified during the negotiation of the agreement. Indeed, the duty of loyalty invoked in many jurisdictions to justify secrecy obligations, which is inherent to the very nature of the employment relationship, is applied with more difficulty in business-to-business relationships among competitors. It is for this reason that the scope of such a presumption should only be applicable in business-to-business contractual agreements, such as R&D agreements, licensing agreements and agreements with suppliers concluded between legal entities and not in business-to-consumer or employment contracts. However, considering that one of the main goals of the Directive is to foster research and innovative efforts, such a presumption should also apply with respect to contractual agreements in which at least one of the parties is a non-business entity, such as a university or research institution.

Crucially, the duration of the non-disclosure and non-use obligation is first and foremost dictated by the will of the parties, in line with the principle of party autonomy that governs civil law. Only in the absence of a specific agreement regarding the duration, the four year post-contractual presumption becomes relevant. The fact that the proposed provision states that non-disclosure and non-use obligations cease once the information no longer meets the requirements of protection for a trade secret stipulated in Article 2(1) TSD ensures that the parties that receive the information are not bound to keep it secret and not use it after it has become generally known among the relevant circles, which would seem unreasonable considering that the object of the contract has ceased to exist. Yet, if the secret is lost for reasons attributable to one of the parties to which the trade secret was disclosed, the secrecy and non-use obligations should remain enforceable with respect to that party, in line with Article 13(2) TSD. By way of contrast, clauses that provide that confidentiality and non-use obligations last until the information becomes generally known should be considered valid, because such a wording provides sufficient legal certainty to the parties at the time that the contract is concluded regarding the temporal scope of the obligations undertaken. It is also in line with the view expressed by competition authorities and the TTBER, which consider that no competition law issues arise with respect to the agreements that regulate the non-use and disclosure of the licensed technology rights after the ex-

piry of the agreement, provided that the rights remain valid and in force.[2692]

Following the line of reasoning suggested by English courts in the context of licensing agreements, the reference to non-disclosure obligations is understood to include also the non-use of the information object of the contract, unless the terms of the agreement provide otherwise.[2693] Indeed, from a systematic perspective it does not always appear feasible to differentiate between use and disclosure because often the use of the information leads to its disclosure. Consequently, in post-contractual scenarios non-disclosure obligations also entail non-use of the information. According to the proposed presumption, in the absence of a specific term of duration, such obligations will be limited to four years after the termination of the agreement.

The recourse to contractual presumptions to balance the interests of the contracting parties is not alien to the IRPs legal system and is frequently included in copyright laws to safeguard the rights of authors, who are deemed to be in a weaker bargaining position than their counterparties. For instance, Article 43(2) of the Spanish Copyright Act provides that in an inter vivos assignment, failure to mention the time limits the assignment to five years.[2694] In the case of non-disclosure and non-use obligations, the four year duration term has been proposed as the default rule as a compromise between the various terms suggested by the different authors.[2695] In effect, in innovation-driven economies, the innovation race renders most technology known among competitors within a few years. Thus, the four years term seems to provide the optimal balance between the interests of all contracting parties.

Ultimately, it should be noted that the relevant provisions of the TRIPs Agreement that regulate undisclosed information do not require that any exceptions to the right conferred comply with the three-step test envisaged for copyright (Article 13 and Article 17 TRIPs), patent rights (Article 30 TRIPs), trade mark rights (Article 17 TRIPs) and design rights (Article

2692 Commission, 'Guidelines on the application of Article 101 of the Treaty on the Functioning of the European Union to technology transfer agreements' [2014] OJ C89/3, para 183 (c).

2693 See chapter 6 § 1 B) I. 2. c).

2694 See María del Carmen Gete-Alonso Valero, 'Artículo 43' 756, 784 in Rodrigo Bercovitz Rodríguez-Cano (ed), *Comentarios a la Ley de Propiedad Intelectual* (3rd edn, Tecnos 2007).

2695 See chapter 6 § 1 B) I. 2.c) and chapter 6 § 1 B) II.2.

26(2) TRIPs). Consequently, the implementation of the proposed presumption would not result in a breach of the TRIPs Agreement.