Appendix 8

Country Specific Questionnaires – Criminal Law

Austria

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

   There is a criminal liability for the violation of trade secrets, which is stipulated in Secs. 122, 123 and 124 Penal Code (Strafgesetzbuch) as well as the criminal provisions contained in the Act against Unfair Competition (please refer to the Commercial and IP Law Questionnaire in this respect). These are the most relevant provisions in this respect.

Sec. 122 Penal Code:	§ 122 Strafgesetzbuch:
(1) Anyone who discloses or exploits a trade or business secret (Para 3) which has been entrusted or made accessible to him in the course of his activity in exercising a surveillance, review or investigation enacted by the law or governmental order, shall be sentenced to a term of imprisonment of up to six months or a fine of up to 360 per diem rates.	(1) Wer ein Geschäfts- oder Betriebsgeheimnis (Abs. 3) offenbart oder verwertet, das ihm bei seiner Tätigkeit in Durchführung einer durch Gesetz oder behördlichen Auftrag vorgeschriebenen Aufsicht, Überprüfung oder Erhebung anvertraut oder zugänglich gemacht worden ist, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
(2) Anyone who commits the deed to obtain a pecuniary advantage for himself or somebody else or to cause a detriment to somebody else, shall be sentenced to a term of imprisonment of up to one year or a fine of up to 360 per diem rates.	(2) Wer die Tat begeht, um sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
(3) Para 1 comprises only trade or business secrets which the offender is obligated to keep secret by law and the disclosure or use of which is suitable to infringe the reasonable interest of the person subject to the surveillance, review or investigation.	(3) Unter Abs. 1 fällt nur ein Geschäfts- oder Betriebsgeheimnis, das der Täter kraft Gesetzes zu wahren verpflichtet ist und dessen Offenbarung oder Verwertung geeignet ist, ein berechtigtes Interesse des von der Aufsicht, Überprüfung oder Erhebung Betroffenen zu verletzen.
(4) The offender shall not be punished if the	(4) Der Täter ist nicht zu bestrafen, wenn die Offenbarung oder Verwertung nach Inhalt und Form durch ein öffentliches oder ein berechtigtes privates Interesse

disclosure or exploitation is justified in content and form by a public or justified private interest.

(5) The offender shall be prosecuted only upon the request of the person whose interest in secrecy is infringed (Para 3).

gerechtfertigt ist.

(5) Der Täter ist nur auf Verlangen des in seinem Interesse an der Geheimhaltung Verletzten (Abs. 3) zu verfolgen.

Sec. 123 Penal Code:

(1) Whoever spies out a trade or business secret with the intent to exploit such secret or to make it available for exploitation by somebody else or to disclose it to the public, shall be sentenced to a term of imprisonment of up to two years or a fine of up to 360 per diem rates. Both penalties may be imposed collectively.

(2) The offender shall be prosecuted only upon request of the injured party.

§ 123 Strafgesetzbuch:

(1) Wer ein Geschäfts- oder Betriebsgeheimnis mit dem Vorsatz auskundschaftet, es zu verwerten, einem anderen zur Verwertung zu überlassen oder der Öffentlichkeit preiszugeben, ist mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen. Beide Strafen können auch nebeneinander verhängt werden.

(2) Der Täter ist nur auf Verlangen des Verletzten zu verfolgen.

Sec. 124 Penal Code:

(1) Whoever spies out a trade or business secret with the intent that it shall be exploited, used or otherwise utilized abroad, shall be sentenced to a term of imprisonment of up to three years. In addition, a fine of up to 360 daily rates may be imposed.

(2) The same punishment shall apply to whoever discloses a trade or business secret, which he is obliged to protect, to exploitation, use or other utilization abroad.

§ 124 Strafgesetzbuch:

(1) Wer ein Geschäfts- oder Betriebsgeheimnis mit dem Vorsatz auskundschaftet, dass es im Ausland verwertet, verwendet oder sonst ausgewertet werde, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen. Daneben kann auf Geldstrafe bis zu 360 Tagessätzen erkannt werden.

(2) Ebenso ist zu bestrafen, wer ein Geschäfts- oder Betriebsgeheimnis, zu dessen Wahrung er verpflichtet ist, der Verwertung, Verwendung oder sonstigen Auswertung im Ausland preisgibt.

Secs. 122 and 123 Penal Code are private prosecution matters; so are Secs. 11 and 12 Act against Unfair Competition.

In addition, there are various provisions in other laws which set out requirements for the protection of trade and business secrets. A detailed review of these provisions would go beyond the scope of this questionnaire. The provisions on the infringement of professional confidentiality (Sec. 121 Penal Code) and the infringement of official secrecy (Sec. 310 Penal Code) take precedence over the more general provisions of Secs. 122 – 124 Penal Code.

Please note that, from a practical point of view, Sec. 11 of Act against Unfair Competition has very little forensic significance. Sec. 12 of Act against Unfair Competition has practically no forensic significance. The practical importance of these two provisions is based on the civil law remedy in the form of claims for cease and desist orders and damages.

The general nature of these provisions is the disclosure or exploitation of trade or business secrets, that have been entrusted to the offender in the course of a professional occupation, or which have been obtained by espionage. The penalties in question are imprisonment or fines. The legal values protected under this framework are the legitimate interest in the confidentiality of trade and business secrets and to punish infringements of such legitimate interests.

The relevant literature, in this respect, in Austria would be the following penal law commentaries:

- Ernst Eugen Fabrizy, Strafgesetzbuch (Penal Code), Manz 2010
- Ernst Eugen Fabrizy, Strafprozessordnung (Code of Criminal Procedure), Manz 2011
- Höpfel/Ratz, Strafgesetzbuch (Penal Code), online commentary, Manz

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

The Penal Code requires the following categories of intent:

- conditional intent (bedingter Vorsatz) for the use or exploitation of the trade or business secret (Sec. 122 (1) Penal Code)
- conditional intent (bedingter Vorsatz) for the exploitation, making available to somebody else for exploitation or publication of a trade or business secret (Sec. 123 Penal Code)
- conditional intent (bedingter Vorsatz) for the exploitation, use or utilisation abroad (Sec. 124 Penal Code)
- intent (Absicht) to obtain a pecuniary advantage for himself or somebody else or to cause a detriment to third parties (Sec. 122 (2) Penal Code)

The provisions stipulated by the Act against Unfair Competition require conditional intent to disclose a trade or business secret for competitive purposes. This requires awareness of the offender that the information in question is a trade or business secret.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

   The infringement of trade secrets may entail sanctions such as fines as well as criminal offences and/or civil lawsuits.

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

   Sec. 122 (4)of the Penal Code stipulates a justification if the disclosure or exploitation is justified in content and form by a public or justified private interest. This justification requires a balancing of the interests involved.

   Sec 19 (3) of the Act against Unfair Competition stipulates that Secs. 11 (2) and 12 do not apply to employees who have performed the action upon instruction by their employer, provided that they could not reasonably be expected to refuse performing the action due to their economic dependence on the employer.

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

   Sec. 122 (1) of Penal Code stipulates that either disclosure or exploitation of trade or business secrets gives rise to criminal liability. Secs. 123 and 124 of Penal Code require the spying out of trade or business secrets in order to give rise to criminal liability.

   Sec. 11 of the Act against Unfair Competition requires either actual disclosure or unauthorized use of the trade or business secret for competitive purposes to give rise to criminal liability.

   The sole risk of dissemination would not normally give rise to criminal liability. Depending on the facts of the case, the attempt to commit any of the offences enlisted above may give rise to criminal liability. According to Sec. 15 (2) of Penal Code, an offender attempts to commit an offence if the decision to carry out the offence has been actuated by an act that directly precedes the actual carrying out of the offence. Preparatory acts remain unpunished.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of

items covered by trade secrets)? How, if at all, are they treated differently by the law?

Penal law recognizes violations of offenders exercising surveillance, review or investigation activities based on law or governmental order (Sec. 122 Penal Code) as well as offences by everybody who spies out trade or business secrets (Sec. 123 Penal Code and Sec. 124 Penal Code for spying out for exploitation or use abroad). The wording of the provisions clarifies that the sanctions are more severe regarding Secs. 123 and 124 Penal Code.

The Unfair competition law recognizes violations of employees and violations of third parties (former employees or anybody who receives information on trade or business secrets). The sanctions are identical in either case.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

   Austrian law does not differ between trade secrets and business secrets. However, trade secrets are often referred to as facts and knowledge of a mostly commercial nature, which are known only to persons acquainted with the internal course of the business, and business secrets referred to more technical factors. These general notions are common in both civil and criminal law.

   Please also refer to our answer to Question 5. above with regard to the conducts that are prohibited under criminal law and the law against unfair competition.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

   Both Austrian criminal and civil law have developed similar standards for the definition of trade and business secrets:

   - Commercial or technical information or processes in relation to the business of a company which are important for the competitive position of the company, and which are
   - only known to certain and limited circle of people,
   - which shall be kept confidential and with regard to which
   - there is a legitimate economic interest in the confidentiality of the information or process.

   This definition includes, inter alia, strategic questions, conditions of purchase, distribution channels, customer lists, tennis lists, turnover on customer accounts, print methods, origin of raw materials, price calculation, sample collection, tenders, recipes, information on the production and storage of goods, methods of production,

design or engineering drawings, patented systems and the like, which comply with the requirements enlisted above.

Austrian case law and literature have excluded the following from protection as a trade or business secret: obvious facts (which, for example, could nevertheless be protected as patents), literary knowledge accessible to everyone, general economic data such as information on cross-border leasing (OLG Innsbruck 4.5.2005, 2 R 103/05x).

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

   Please see our answer to Question 8. above with regard to the standards for trade and business secrets. The patentability of the items covered by trade secrets does not have any impact on the extent of the protection granted by the law.

   However, please note if a trade or business secret is patented, it will no longer be confidential and will thus lose its trade or business secret status.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

    Under Austrian law, registered IP rights such as trade marks, patents, utility models, designs, mask work rights and supplementary protection certificates also enjoy criminal protection. Please refer to Sec. 60 Trade Mark Act (Markenschutzgesetz), Sec. 159 Patent Act (Patentgesetz), Sec. 42 Utility Model Act (Gebrauchsmustergesetz), Sec. 35 Design Act (Musterschutzgesetz), Sec. 22 Mask Work Right Act (Halbleiterschutzgesetz) and Sec. 7 Supplementary Protection Certificate Act (Schutzzertifikatsgesetz) for further information. The penalties range from fines to imprisonment of up to two years for infringement in the course of commercial activities.

<u>B. CRIMINAL LITIGATION</u>

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

   Secs. 122 and 123 of Penal Code as well as Secs. 11 and 12 of the Act against Unfair Competition are private prosecution matters. In such case, the offender will be prosecuted at the initiative of the injured party only. In such case, the injured party may file a private criminal action which has to fulfil the requirements of a bill

of indictment. Only the injured party is entitled to start a proceeding and/or to claim damages (i.e. the owner of the business).

Sec. 124 of Penal Code is an official action, in which the offender will be prosecuted solely upon initiative of the Public Prosecutor.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

   Criminal proceedings are effected according to the general principles of the Austrian Code of Criminal Procedure. The private prosecutor is generally entitled to the same rights as the public prosecutor (with exceptions regarding certain sanctions). Any evidence that serves to help find the truth is permitted, unless it is explicitly prohibited (such as confessions obtained following torture or illegal influence on the freedom to make up and manifest one's mind). Valid evidence would be documents, witnesses, expert evidence or evidence by inspection

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

   In private prosecution matters, the preliminary investigation is not open to the private prosecutor. The private prosecutor may only apply for provisional pecuniary orders.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

   Yes, under Austrian law, companies may be liable for trade secret violations committed by their decision-makers (such as directors, executive committee members, authorized offers) or employees. The Act on Corporate Criminal Liability (Verbandsverantwortlichkeitsgesetz) sets out the conditions for the liability of legal entities and business partnerships.

2. If so, which type of liability arises for companies? Which penalties shall apply?

   The company is liable for trade secret violations either committed by a decision-maker or by employees who have not sufficiently been monitored and supervised.

The company is only liable if the violation has been committed in the favour of the company or if the violation has infringed obligations which fall within the company's responsibility. With regard to decision-makers, unlawful and culpable violations fall within the scope of the Act on Corporate Criminal Liability. With regard to employees, unlawful violations committed by behaviour which disregards reasonable diligence are covered by the Act on Corporate Criminal Liability, if the company fails to take essential technical, organizational and personal measures to prevent such violations. Culpable behaviour is not required with regard to employees' violations.

The applicable penalties are fines, which are calculated in per diem rates. The number of per diem rates which is adjudicated, is calculated based on the penalties provided for in the infringed provision of the Penal Code (up to 40 per diem rates in case of infringement of Sec. 122 (1) Penal Code, up to 55 per diem rates in case of infringement of Sec. 122 (2) Penal Code, up to 70 per diem rates in case of infringement of Sec. 123 Penal Code and up to 85 per diem rates in case of infringement of Sec. 124 Penal Code). The per diem rate is calculated on the profit situation and can range between the minimum of EUR 50,- and the maximum of EUR 10.000,-. The maximum penalty amounts to EUR 1.800.000,-.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

   The same court at which the procedures against the infringer have been opened, may adjudicate the cases of liability of companies (Sec. 15 (1) Act on Corporate Criminal Liability).

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

   According to the provisions in the Penal Code, the following obligations apply:

   - Sec. 122: The business secret has either been entrusted or made accessible in the course of an activity in exercising a surveillance, review or investigation enacted by the law or governmental order. Only trade or business secrets which the offender is obliged to keep secret by law and the disclosure or use of which is suitable to infringe the reasonable interests of the person subject to the surveillance, review or investigation fall within the scope of this provision.

   - Sec. 123: The business secret is spied out with the intent to exploit such secret or to make it available. There is no requirement for the information to be expressly stated to be a trade or business secret. The trade or business secret has to be spied out unlawfully, otherwise Sec. 123 does not apply. The same reasoning applies to Sec. 124 (spying out for the purpose to exploit, use or otherwise utilise the trade or business secret abroad).

   There is no differentiation between employees or other persons.

According to the penal provisions in the Act against Unfair Competition, the following obligations apply:

- Sec. 11 Para 1: This provision applies to employees and requires the disclosure of trade or business secrets for competitive purposes without authorisation during the duration of the employment relationship. The trade or business secrets must have been made accessible to him or entrusted to him due to his employment. There is no requirement to expressly state the intention to keep the knowledge secret. It is sufficient if such intention is apparent from the circumstances of the case.

- Sec. 11 Para 2: This provision applies to anybody who - without authorisation and for competitive purposes - uses or discloses to others any trade or business secrets which he has received by information from an employee as stated in Para 1 above or which he has received by an act of his own which is illegal or contrary to public policy. This provision applies to any offender (also former employees). There is no requirement to expressly state the intention to keep the knowledge secret. It is sufficient if such intention is apparent from the circumstances of the case.

- Sec. 12: This provision applies to other persons than employees: the unauthorised use or disclosure to another party of technical documents or requirements entrusted to somebody in the course of business falls within the scope of this provision. The use or disclosure requires a competitive purpose. There is no requirement for an expressly stated intention to keep the information secret.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

   With regard to the provisions of the Penal Code, the offender does not have to qualify as a competitor or potential competitor.

   With regard to the provisions of the Act against Unfair Competition, the offender has to act for competitive purposes. However, the qualification as a competitor or potential competitor is not required as such.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

   Under Austrian criminal law, an aggrieved person may not bring damage claims in the course of criminal proceedings. However, a conviction in criminal proceedings may serve as a basis for the assertion of damage claims in civil proceedings - which will have to be initiated independently of the criminal proceedings.

Belgium

A. APPLICABLE REGULATORY FRAMEWORK

1.Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Yes, trade secrets violation constitutes a criminal offence under Belgian law.

Article 309 of the Criminal Code concerns a specific type of trade secrets: the "manufacturing secret" (*fabricagegeheim / secret de fabrication*). This provision however only applies to "manufacturing secrets" disclosed by (former) employees or civil servants. "Manufacturing secrets" are defined by the Belgian Supreme Court (*Hof van Cassatie / Cour de Cassation*) as *"technical data which, in contributing to the realisation of operations put in place in a factory to obtain a certain product, are liable to provide to the manufacturer technical advantages and which ensure a competitive superiority over his competitors so that the manufacturer obtains an economical benefit by not disclosing the information to his competitors"*[1]. In its decision of 26 June 1975, the Belgian Supreme Court also ruled that, absent a legal definition of "manufacturing secret" in Belgian law, it is up to the court ruling on the merits to decide whether, in a given case, a manufacturing process qualifies as a "manufacturing secret"[2].

Article 309 of the Criminal Code also provides for specific criminal sanctions in case employees working or having worked in a factory reveal any "manufacturing secrets" from that factory to third parties with fraudulent intent. The sanctions include imprisonment of three months to three years and a fine of EUR 300 to EUR 12,000.

Text of article 309 of the Belgian Criminal Code:

In Dutch:	In French:	In English (free translation):
"Hij die geheimen van de fabriek waarin hij werkzaam geweest is of nog is, kwaadwillig of bedrieglijk aan anderen meedeelt, wordt gestraft met gevangenisstraf van drie maanden tot drie jaar en met geldboete van vijftig euro tot tweeduizend euro".[3]	*"Celui qui aura méchamment ou frauduleusement communiqué des secrets de la fabrique dans laquelle il a été ou est encore employé, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de cinquante euros à deux mille euros".*	*"The individual who communicates in a deceitful or malicious way manufacturing secrets of the factory where he is working or has worked, will be punished with an imprisonment from three months to three years and a penalty fine from fifty euro to two thousand euro".*

Article 458 of the Criminal Code concerns the professional privilege (*beroepsgeheim / secret professionnel*) for medical doctors, surgeons, health officers, pharmacists, midwives and all other persons who by virtue of their status or profession have knowledge of secrets entrusted to them, and disclose those secrets.

[1] Supreme Court 27 September 1943, *Pas.* I, 358.
[2] Supreme Court 26 June 1975, *Pas.* 1975, I, 1043.
[3] Please note that surcharges apply so that, as from 1 January 2012, the amounts of all criminal penalties must be multiplied by 6 (see, Act of 28 December 2011 containing Miscellaneous Provisions (II)).

A person who commits a breach of Article 458 of the Criminal Code faces imprisonment of 8 days to six months and a fine of EUR 600 to EUR 3,000.

Text of article 458 of the Criminal Code:

In Dutch:	In French:	In English (free translation):
"Geneesheren, heelkundigen, officieren van gezondheid, apothekers, vroedvrouwen en alle andere personen die uit hoofde van hun staat of beroep kennis dragen van geheimen die hun zijn toevertrouwd, en deze bekendmaken buiten het geval dat zij geroepen worden om in recht of voor een parlementaire onderzoekscommissie getuigenis af te leggen en buiten het geval dat de wet hen verplicht die geheimen bekend te maken, worden gestraft met gevangenisstraf van acht dagen tot zes maanden en met geldboete van honderd euro tot vijfhonderd euro".	*"Les médecins, chirurgiens, officiers de santé, pharmaciens, sages-femmes et toutes autres personnes dépositaires, par état ou par profession, des secrets qu'on leur confie, qui, hors le cas où ils sont appelés à rendre témoignage en justice ou devant une commission d'enquête parlementaire et celui où la loi les oblige à faire connaître ces secrets, les auront révélés, seront punis d'un emprisonnement de huit jours à six mois et d'une amende de cent euros à cinq cents euros"*.	*"Medical doctors, surgeons, health officers, pharmacists, midwives and all other persons who by virtue of their status or profession have knowledge of secrets entrusted to them, and disclose them, except in case they are called to give testimony in the framework of court proceedings or a parliamentary inquiry or in case they are required by law to disclose those secrets, shall be punished with imprisonment from eight days to six months and a fine of one hundred to five hundred euro".*

Articles 461 and 464 of the Criminal Code sanctions theft. A person who is prosecuted on the basis of Art. 309 of the Criminal Code, is likely to be sued also on the basis of Article 461 Criminal Code as well as Article 464 Criminal Code if the offender is a (former) employee. A breach of Articles 461 and 464 of the Criminal Code will be sanctioned with imprisonment from 1 month to five years and a fine from EUR 156 to EUR 3,000 (see, Article 463 Criminal Code).

Text of Articles 461 and 464 of the Criminal Code:

In Dutch:	In French:	In English (free translation):
Art. 461 *"Hij die een zaak die hem niet toebehoort, bedrieglijk wegneemt, is schuldig aan diefstal. Met diefstal wordt gelijkgesteld het bedrieglijk wegnemen van andermans goed voor een kortstondig gebruik."*	*Art. 461* *"Quiconque a soustrait frauduleusement une chose qui ne lui appartient pas, est coupable de vol. Est assimilé au vol le fait de soustraire frauduleusement la chose d'autrui en vue d'un usage momentané."*	*Art. 461* *"Any person who fraudulently takes away something that does not belong to him, is guilty of theft. The fraudulent removal of another's property for temporary use is equated with theft."*
Art. 464 *"De gevangenisstraf is ten minste drie maanden, indien de dief een*	*Art. 464* *"L'emprisonnement sera de trois mois au moins, si le voleur est un domestique*	*Art. 464* *"The imprisonment is at least three months if the*

dienstbode of een loondienaar is, zelfs wanneer hij de diefstal gepleegd heeft ten nadele van andere personen dan die welke hij diende, maar die zich bevonden hetzij in het huis van de meester, hetzij in het huis waar hij hem vergezelde, of indien de dief een werkman, gezel of leerling is, die de diefstal heeft gepleegd in het huis, het werkhuis of het magazijn van zijn meester, of ook indien de dief een persoon is die gewoonlijk arbeid verricht in de woning waar hij gestolen heeft."

ou un homme de service à gages, même lorsqu'il aura commis le vol envers des personnes qu'il ne servait pas, mais qui se trouvaient soit dans la maison du maître, soit dans celle où il l'accompagnait, ou si c'est un ouvrier, compagnon ou apprenti, dans la maison, l'atelier ou le magasin de son maître, ou un individu travaillant habituellement dans l'habitation où il aura volé."

thief is a maid or a wage slave, even when the theft has been committed against persons other than those he served, but who found themselves either in the house of the master, either in the house where he was accompanying him, or if the thief is a workman, journeyman or apprentice, who has committed the theft in the house, the workhouse or the warehouse of his master, or even if the thief is a person who usually performs work in the house where he has stolen."

Article 491 of the Criminal Code sanctions abuse of confidence. When business secrets are physically incorporated into documents, data carriers or other tangible property that were made available to the offender, with a clear demarcation of the use that could be made of it, and this person then deceptively discloses these (or a copy thereof) to an unauthorized third party, this conduct qualifies as a breach of Article 491 of the Criminal Code. A breach of Article 491 of the Criminal Code will be sanctioned with imprisonment of 1 month to five years and a fine from EUR 156 to EUR 3,000.

Text of Article 491 of the Criminal Code:

In Dutch:

"Hij die ten nadele van een ander goederen, gelden, koopwaren, biljetten, kwijtingen, geschriften van om het even welke aard, die een verbintenis of een schuldbevrijding inhouden of teweegbrengen en die hem overhandigd zijn onder verplichting om ze terug te geven of ze voor een bepaald doel te gebruiken of aan te wenden, bedrieglijk verduistert of verspilt, wordt gestraft met gevangenisstraf van een maand tot vijf jaar en met geldboete van zesentwintig euro tot vijfhonderd euro. De schuldige kan bovendien worden veroordeeld tot ontzetting van rechten overeenkomstig artikel 33."

In French:

" Quiconque aura frauduleusement soit détourné, soit dissipé au préjudice d'autrui des effets, deniers, marchandises, billets, quittances, écrits de toute nature contenant ou opérant obligation ou décharge et qui lui avaient été remis à la condition de les rendre ou d'en faire un usage ou un emploi déterminé, sera puni d'un emprisonnement d'un mois à cinq ans et d'une amende de vingt-six euros à cinq cents euros.
Le coupable pourra, de plus, être condamné à l'interdiction, conformément à l'article 33."

In English (free translation):

"He who fraudulently misappropriates or wastes to another's detriment goods, monies, merchandise, tickets, discharges, writings of any kind, that include or cause an obligation or a debt liberation and are presented to him under an obligation to return them or to use them for a particular purpose, shall be punished with imprisonment from one month to five years and a fine of twenty-six euros to five hundred euros.
The culprit can also be sentenced to deprivation of rights under Article 33."

Article 492bis of the Criminal Code sanctions abuse of corporate assets by directors, in fact or in law, civil and commercial companies, or non-profit associations. Corporate assets include both physical and intangible, movable and immovable goods. "Know-how" refers to all secret and transferable knowledge of a company which can be used during the production or distribution of goods or the provision of services, and therefore forms of the corporate assets, as protected by Article 492bis Criminal Code. Third parties such as competitors, which are not directors of the injured company, can still be prosecuted as (co-)offender (e.g., provocation) or accomplice to the crime committed by a director.

A breach of Article 492-bis of the Criminal Code will be sanctioned with imprisonment of from 1 month to five years and a fine from EUR 156 to EUR 3,000.

Text of Article 492bis of the Criminal Code:

In Dutch:	In French:	In English (free translation):
"Met gevangenisstraf van een maand tot vijf jaar en met geldboete van honderd euro tot vijfhonderdduizend euro worden gestraft de bestuurders, in feite of in rechte, van burgerlijke en handelsvennootschappen, alsook van verenigingen zonder winstoogmerk, die met bedrieglijk opzet en voor persoonlijke rechtstreekse of indirecte doeleinden gebruik hebben gemaakt van de goederen of van het krediet van de rechtspersoon, hoewel zij wisten dat zulks op betekenisvolle wijze in het nadeel was van de vermogensbelangen van de rechtspersoon en van die van zijn schuldeisers of vennoten. *De schuldigen kunnen daarenboven veroordeeld worden tot ontzetting van hun rechten overeenkomstig artikel 33."*	*"Sont punis d'un emprisonnement d'un mois à cinq ans et d'une amende de cent euros à cinq cent mille euros, les dirigeants de droit ou de fait des sociétés commerciales et civiles ainsi que des associations sans but lucratif qui, avec une intention frauduleuse et à des fins personnelles, directement ou indirectement, ont fait des biens ou du crédit de la personne morale un usage qu'ils savaient significativement préjudiciable aux intérêts patrimoniaux de celle-ci et à ceux de ses créanciers ou associés.* *Les coupables peuvent, de plus, être condamnés à l'interdiction, conformément à l'article 33."*	*"Are punished with imprisonment of one month to five years and a fine of hundred dollars to five hundred thousand euros, the directors, in fact or in law, civil and commercial companies, as well as non-profit associations, who have used with fraudulent intent and for personal direct or indirect purposes the property or the credit of the legal entity, although they knew that such was in a meaningful way to the disadvantage of the legal interests of the legal entity and those of its creditors or partners.* *The guilty parties may in addition be sentenced to deprivation of their rights under Article 33."*

Article 504bis of the Criminal Code sanctions bribery. This provision lends itself particularly to punish (agreements regarding) the non-permissible publication of any type of business secrets, including non-materialized secrets. A breach of Article 504bis of the Criminal Code will be sanctioned with imprisonment of 6 months to two years and a fine from EUR 600 to EUR 600,000.

Text of Article 504bis of the Criminal Code:

In Dutch:

Art. 504bis
"§ 1
Passieve private omkoping bestaat in het feit dat een persoon die bestuurder of zaakvoerder van een rechtspersoon, lasthebber of aangestelde van een rechtspersoon of van een natuurlijke persoon is, rechtstreeks of door tussenpersonen, voor zichzelf of voor een derde, een aanbod, een belofte of een voordeel van welke aard dan ook vraagt of aanneemt, om zonder medeweten en zonder machtiging van, naar gelang van het geval, de raad van bestuur of de algemene vergadering, de lastgever of de werkgever, een handeling van zijn functie of een door zijn functie vergemakkelijkte handeling te verrichten of na te laten.

§ 2
Actieve private omkoping bestaat in het rechtstreeks of door tussenpersonen voorstellen aan een persoon die bestuurder of zaakvoerder van een rechtspersoon, lasthebber of aangestelde van een rechtspersoon of van een natuurlijke persoon is, van een aanbod, een belofte of een voordeel van welke aard dan ook voor zichzelf of voor een derde om zonder medeweten en zonder machtiging van, naar gelang van het geval, de raad van bestuur of de algemene vergadering, de lastgever of de werkgever, een handeling van zijn functie of een door zijn

In French:

Art. 504bis
« § 1er
Est constitutif de corruption privée passive le fait pour une personne qui a la qualité d'administrateur ou de gérant d'une personne morale, de mandataire ou de préposé d'une personne morale ou physique, de solliciter ou d'accepter, directement ou par interposition de personnes, une offre, une promesse ou un avantage de toute nature, pour elle-même ou pour un tiers, pour faire ou s'abstenir de faire un acte de sa fonction ou facilité par sa fonction, à l'insu et sans l'autorisation, selon le cas, du conseil d'administration ou de l'assemblée générale, du mandant ou de l'employeur.

§ 2
Est constitutif de corruption privée active la fait de proposer, directement ou par interposition de personnes, à une personne qui a la qualité d'administrateur ou de gérant d'une personne morale, de mandataire ou de préposé d'une personne morale ou physique, une offre, une promesse ou un avantage de toute nature, pour elle-même ou pour un tiers, pour faire ou s'abstenir de faire un acte de sa fonction ou facilité par sa fonction, à l'insu et sans l'autorisation, selon le cas, du conseil d'administration ou de l'assemblée générale, du mandant ou de l'employeur. »

In English (free translation):

Art. 504bis
"§ 1
Passive private bribery consists in the fact that a person who is director or manager of a corporation, agent or servant of a legal or a natural person, directly or through intermediaries, for himself or a third party, requires or assumes an offer, promise or advantage of any kind, to, without knowledge and without authorization of, as appropriate, the board of directors or the general assembly, the principal or the employer, to perform or refrain from performing an act of or facilitated by his function.

§ 2
Active private bribery consists in directly or through intermediaries making an offer, promise or advantage of any kind for themselves or for a third party to a person who is a director or manager of a corporation, agent or servant of a legal or a natural person, without knowledge and without authorization, as appropriate, of the board of directors or the general assembly, the principal or the employer, to perform or refrain from performing an act of or facilitated by his function.

functie vergemakkelijkte handeling te verrichten of na te laten."

Article 550bis of the Criminal Code sanctions hacking. Depending on the type of hacking (internal or external) and whether there is fraudulent intent, sanctions vary from imprisonment of 3 months to five years and a fine from EUR 156 to EUR 1,200,000.

Text of Article 550bis of the Criminal Code:

In Dutch:

Art. 550bis
§ 1
Hij die, terwijl hij weet dat hij daar toe niet gerechtigd is, zich toegang verschaft tot een informaticasysteem of zich daarin handhaaft, wordt gestraft met gevangenisstraf van drie maanden tot een jaar en met geldboete van zesentwintig euro tot vijfentwintig duizend euro of met een van die straffen alleen.
Wanneer het misdrijf, bedoeld in het eerste lid, gepleegd wordt met bedrieglijk opzet, bedraagt de gevangenisstraf zes maanden tot twee jaar.

§ 2
Hij die, met bedrieglijk opzet of met het oogmerk om te schaden, zijn toegangsbevoegdheid tot een informaticasysteem overschrijdt, wordt gestraft met gevangenisstraf van zes maanden tot twee jaar en met geldboete van zesentwintig euro tot vijfentwintigduizend euro of met een van die straffen alleen.

(…)

§ 6
Hij die opdracht geeft of aanzet tot het plegen van een van de misdrijven, bedoeld in §§ 1 tot 5, wordt

In French:

Art. 550bis
§ 1er
Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprisonnement de trois mois à un an et d'une amende de vingt-six euros à vingt-cinq mille euros ou d'une de ces peines seulement.
Si l'infraction visée à l'alinéa 1er, est commise avec une intention frauduleuse, la peine d'emprisonnement est de six mois à deux ans.

§ 2
Celui qui, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique, est puni d'un emprisonnement de six mois à deux ans et d'une amende de vingt-six euros à vingt-cinq mille euros ou d une de ces peines seulement.

(…)

§ 6
Celui qui ordonne la commission d'une des infractions visées aux §§ 1er à 5 ou qui y incite, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de cent euros à deux cent mille

In English (free translation):

Art. 550bis
§ 1
He who, while knowing that he is not yet entitled to it, accesses or controls a computer system, is punished with imprisonment from three months to a year and a fine of twenty-six euro2 to twenty-five thousand euro or with one of these penalties.
When the offense provided for in the first paragraph, is committed with fraudulent intent, the maximum prison sentence is six months to two years

§ 2
He who, with fraudulent intent or intent to harm, exceeds his legitimate access to a computer system, is punished with imprisonment from six months to two years and a fine of twenty-six euro to twenty-five thousand euro or one of these penalties.

(…)

§ 6
He who instructs or encourages to commit an offense specified in §§ 1 to 5 shall be punished with imprisonment from six months to five years and a fine of one hundred euro to two hundred thousand euro or one of these penalties.

gestraft met gevangenisstraf van zes maanden tot vijf jaar en met geldboete van honderd euro tot tweehonderdduizend euro of met een van die straffen alleen.

§ 7
Hij die, terwijl hij weet dat gegevens bekomen zijn door het plegen van een van de misdrijven bedoeld in §§ 1 tot 3, deze gegevens onder zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig euro tot honderdduizend euro of met een van die straffen alleen.

euros ou d'une de ces peines seulement.

§ 7
Celui qui, sachant que des données ont été obtenues par la commission d'une des infractions visées aux §§ 1er à 3, les détient, les révèle à une autre personne ou les divulgue, ou fait un usage quelconque des données ainsi obtenues, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à cent mille euros ou d'une de ces peines seulement.

§ 7
He who, while knowing that the data were obtained by committing an offense described in §§ 1 to 3, retains these data, reveals or spreads these data to another person, or makes any use of it, is punished with imprisonment of six months to three years and a fine of twenty-six euro to a hundred thousand euro or with one of these penalties.

List of relevant literature on the matter:

- BALLON, G., "Know-how en zijn bescherming", in *Liber Amicorum R. Blanpain*, Brugge, Die Keure, 1998, 673;
- CORNIL, L., WYCKAERT, M., GRENSON, C., DE BAUW, H., DEWANDELEER, D., "Het zakengeheim: een voorstelling in vier bedrijven", *Cah.jur.* 2011, afl. 1, p. 5.;
- KEUSTERMANS J. en MOLS F., "De wet van 28 november 2000 inzake informaticacriminaliteit : een eerste overzicht", *RW* 2001-02, nr. 21, 727;
- On Belgian criminal law in general: see C., VAN DEN WYNGAERT, *Strafrecht, strafprocesrecht & internationaal strafrecht in hoofdlijnen*, Antwerpen, Maklu, 2006, 1314 p.

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

Under general criminal law, both a moral element (mental state or *mens rea*) and a material element (conduct *actus reus*) are required for establishing a criminal offence. This means that, to establish trade secrets violation as a criminal offence, the illegitimate disclosure must have taken place and the offender must have acted purposely, knowingly, recklessly, or negligently. Disclosure out of mere indiscretion, carelessness or ignorance will however not suffice.

The moral element (*mens rea*) is thus available when the accused, by the disclosure of a trade secret, wished to provide himself with an unlawful income that he would not have had if he had not committed the crime[4]. The pursuit of other specific purposes, such as

[4] Antwerp Court of Appeal, 31 March 2009, *ICIP* 2009, vol. 1, 133.

harming competitors or obtaining advantages from the use, will probably satisfy the condition of *mens rea*.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

The violation of trade secrets entails other criminal offences (as discussed above).

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

The alleged offender will not be prosecuted if he is able to demonstrate that one of the constitutive elements of a criminal offence has not been fulfilled (e.g., that the secret trade cannot be considered as such because the information is public).

The offender may also invoke a defence (similar to *"just cause"*) if there are certain conditions under which he may not be prosecuted, including circumstances where the violation results from a public order, the law, legitimate defense, state of emergency, irresistible coercion or insanity[5].

A *"de minimis threshold"* may also be applied by the Public Prosecutor in the framework of a prosecution policy, i.e., when deciding whether or not to prosecute an offence. The accused can however not invoke this as a defence in criminal court proceedings. Neither does a "fair use" defence exist under Belgian criminal law.

There is no case law available where any of these "safe harbor" clauses have been invoked with respect to abuse of trade secrets.

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

An attempt to illegitimately disclose trade secrets can be prosecuted. The risk of dissemination or disclosure of trade secrets as such will however not suffice and cannot therefore give rise to criminal liability.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

Belgian criminal law distinguishes:

(i) illegitimate disclosure of manufacturing secrets by a (former) employee

This only applies to the illegitimate disclosure to a third party of manufacturing secrets by a (former) employee (or civil servant) with fraudulent intent.

(ii) violation of the professional privilege

This only applies to medical doctors, surgeons, health officers, pharmacists, midwives and all other persons who by virtue of their status or profession have knowledge of secrets entrusted to them (e.g., attorneys), and disclose those secrets.

(iii) theft

[5] See, *inter alia*, Articles 70-71 Criminal Code.

The main limitation here lies in the fact that the stolen good must be tangible and movable. Hence, the theft of non-materialized (intellectual) rights is in principle not covered by this provision. However, when incorporated in a material carrier (for example, in a written document or an IT- data carrier), the theft may still be considered as theft. If the thief is an employee, this constitutes an aggravating circumstance.

(iv) abuse of confidence

This also only applies to business secrets that are physically incorporated into documents, data carriers or other tangible property.

(v) abuse of corporate assets

A conviction for abuse of corporate assets is only possible if committed by directors, in fact or in law, civil and commercial companies, or non-profit associations. Third parties such as competitors, which are not directors of the injured company, can still be prosecuted as (co-)offender (e.g., provocation) or accomplice to the crime committed by a director.

(vi) bribery

Bribery includes both passive and active bribery and punishes the non-permissible publication of any type of business secrets, including non-materialized secrets.

(vii) hacking

This applies to both the offender and any person encouraging or instructing to commit the act of hacking. The sanctions will vary depending on the type of hacking (internal or external) and whether there is fraudulent intent.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

The threshold for establishing trade secrets violation under intellectual property law rules is generally lower. For example, the mere illegitimate disclosure of a trade secret can be remedied under civil litigation but not under criminal law where, in a claim based on Article 309 Criminal Code, it must be demonstrated that the trade secret has been disclosed to a third party and with fraudulent intent. In addition, whereas disclosure out of mere indiscretion, carelessness or ignorance will not suffice to establish criminal liability, such disclosure can probably still be remedied under civil law (thus including commercial and intellectual property law) provisions.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

Depending on the legal grounds invoked, there may be limitations as to the items covered by legal protection of trade secrets. One must therefore carefully select the appropriate legal ground depending on the type and nature of the trade secret that has illegitimately been disclosed.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

The trade secret must be secret and belong to a person or a company. If a claim is based on Article 309 Criminal Code, the owner of the trade secret must also demonstrate that he has taken reasonable steps to keep it secret.

Patentability as such of the items covered by trade secrets will not impact on the extent of the protection granted by law. This results from the so-called negative reflex effect, according to which in the absence of an IP right, one may not claim protection as an IP right, even if the conditions for IP protection are fulfilled. In other words, in the absence of a patent, one may not claim protection as if a patent had been granted. This makes sense since patent protection comes with disclosure of an invention and is limited to 20 years. If, on the other hand, patent protection were granted without the need to obtain a patent, the need of disclosure and the time limitations could be circumvented.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Yes. The Anti-Piracy Act of 15 May 2007 (which implemented EU Regulation 1383/2003 of 22 July 2003 concerning customs action against goods suspected of infringing certain intellectual property rights and the measures to be taken against goods found to have infringed such rights) provides for criminal protection and sanctions against any person infringing a trademark, copyright or related right, design right, patent, supplementary protection certificate, plant variety right, protected designation of origin or protected geographical indication.

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

The Public Prosecutor may prosecute the offender *ex officio*. The holder of a secret may also introduce a claim. Introducing a claim is a procedure which is not very costly and is only limited to the drafting of the claim. Upon receiving the claim, criminal investigations can be initiated, but the initiative is left to the Public Prosecutor. After the investigation, it will again be the Public Prosecutor (or the examining magistrate if the investigation is passed on to him when certain investigatory measures need to be taken) who will decide whether the case will be referred to the criminal court or not.

Any party demonstrating an interest (i.e., standing to sue) may start proceedings and claim damages.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

The offence may be proved by any legal means, including confessions, testimonials, expert evidence, presumptions, etc. provided that these have been legally acquired.

Obviously, it must be demonstrated that the information that has illegitimately been disclosed constitutes a trade secret (or a manufacturing secret in case a claim is based on Article 309 Criminal Code) and that this secret has been abused.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets,

as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

In civil proceedings, an *ex parte* order to search premises and computer systems for misappropriated data and to require the defendant to provide information as to the whereabouts of documents and files containing such data is only available for infringement of an intellectual property right, thus excluding trade secrets.

In criminal proceedings, however, the examining magistrate has the widest investigative powers which implies that he can order all measures necessary, thus including ordering a search of the premises and computer systems for misappropriated data and requiring the defendant to provide information as to the whereabouts of documents and files containing such data. The holder may also ask the examining magistrate to order a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Pursuant to Article 5 Criminal Code, a company can be held criminally liable for criminal offences which either have an intrinsic connection with the achievement of the company's corporate purpose or the perception of its interests, or which, according to the circumstances, were committed on the company's behalf. The legislator did not specify the individuals or bodies for which a company can be held criminally liable. Certainly, the company's liability is not limited to criminal offences committed by its legal or statutory bodies.[6]

Therefore, the answer to this question is yes: companies may be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage.

2. If so, which type of liability arises for companies? Which penalties shall apply?

Criminal penalties with respect to companies include fines, the confiscation of goods, the order to stop the infringing acts (even if part of the corporate purpose), the (temporary) closure or even the winding up of the company (only in very severe cases)[7].

According to Article 41*bis*, §1 of the Criminal Code, when the law imposes a prison sentence and a fine, the company which has been convicted of a criminal offence must only pay a fine calculated as follows:

- minimum EUR 500 multiplied by the number of months of the minimum prison sentence. This amount may however not be lower than the minimum fine determined for that offence;
- maximum EUR 2,000 multiplied by the number of months of the maximum prison sentence. This amount may however not be lower than double the maximum fine determined for that offence.

[6] C., VAN DEN WYNGAERT, *Strafrecht, strafprocesrecht & internationaal strafrecht in hoofdlijnen*, Antwerpen, Maklu, 2006, p. 132.
[7] Article 7bis of the Criminal Code.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

Cases of liability of companies for trade secrets violations will be adjudicated by the Criminal Court (*correctionele rechtbank / tribunal correctionnel*)[8].

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

It depends on the legal ground invoked. A person invoking a violation of Article 309 Criminal Code must have taken all necessary measures with a view to protecting the manufacturing secrets vis-à-vis third parties. This can be done by requiring the employees of the company owning the secret to honour its confidentiality and sign a confidentiality clause. This also applies to former employees. However, since Article 309 Criminal Code does not apply to persons other than (former) employees, the latter cannot be pursued on this basis regardless of whether a specific obligation to keep secret the information has been expressed.

The other legal grounds (violation of the professional privilege, theft, abuse of confidence, etc.) do not require an express obligation to keep secret the information.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

No. The offender may be any individual or legal entity, including a competitor or potential competitor.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

Yes. In criminal proceedings, one can choose to either just draft the criminal complaint as 'injured party', or become a 'civil party' (*burgerlijke partij / partie civile*) which means that that party will be informed of the investigation (one can become 'civil party' from the beginning, when introducing the claim, or later on in the procedure if wanted). A civil party also has the right to suggest certain investigatory measures and will be heard when is decided upon referral to the criminal court. Being a 'civil party' gives a party more rights, but is also more costly because of the time spent in following up the investigation (looking in the criminal files and drafting a petition for additional investigatory measures if needed, attending the oral hearings in order to ask for referral of the infringer, etc.). Remedies include imprisonment and fines. In addition, if the offender is convicted, the holder of the trade secret who has chosen to become a 'civil party' may subsequently claim damages.

Any civil lawsuit will be temporarily suspended pending the final outcome in the criminal proceedings. This principle is known as 'le criminal tient le civil en état' and is expressed in Article 4 of the Preliminary Title of the Code of Criminal Procedure (*Voorafgaande titel van het Wetboek van strafvordering / Titre préliminaire du Code de procédure pénale*).

[8] Article 179 of the Code of Criminal Procedure (*Wetboek van strafvordering / Code d'instruction criminelle*).

Bulgaria

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

As will be demonstrated, criminal liability for trade secret violations is most underdeveloped among other types of legal redress (i.e. civil remedies in contract and tort). The *Criminal Code* does not specifically incriminate trade secret violations. There are however other more general crimes in the *Criminal Code* that may incorporate trade secret violations as well. Please note that there is no case law on trade secrets that is available through legal information providers in order to support the conclusion that the offences analyzed below would include trade secrets. In our opinion, few statutory offences may be used for the purposes of punishing trade secret violations. The conditions for conviction of each offence are examined below.

(i) Crimes against the Activities of the State and Other Entities

The conditions for conviction for disclosure of service/ office secrets under Article 284 of the *Criminal Code* require the following conduct and fault elements:

Conduct elements

- An official discloses to another person or publicly announces information, which has been entrusted to him/ her or being accessible by virtue of his/ her occupation;

- Such disclosure shall be to the detriment of the state, an enterprise, an organization or private person;

Fault elements

- The official acts with the knowledge that the information disclosed is a service/ office secret; and

- The official acts with direct intention.

Officials committing this crime are liable to imprisonment for a term not exceeding two years or probation. The *Criminal Code* contains an exhaustive definition of the term "*official*".

"*Official*" shall be construed as any person assigned to carry out against remuneration or for free, temporarily or permanently:

- The duties of office in a state institution, with the exception of persons who carry out activities related exclusively to material performance;

- Management, safeguarding or management of property belonging to others within a state enterprise, co-operative, public organization, other legal entity or sole proprietor, as well as a notary and assistant-notary, private enforcement agent and assistant private enforcement agent.

Accordingly, the term "official" may include virtually any person in charge of the management of a legal entity possessing trade secrets even though this would most often be a public official, not a manager or employee in a company.

Secondly, persons, who are not officials, but who commit the above conduct and fault elements, shall also be found guilty of a crime. For the purposes of the conduct elements, these persons shall work in a state institution, enterprise or public organization to whom information that represents a service secret has become known by virtue of their occupation.

Thirdly, if the conduct and fault elements above are committed by an expert, translator or interpreter with respect to information which has become known to him/ her in connection with a task assigned under the condition to keep the information secret, he/ she shall be guilty of a crime and be held liable to imprisonment for a term not exceeding two years or probation.

(ii) Business Bribe

Violations of trade secrets may also be criminally prosecuted under the provisions on "*business bribe*." On a rather general note, this would involve disclosure of information for something in return. The conditions for conviction for "*business bribe*" under Article 225c of the Criminal Code require the following conduct and fault elements:

Conduct elements ("passive bribery")

- A person carries on assignments for legal entities or sole-traders and he/ she requests or accepts financial or other advantage, which is not due, or accepts a promise for financial or other advantage, in return for performing or refusing to perform an activity in breach of his/ her responsibilities to carry out business activities; and

Fault elements

- Such persons shall act with direct intention.

Persons committing this crime are liable to imprisonment for a term not exceeding five years or a fine not exceeding BGN 20,000 (approx EUR 10,256).

On the other hand, a person offering a financial or other advantage may also be held liable to imprisonment for a term not exceeding three years or a fine not exceeding BGN 15,000 (approx EUR 7,629). He/ she has to act with direct intention ("*active bribery*").

These provisions may find application with respect to individuals, including but not limited to managers and/ or employees of a company, trade agents, trade intermediaries, shop assistants and/ or counter-parties in possession of trade secrets. In addition, any person offering the advantage in return for violation of a trade secret may also be held liable. The circle of persons in this respect is virtually unlimited.

Finally, individuals acting as intermediaries and therefore making arrangements for a business bribe to take place shall also be found guilty of a crime and be held liable to imprisonment for a term not exceeding one year or a fine not exceeding BGN 5,000 (approx EUR 2,564). They shall act with direct intention.

(iii) Computer Crimes

First, the conditions for conviction for "*Computer Crimes*" under Article 319a of the *Criminal Code* require the following conduct and fault elements:

Conduct elements

- A person copies, uses or obtains access to computer data in a computer system without permission, where such permission is required; and

Fault elements

- Such persons shall act with direct intention.

Persons committing computer crimes shall be guilty of a crime and be held liable to a fine not exceeding BGN 3,000 (approx. EUR 1,538).

In particular, whe an act characterized by the conduct and fault elements above has been committed with regard to information that qualifies as a state secret or a secret to another person/ entity protected by the law, the person committing such act shall be guilty of a crime and be held liable to imprisonment from a term of one to three years, unless a greater sanction shall be imposed.

In the event that severe consequences have resulted from commissioning the above crime, a person shall be held liable to imprisonment for a term of one to eight years.

Secondly, the conditions for conviction for "*Computer Crimes*" under Article 319e of the *Criminal Code* require the following conduct and fault elements:

Conduct elements

- A person discloses passwords or codes for access to a computer system or to computer data and as a result personal data or information, which qualifies as a state secret or secret of another entity that is protected by the law, has been disclosed; and

Fault elements

- Such persons shall act with direct intention. He/ she may also act with the purpose of obtaining some benefit.

A person committing the above conduct and fault elements shall be guilty of a crime and be held liable to imprisonment for a term not exceeding one year. Only where a person acts with the purpose of obtaining benefit or grave damages have resulted from the act, he/ she shall be liable to imprisonment for a term not exceeding three years.

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

In general, no special purpose is required in order to hold a person guilty of a crime for violation of trade secrets as shown in Part A, Section 1 above. However, a special purpose may be a condition for conviction resulting in a greater sanction as is the case for computer crimes (Article 319 e of the *Criminal Code*). Therefore, the requirement for demonstration of purpose is rather an exception.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

The criminal offences that violation of trade secrets may possibly entail are listed in Section 1 above. Apart from that, violations of trade secrets normally result in civil lawsuits in contract or tort law. Please refer to the respective chapeau of Part B of both the Competition and IP Law Questionnaire and Competition Law Questionnaire.

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

There are no specific "safe harbors" provided by law in the context of trade secrets. However, there are general rules that may be relied on as a defense in criminal proceedings.

(i) Lack of Crime (non-incrimination provision)

Article 9 (2) of the *Criminal Code* states that the conduct of an act, which although formally fulfilling conditions for conviction of a crime, may not be incriminated on the condition that such acts are not dangerous to society or the danger is manifestly insignificant. This provision operates as a *de-minimis* test that if successfully passed, would negate criminal liability.

(ii) Substituting Criminal for Administrative Liability

Article 78a of the *Criminal Code* provides that a person may be released from criminal liability by the court, by imposing an administrative sanction, which is a fine ranging from BGN 1,000 to BGN 5,000 (approx. EUR 512 to EUR 2,564), where the following conditions are satisfied altogether:

- The person is liable to imprisonment for a term not exceeding three years or less - when acting with intention, or imprisonment for a term not exceeding five years or less - when acting by negligence/ recklessness;
- The person had not been sentenced for a crime and had not been previously released from criminal liability pursuant to this section; and
- Any damages to property, which have been caused by the crime, have been restored.

Administrative liability may not substitute criminal liability in one of the following events:

- Inflicting severe body injuries or causing death;
- The person committing the crime had been intoxicated;
- Multiple crimes have been committed; or
- The crime was committed against a public authority/ official.

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

No, it may not. Crimes possibly related to trade secrets require an act to take place in order to fulfill the conditions for conviction of a particular crime. The mere existence of risk will not suffice. Please refer to Section 1 above to see the conditions for conviction of the crimes shown.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

In practice, the conditions for conviction of each crime under Part A, Section 1 above are framed in a way that personal qualities of the offender or the type of items protected make a difference among the crimes examined. Some basic characteristics of the conditions for conviction may provide for distinction of the crimes shown, as already implied.

First of all, "*Crimes against the Activities of the State and Other Entities*" do require a special capacity of the person committing the crime – he/ she shall be an "official." [1] As discussed above, there is an express definition of the term "*official*." Despite the fact that the term is broadly defined, it reduces the scope of application of the conditions for conviction – the person committing the crime shall have the capacity of an official.

Secondly, albeit "*Business Bribe*" does not require special capacity of the offender, the conditions for conviction imply that the offender holds a position allowing him/ her to disclose trade secrets (i.e. access to trade secrets shall be entrusted in first place).

Thirdly, "*Computer Crimes*" do require that the items (information) subject to the crime be suitable for storage in a computer system or data. This quality of the object protected makes the crime distinct from the other ones.

The very practical significance of the above distinctions is related to the conditions for conviction and the type, and severity, of the sanction that shall be imposed.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

As already discussed, trade secrets and intellectual property rights are two separate matters in principle.[2] This applies equally in the realm of criminal law as the *Criminal Code* does not incriminate trade secrets violations specifically. The *Criminal Code* is likewise not concerned with the notion of trade secrets at all. The code nevertheless prompts that trade secrets shall represent information of specific type in certain cases (i.e. for computer crimes it would be information storable in computer system/ data).

Therefore, it is only when trade secrets contain objects of intellectual property that may premise the protection of trade secrets as objects of intellectual property. Such protection would have nothing to do with the trade secrets themselves. It would be exclusively concerned with the objects of intellectual property as such.

In this context, certain conducts are prohibited under intellectual property law, which do not necessarily result in the criminal offences shown in Part A, Section 10 below. The most outstanding of these include:

Law on Registration of Patents and Utility Models

- Claims for establishment of the actual inventor;

[1] Please refer to Section 1 (i) "Crimes against the Activities of the State and Other Entities" above
[2] Please refer to Part A, Section 4 of the Commercial and IP Law Questionnaire

- Claims for establishment of the right to apply for registration of patents;

- Claims concerning the amount of royalties in cases of compulsory licensing.

These claims are generally heard by the Sofia City Court. Such claims may be brought before the court in the context of protection of useful models as well.

Law on Industrial Design

- Claims for establishment of authorship or joint authorship.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

No, there are no general limitations as to the items covered by protection of trade secrets. Only in the context of "*Computer Crimes*", an implied limitation may be found to exist as these crimes do apply to acts that are purported to deal with computer systems and/ or data. Trade secrets shall therefore represent information that may be stored in a computer system or data.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

Affirmative, in order to protect trade secrets as object of intellectual property law, they shall consist of and satisfy all the requirements for protection as such objects. Trade secrets on their own are not afforded legal protection as intellectual property. In particular, the patentability of items would be of crucial importance to the conditions for enforcement/ protection of intellectual property rights.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

As an extension to Part A, Sections 8 and 10 above, trade secrets may avail themselves to legal protection as objects of intellectual property on the condition that they consist of such objects (i.e. patents, useful models, industrial designs). To such an extent, trade secrets may be protected under the provisions of the *Criminal Code* on violations of intellectual property rights.

Plagiarism

The conditions for conviction for plagiarism under Article 173 (2) of the *Criminal Code* require the following conduct and fault elements:

Conduct elements

- A person submits for registration or registers in his/ her own name the invention, useful model or industrial design of another; and

Fault elements

- This person shall act with intention.

A person found guilty of a crime shall be liable to imprisonment for a term not exceeding two years or a fine of BGN 100 to BGN 300 (approx. EUR 51 to EUR 153), and public reproach.

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

Under the Bulgarian *Code on Criminal Procedure*[3] some offences are prosecuted upon the initiation of the prosecutor while others upon the petition of the sufferer. All crimes, cited in Part A, Section 1 above shall be prosecuted at the initiative of the public prosecutor.

Please note however that investigation shall be initiated on the condition that there is a statutory cause and provided that there is sufficient data that a crime has been committed. Pursuant to the *Code on Criminal Procedure* statutory causes giving rise to an investigation are: (i) a notification to the investigation authorities (those including the prosecutor) for a committed crime; (ii) information for a committed crime in mass media; (iii) confession of the offender before the investigation authorities; and (iv) immediate discovery of signs of a committed crime.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

As a general rule of criminal procedure, the burden of proof is with the prosecutor when crimes prosecuted upon the initiative of the prosecutor are concerned. There is no specific evidence to be brought before the investigation authorities and the court to prove that an abuse of trade secrets has occurred as this will to a great extend depend on the particulars of each case. Nevertheless, evidence that may be collected in criminal proceedings is exclusively and exhaustively provided for in the *Code on Criminal Procedure* (for example, material evidence, witness statements, documents, protocols for different investigation actions, expert opinions, etc).

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

The investigation authorities shall collect evidence *ex officio* or upon the request of interested parties. The court shall collect evidence upon the request of the parties to the proceedings or *ex officio*. In each case the competent authority is entitled to assign an inspection of areas, premises, movables and persons in order to examine and preserve traces of crime. Further, with the permission of the judge (both at the stage of investigation and the stage of court proceedings) a search of premises and computer systems and seizure of movables, documents and computer data may be performed. The offender may lawfully refuse to provide explanations and cannot be obliged to provide information as to the whereabouts of documents and files.

Ex parte orders aiming to cease the risk of further consequences arising from the misuse of trade secrets or precautionary seizure to avoid the continuation of the offence and the perpetuation of the consequences are not available under Bulgarian criminal procedure law, although the interested party in the investigation procedure, respectively, a party to

[3] Article 208 of the Code on Criminal Procedure

the court proceedings may extend such request to the investigation authorities/ the court.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Criminal liability of companies may not be invoked in Bulgarian law. It is only individuals that may be prosecuted for crimes in Bulgaria.

2. If so, which type of liability arises for companies? Which penalties shall apply?

Not applicable.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

Not applicable.

Cyprus

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Yes, there is criminal liability for trade secrets violation in Cyprus, though trade secrets are not defined in these legislative provisions. The general nature of this criminal liability involves the unauthorized disclosure of such information to third parties by any civil servant in the course of their official duties / investigations into the commercial activities of a company or an individual. The potential penalties are monetary fines and/or imprisonment (see the legislative provisions below). Legislation with such criminal provisions include the following:

(1) Commercial Descriptions Law 1987 – Law N. 5/87 – Consumer Protection Law.

(2) General Product Safety Law 2004 – Law N. 41(I)/2004– Consumer Protection Law.

(3) Competition Law 2008 – Law 13(I)/2008- Competition law.

(4) The Control of Concentrations Between Undertakings Laws 1999 to 2000 –

Competition Law.

(5) The Criminal Code (Chapter 154)- Law N. 167(I)/2011-Criminal Law.

The text of the relevant provisions (English translation from Greek original text) are as follows:

(1) Commercial Descriptions Law 1987 – Law N. 5/87

Article 26 (5):

"If any person discloses to another person-
(a) any information obtained from premises which he entered in accordance with this article and which concerns a manufacturing process or trade secret or
(b) any information which was obtained in the course of the enforcement of this Law, commits a criminal offence, unless the disclosure occurred during or for the completion of his or any other person's duties under this Law, and is subject to, if convicted, to imprisonment for a period not exceeding 12 months or a financial penalty which does not exceed 750 Cyprus Pounds [1275 Euros] or to both such penalties."

Please note that the persons referred to in this Law that can enter premises to enforce this Law (under Article 26(1) (a) & (b) of Law N.5/87) are those authorised by the Minister of Commerce, Industry & Tourism (under Article 24 of Law N.5/87) and these are usually government officers of the Consumer Protection Department of the Ministry of Commerce, Industry and Tourism.

(2) General Product Safety Law 2004 – Law N. 41(I)/2004

(Harmonising national law with EC Directive 2001/95/EC dated 3rd Dec. 2001 for general safety of products.)

"Article 36
(1) In accordance with the provisions of the above article, a person is guilty of a crime, if he discloses or allows to be disclosed any information which is covered by professional secrecy and which

(a) Has been obtained as a result of any person carrying out their duties imposed by the Regulations and Orders issued in accordance with this Law or any other provision of this Law or

(b) involves a secret manufacturing method or trade secret and which has been obtained from this whilst carrying out their official duties in accordance with the provisions of this Law.

(2) Sub-article (1) above is not enforceable for information which relates to product safety characteristics, which must be published, if the circumstances so dictate, so that the health and safety of consumers is protected.

(3) The protection of professional secrets does not prevent:

(a) Conveying useful information to the relevant authority from other state or not authorities and vice versa, in order to ensure the effectiveness of the control and supervision procedures of the marketplace:

It is implied that authorities which receive information which is covered by professional secrecy ensure that it is duly protected.

(b) the disclosure of information :

(i) for purposes of evidence in a criminal case which is pending in court

(ii) for purposes of protecting public health or other official purpose.

(4) A person who breaches any provision of this Article is guilty of a criminal offence and is subject to imprisonment which does not exceed 6 months or a monetary fine which does not exceed 1000 Cyprus Pounds [1700 Euros] or both such penalties."

The relevant authority here is the Consumer Protection Department of the Ministry of Commerce, Industry & Tourism and the officers carrying out their duties to enforce the provisions of this Law are the officers of Consumer Protection Department of the Ministry of Commerce, Industry & Tourism.

(3) Competition Law 2008 – Law 13(I)/2008

(To regulate and protect free competition in the Republic of Cyprus and enforce EC Reg. 1/2003 of 16/12/2002 to enforce the competition regulations in Articles 81 & 82 of the Treaty as amended by EC Reg 1419/2006 of 25/9/2006)

Article 33. –

(1) The President, the other members and the substitutes of the Committee, the persons who work under the supervision of the Committee, the employees of the Service and other civil servants who receive information as a result of their position or in the course of the exercise of their official duties, business secrets and confidential information, have

a duty of confidentially and are bound not to communicate and/or publicize such information except to the extent that they are obliged to do so-

> (a) to prove a breach of articles 3 and/or 6 of this Law and/or Articles 81EC and/or 82EC
>
> (b) to enforce the provisions of this Law

(2) The obligation of confidentiality is also imposed on any other natural or legal person who receives knowledge of such information during the course of the implementation of the foreseeable procedure covered by the present Law.

(3) Notwithstanding Article 38, breach of the confidentially obligations under this article constitutes, in the case of civil servants, a heavy disciplinary offence punishable under the relevant disciplinary rules.

(4) No provision of the present Law prevents the communication and/or publication of information for the purposes of the implementation of the European Competition Law.

Article 38: A person who breaches their obligation of confidentiality which is imposed by Article 33, commits a criminal offence punishable by imprisonment which does not exceed 1 year or with a monetary fine which does not exceed Euro 3,500 Euros and/or both of these penalties."

(4) <u>The Control of Concentrations Between Undertakings Laws 1999 to 2000</u>

Duty of Confidentiality

Section 51(1) – Any authorised officer or other public officer who acquires directly or indirectly knowledge of any matter in relation to a concentration, as a result of the application of any provision of this Law, may not disclose it to any person, unless when and to whoever it is necessary to do so for the execution of his duties.

Section 51(2)- Any person contravening the duty of confidentiality pursuant to subsection (1) shall commit an offence punishable with imprisonment up to six months or with a fine up to one thousand seven hundred and eight euros or with both such imprisonment and fine.

Schedule III (Section 15)- Information Required to be Included in the Notification of a Concentration:

> (7) Confidentiality- Where any of the information included in the notification is regarded as confidential by the parties of the concentration, this must be marked as confidential and the reasons justifying such confidentiality must be mentioned. Such information may, in exceptional cases, be given in a separate envelope and due reference must be made thereto in the text of the notification.

(5) <u>The Criminal Code (Chapter 154)- Law N. 167(I)/2011</u>

Section 135(1): A public servant who publishes or discloses information or facts which he has been informed or a document which he received due to his official position and which he has a duty to keep confidential except to the person to whom he has a duty to publish or notify this information is guilty of a misdemeanour [minor] crime.

S. 135(2): A public servant who without lawful authority excludes or copies a document which belongs to his employer is guilty of a misdemeanour and is subject to a fine which

does not exceed 1000 Cyprus Pounds [1700 Euros] or to imprisonment which does not exceed one year and/or both these penalties.

S. 135(3): Any person who is not legally authorised for this, who discloses in any manner a state secret is guilty of a misdemeanour.

For the purposes of this section, "state secret" includes any document, information or circumstance whose disclosure would harm the security or the economy or generally the interests of the Republic of Cyprus or public order or generally the public interest and the knowledge of which by its nature, must not be extended beyond the limited circle of government bodies, authorities or services.

S. 135(4): A criminal prosecution for the crime set out in this section is exercised only by the Attorney General of the Republic or with his consent.

S. 135(5): For the purposes of this section the term "public servant" has the definition accorded by section 4 of this Law namely "a person who serves in the civil service".

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

No, the relevant legislative provisions do not establish any specific requirements as to the purposes that the infringer may necessarily pursue to be criminally liable for the disclosure of trade secrets, for example harming competitors or obtaining advantages from their use.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

Under the current legislative provisions in Cyprus, depending on who violates trade secrets the person can face either criminal offences and/or be faced with a civil lawsuit. If the person who violates a trade secret is a civil servant, there are various criminal provisions in current legislation which make such a person liable to a criminal offence facing monetary fines and/or imprisonment if convicted by the court (see our answers to Q1 above). If the person who violates a trade secret is not a civil servant but an employee in a company who discloses his company's trade secrets to a third party he is more likely to face a civil action by his employer for breach of his employment contract (the relevant confidentiality clause) or breach of his non-disclosure agreement (if applicable).

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "fair use", "just cause", "de minimis threshold")?

References to trade secrets in existing legislation are not defined and the primary focus of such legislation is not the protection of trade secrets. In this context, there do not appear to be any current provisions establishing "safe harbor" clauses. Nevertheless, there are some "just cause" provisions where a civil servant may disclose trade secrets and/or confidential information for example:

(a) General Product Safety Law 2004 (Law N. 41(I)/2004) Art. 36 (2) & (3) (see full details of this legislation in our answer in Q1 above) which permits the disclosure of trade secrets (in the form of product safety characteristics) by a civil servant (officer of

the Ministry of Commerce) "if the circumstances so dictate, so that the health and safety of consumers is protected" (Art. 36 (2)) and "conveying useful information" to another state "in order to ensure the effectiveness of the control and supervision procedures in the marketplace" (Art. 36 (3)(a)) and the "disclosure of information... for purposes of evidence in a criminal case which is pending in court [and] for purposes of protecting public health or other official purpose" (Art. 36 (3)(b)(i) & (ii)).

(b) Competition Law 2008 (Law 13(I)/2008) Art. 33 (1) & (4) (see full details of this legislation in our answer in Q1 above) which permits the disclosure of "business secrets and confidential information" in order to " prove a breach of articles 3 and/or 6 of this Law and/or Articles 81EC and/or 82EC" and in order to "enforce the provisions of this Law" (Art. 33 (1)) and disclosure of such information " for the purposes of the implementation of the European Competition Law" (Art. 33 (4)).

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

Technically, under the current criminal provisions in legislation, criminal liability exists where actual dissemination or disclosure of trade secrets occurs to any third party (one or more individuals or commercial entities) and not where there is merely a risk of dissemination or disclosure.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

There are currently no distinctions in the legislative provisions as to different types of trade secret violations and the criminal penalties (monetary fines and/or imprisonment) apply to any trade secret violation by a civil servant as described previously (subject to the "just cause" exceptions outline in our answers to Q4 above).

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

Intellectual property infringements (e.g. trademarks, patents and designs) are civil law matters covered by the civil law, where the evidential standard of proving the infringement is of a lower (easier) standard (balance of probabilities) than that in a criminal case (beyond a reasonable doubt). Hence the current legislative provisions that make it a criminal offence for civil servants to disclose trade secrets cannot be compared to the requirements provided for by intellectual property law. In any case, trade secrets and confidential information are not protected by intellectual property law in Cyprus.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

No, though there are currently no definitions of trade secrets in the legislative provisions nor details as to the format that such trade secrets can be in (e.g. documents, know-how, ideas etc).

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

No specific requirements are provided for by the current legislative provisions, in order to be legally protected.

No, the patentability of items covered by trade secrets does not impact on the extent of legal protection as far as the current legislative provisions are concerned. The court hearing a civil case (employer/employee) involving unauthorized disclosure of trade secrets may of course take into consideration that the items covered by trade secrets may also be patentable in deciding the level of damages, though we are not aware that such considerations have arisen yet in existing local case law.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

No, there is currently no criminal protection of other IP registered rights such as patents and trademarks.

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

The equivalent of the Public Prosecutor here is the Attorney General's Office. If the offender breaches the relevant criminal provisions, he can be prosecuted if the Attorney General's Office decides that there is enough evidence to warrant a successful criminal prosecution.

The holder of a secret is not required to file a report of the offence with the Attorney General's Office in order to start a criminal prosecution and thus enforce a trade secret violation.

It is not applicable that only certain subjects are entitled to start a proceeding and/or claim any damages.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

In a criminal prosecution, there is no specific evidence to be brought to court in order to substantiate a disclosure of a trade secret according to the current legislative provisions.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

In a criminal proceeding, a search warrant can be issued by the court to the police (not to the holder of a trade secret) to carry out these actions.

The holder of a trade secret can apply for an ex parte court order (Anton Piller-style order) to search premises and seize evidence without prior warning to the defendant and require the defendant to provide information as to the location of documents and files containing such data only in the context of civil proceedings.

In a criminal proceeding, the police can request the court to issue them with the equivalent of an ex parte injunction against the defendant to stop the risk of further disclosure/misuse of trade secrets.

The holder of a trade secret, may apply for an ex parte injunction to stop the risk of further disclosure/misuse of trade secrets only in the context of civil proceedings.

The holder of a trade secret in a civil proceeding can also apply to the court for a Mareva injunction (on its own or in combination with an Anton Piller order) which enables the applicant to have the defendant's assets frozen so they cannot be dissipated to frustrate the court judgment. This can be very damaging to a defendant as the overall effect of court granting a Mareva injunction and/or an Anton Piller order against the defendant is to destroy a business' day-to-day operation by freezing most of its assets and potentially revealing important information to its competitors.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

In general, companies as legal persons can be defendants or plaintiffs independent of their agents, employees etc. Companies and their agents, employees etc can be joint defendants.

Although current legislative provisions do not make specific reference to legal persons (companies and their representatives) being liable for trade secret violations, Section 14 of Law N. 22 (III)/2004 (Law Implementing The Treaty of the Council of Europe Against Internet Crime Signed in Budapest on 23.11.2001) states that companies (and their legal representatives such as all the Board of Directors and/or individual Directors and/or the Managing Director) can all be jointly liable for any actions which are defined as crimes under this law for example illegal access (e.g. computer hacking) or misuse of computer data and systems (databases) etc. Trade secret violations are not specifically mentioned under this Law but could easily be included under these crimes.

Specifically, in our legal research we had meetings with the Internet Crime Unit at Police Headquarters and they informed us that a recent pending criminal case which arose in February 2012 involving the theft of trade secrets (client contact data stolen from computer server) from a financial services company by another competitor company is being prosecuted under Law N. 22 (III)/2004 (Law Implementing The Treaty of the Council of Europe Against Internet Crime Signed in Budapest on 23.11.2001)

2. If so, which type of liability arises for companies? Which penalties shall apply?

In the context of our answer in Q1 above, Section 13 of Law N. 22 (III)/2004 provides that any person who commits any of the crimes prohibited by this Law can be punished with imprisonment not exceeding 5 years and/or a monetary fine up to 20,000 Cyprus Pounds (34,000 Euros).

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

The local Criminal District Court as the first instance court and the Supreme Court as the appeal court.

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

No, there is no specific obligation to keep secret the information to be expressed in order for a trade secret violation to occur. Usually trade secret protection focuses on employees of the company owning the respective trade secret. There is though, a distinction between this scenario (usually dealt with by non-disclosure clauses in employment contracts of such employees) and other scenarios involving persons other than employees, for example public sector employees who come across trade secrets in the course of their investigations into a company (eg investigations by officers at the CPC and the Ministry of Commerce, Industry & Tourism).

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

No, this is not required. For example, public sector employees working in government departments that come across trade secrets in the course of company investigations are prohibited from publicly disclosing such information by various national legislative criminal provisions referred to previously and also by various internal administrative procedures relating to public sector employees.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

Any claim for damages that the aggrieved person (or company) wishes to bring is usually included in a civil lawsuit for compensation and this civil process is separate from any prior or concurrent criminal proceeding brought against any person (e.g. public sector employee) disclosing a trade secret.

Any conviction in a criminal case can be used as evidence in a subsequent civil case.

Czech Republic

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Yes; criminal liability exists in the Czech Republic for trade secrets violations in economic competition. Pursuant to Article 248 (1) h) of Act No. 40/2009, Coll., as amended, Criminal Code ("Criminal Code"), a person who, participating in competition, commits an act of unfair competition (as defined under Act No. 513/1991, the Commercial Code, i.e. conduct in contradiction of good practices of competition which is capable of causing damage to other competitors or consumers) by infringing upon trade secrets and causes damage of or in excess of CZK 50,000 (approx. EUR 2,000) to other competitors or to a consumer or equips someone with unjustified benefits in this amount or greater, shall be punished with up to three years imprisonment, a statutory fine of up to CZK 36.5 million (approx. EUR 1.5 million) or forfeiture of property. The same punishment can be imposed upon a person that has concluded an agreement violating competition, causing by such action a disadvantage of higher extensity to other competitors or to a consumer or equipping somebody with unjustified benefits of a higher extensity. More severe penalties (imprisonment up to 5 or even 8 years) are available in case of aggravating circumstances (such as larger extent of damage or unjustified benefit, repeated offense, causing insolvency of the aggrieved party), etc.

This criminal offense cannot be committed by a legal entity; only a natural person (individual) can commit this crime. This does not, however, exclude criminal liability of executives or board members of a legal entity for such offense.

The legal values protected are the general interest on protection of the rules of economic competition and fair competition.

Relevant literature on this matter:

J. Jelínek and Co. *Substantial Criminal Law*. Leges, 2010
= J. Jelínek a spol. *Trestní právo hmotné*. Leges, 2010

Šámal and Co. *Criminal Code II Commentary.* 2010
= Šámal a spol. *Trestní zákoník II komentář.* 2010

A. Nett, *"Dominant Position Abuse as a Criminal Offence"*, Criminal Law, Issue 3, p. 24, March 2007
= A. Nett, *"Zneužití dominanntího postavení na trhu jako trestný čin"*, Trestní právo, Issue 3, p. 24, March 2007

A. Nett, "*About Changes of the Criminal Law in the Field of Economic Criminal Activities and about the Rule of Ultima Ratio*", In: J. Jelínek. On a New Criminal Code. Anthology from an International Scientific Conference Juridical Days of Olomouc. Leges, 2009, p. 114
= A. Nett, "*Ke změnám trestního práva na úseku hospodářské trestné činnosti a k zásadě ultima ratio*", In: J. Jelínek. O novém trestním zákoníku. Sborník z mezinárodní vědecké konference Olomoucké právnické dny. Leges, 2009, p. 114

F. Púry, "*Comments to the Statutory Regulation of the Economic Criminality in the Czech Republic*", Trestní právo, Issue 9, p. 11, September 2000

= F. Púry, "*Poznámky k právní úpravě hospodářské kriminality v České republice*", Trestní právo, číslo 9, p. 11, September 2000

J. Teryngel. *About Criminal Liability of the Enterpreneur*. Orac, 1998
= J. Teryngel. *Nad trestní odpovědností podnikatele*. Orac, 1998

J. Teryngel, "*About the Punishment of Economic Criminal Offences in the New Criminal Code*", Criminal Law, Issue 6, June 2009, p. 12
= J. Teryngel, "*K postihu hospodářských trestných činů v novém trestním kodexu*", Trestní právo, Issue 6, June 2009, p. 12

Zbyněk Žďárský, "*Civil and Criminal Law Context of Unfair Competition and Protection thereof*", Trestněprávní revue, Issue 12, December 2003, p, 352
= Zbyněk Žďárský, "*Civilněprávní a trestněprávní souvislosti nekalé soutěže a ochrany proti ní*", Trestněprávní revue, Issue 12, December 2003, p, 352

Pavel Šámal, "*Unfair Competition and the Possibilities of its Punishment according to the Effective Statutory Regulation and according to the Effect of the New Criminal Code*", In: Anthology XVII. Juridical Days of Karlovy Vary. Linde, 2009, p. 292-304
= Pavel Šámal, "*Nekalá soutěž a možnosti jejího postihu podle platné úpravy a za účinnosti nového trestního zákoníku*", In: Sborník XVII. Karlovarské právnické dny. Linde, 2009, p. 292-304

P. Šámal, F. Púry, A. Stolář, I. Štenglová. *Entrepreneurship and Economic Criminality in the Czech Republic*. C. H. Beck, 2001
= P. Šámal, F. Púry, A. Stolář, I. Štenglová. *Podnikání a ekonomická kriminalista v České republice*. C. H. Beck, 2001

P. Šámal. *Outline of the Criminal Code 2004-2006.* C. H. Beck, 2006, p. 235-236
= P. Šámal. *Osnova trestního zákoníku 2004-2006.* C. H. Beck, 2006, p. 235-236

A. Stolář, P. Šámal, F. Púry, I. Štenglová. "*Criminal Activity in the Czech Capital Market and Banking Sector*." Booklets of the Ministry of Justice of the Czech Republic, Volume 58. Institute for Further Education of Judges, 1998
= A. Stolář, P. Šámal, F. Púry, I. Štenglová. "*Trestná činnost na českém kapitálovém trhu a v bankovní sféře*." Příručky Ministerstva spravedlnosti ČR, Volume 58. Institut pro další vzdělávání soudců, 1998

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

The infringer must have the deliberate intention necessary to commit this offence - and his actions must result in damage of or in excess of CZK 50,000 (approx. EUR 2,000) to other competitors or to a consumer, or he must equip someone with unjustified benefits in or in excess of the above amount. Such damage or unjustified benefit must be included in the offender's intention. If such intentional conduct does not lead to damages in the level stipulated above, it may be considered as attempted violation, which is generally sanctioned the same way as a fully committed offense.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

Under specific circumstances, violation of trade secrets may also constitute the following offenses: infringement of secrecy of messages being delivered, insider trading, infringement of secrecy of documents kept in privacy, unauthorized access to a

computer system and to a data carrier, provision and storage of an access-device and a password to a computer system and other similar data or, as the case may be, negligent damage of an entry in a computer system and in a data carrier as well as damage to the facilities of a computer.

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

As regards the infringement of trade secrets pursuant to Article 248 (1) h) of the Criminal Code, this is only regarded as committed if damages result in or in excess of the amount of CZK 50,000 (approx. EUR 2,000) to other competitors or to a consumer, or someone must have been equipped with unjustified benefits in or in excess of this amount.

In addition, there are several general principles leading to non-prosecution for an infringement. Leading these is the principle of subsidiarity of criminal punishment, which provides that responsibility for a criminal offense shall be applied only in socially harmful cases and where the available sanctions under civil or administrative law would not be sufficient.

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

The risk of dissemination of a trade secret may, under certain circumstances, constitute the offense described in Sections 1 or 3, particularly in cases where such risk of dissemination was created by the offender in an attempt to violate the trade secret. Such attempted violation is generally sanctioned under the same rules as the fully committed offense.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

The Commercial Code describes in its Article 51 different types of violation of trade secrets.

According to this Article:

"Infringement of a trade secret involves acts whereby an acting person unlawfully informs another person about a trade secret, or provides him with access to it, or exploits it for his own or another person's benefit, if such trade secret can be made use of in competition, and of which the acting person learned:

(a) as a result of having been entrusted with that secret, or by having gained access to it otherwise (e.g. through technical documentation, instructions, drawings, models or patterns) on the basis of an employment or other relationship with the competitor, or while performing a function to which the individual was appointed by a court or some other authority; or

(b) through his own or another person's unlawful acts."

Violations generally do not differ according to the personal qualities and the type of items covered by trade secrets; they, however, differ according to the damage caused (please see Section 1 above).

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

Both Czech Intellectual property law and Criminal Law refer to the same definition of trade secrets in the Commercial Code as described above.

However, violation of a trade secret will only amount to a criminal offense if it is intentional and if it resulted in damage of or in excess of CZK 50,000 (approx. EUR 2,000) to other competitors or to a consumer or someone was equipped with unjustified benefits in or in excess of this amount.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

Trade secrets are construed very broadly under Czech Law. Trade secrets are all facts of commercial, manufacturing or technical nature relating to business which have real or at least potential material or immaterial value, are not generally accessible in relevant business circles, and shall, according to the will of the entrepreneur, be undisclosed - and where the entrepreneur secures that they remain secret by appropriate means.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

Please see Section 9 for the description of a trade secret; any trade secret fulfilling these requirements is subject to legal protection.

Criminal protection of protected industrial rights (patents) is stricter than protection of trade secrets. Breach of a trade secret constitutes a criminal offense only when damage or unlawful profit of or in excess of CZK 50,000 (approx. EUR 2,000) occurs, while the breach of a patent constitutes a criminal offense when it results in damage in excess of CZK 5,000 (approx. EUR 200).

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Yes; criminal protection of trademarks, business names, appellations of origin, geographical indications, patents, utility models, industrial designs, topography of semi-conductor products, copyright and database rights exists in the Czech Republic.

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

The Czech Police and State Attorney should generally initiate proceedings *ex officio*. In practice, the Public Prosecutor would have only limited means to discover violations of a trade secret without criminal complaint from the trade secret holder.

The aggrieved party has the right to participate in criminal proceedings as an ancillary participant and claim damages from the offender.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

There is no specific evidence proving an abuse of trade secrets. According to the law, any legally gathered evidence capable of establishing the facts of case may be applied. Generally, it would have to be established that a trade secret conforming to the requirements set out in Section 9 above was illegally and intentionally violated by the accused person in order to establish his or her criminal liability for such offense.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

The holder does not have any of the aforementioned rights. The holder may, nevertheless, turn to a court with a petition to supplement evidence in civil proceedings, including a proposal for such searches. However, in criminal proceedings it is for the state attorney/court to decide whether these searches will be carried out.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Companies cannot be found liable for a trade secret violation. However, they may be found liable for certain other criminal offenses, as described under Section 3 above.

2. If so, which type of liability arises for companies? Which penalties shall apply?

Generally, companies may be punished by dissolution, forfeiture of assets, statutory fine, forfeiture of a thing or other assets, ban on activity, prohibition against performance of public orders and against participation in proceedings of concession or of public order, and/or prohibition against accepting the subventions or by publishing of the judgment.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

Criminal proceedings against companies are carried out by criminal courts.

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

No such specific obligation is required for a trade secret violation to occur. Provided that all characteristics of trade secret violation are fulfilled (as discussed above) there is also no distinction based on the types of offenders and their relations to the aggrieved party.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

The offender must at least somehow be participating in the competition to be held liable for this criminal offense. The courts usually tend to interpret the competition relationship very broadly, taking into account all specific circumstances of the case. It is generally understood that the offender may be direct, indirect, future or potential competitor or acting for such competitor. The offender does not even have to be an entrepreneur. There may also be so called "ad hoc competition relationship", extending to cases where the offender and the aggrieved party are normally not competitors, however, have to be viewed as competitors under the circumstances of the specific case.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

The aggrieved party may bring a claim for damages in criminal proceedings unless the civil court has already decided his/her claim in the civil proceedings and the decision is final and effective. The procedural deadline for such claim is the start of taking evidence by the criminal court (which usually occurs on the first court hearing). The civil court may subsequently stay the civil proceedings until the claim is decided in the criminal proceedings, on the other hand, the criminal proceedings will not be stayed based on the parallel civil proceedings. In any case the damages based on the same facts can be awarded only once and therefore, if the criminal court already awarded damages and the decision is final and effective, the civil court would have to dismiss the damages claim based on the same facts

Denmark

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Yes, the Criminal Code (in Danish, "straffeloven") and the Marketing Practices Act (in Danish, "markedsføringsloven") cover the unauthorized appropriation and misuse of trade secrets.

The Criminal Code, Section 263 covers the illegal access to certain information, including trade secrets. This provision also covers the "secrecy of the mails".

Section 264(1) of the Criminal Code covers breaking and entering. If the breaking and entering is done with the intent of obtaining trade secrets, then it is an aggravating circumstance covered by subsection 2.

Section 19 of the Marketing Practices Act covers the unauthorized appropriation and misuse of trade secrets.

Ordinary violations of Section 19 are subject to criminal liability under the Marketing Practices Act section 30(4) on the request of the injured party. The punishment under this provision is financial penalty or imprisonment for a maximum of 1 year and 6 months.

Grave violations also constitute a violation of section 299a of the Criminal Code, referring to section 19 of the Marketing Practices Act. The punishment under this provision is imprisonment for a maximum of 6 years.

The injured party may claim damages for violation of the Criminal Code.

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

With the abovementioned exception of breaking and entering, the provisions contain no requirements as to the purposes of the infringer.

Criminal liability under Section 263, 264 and 299a of the Criminal Code requires intent, whereas criminal liability under Section 30 of the Marketing Practices Act requires negligence; see Section 19 of the Criminal Code.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

As mentioned above the violation of trade secrets may entail obtaining illegal access to trade secrets and/or breaking and entering.

In most cases, however, violation of trade secrets results in a civil lawsuit without any criminal charges; see the answers to the "commercial and IP law questionnaire".

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "fair use", "just cause", "de minimis threshold")?

No, see item 1 and 2.

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

As a main rule intent is a precondition to criminal liability. Nevertheless, under certain circumstances the sole risk of dissemination or disclosure of trade secrets may give rise to criminal liability under section 19 of the Marketing Practices Act or Section 263, 264 or 299a of the Criminal Code, provided that the risk is significant and is caused by the negligence of the employee.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

See item 1.

The Subsections of Section 19 of the Marketing Practices Act covers different types of trade secret violations:

(1); undue appropriation of trade secrets in a contract of service or in the performance of assignments.

(2), (3) and (4); undue use or passing on of duly appropriated trade secrets.

(5); Tradesmen's use of trade secrets acquired in conflict with Subsection (1)-(4).

Said violations are not treated differently by the law. However, grave violations are covered by the Criminal Code Section 299a.

The Criminal Code, Section 263(3) covers the illegal access to certain information, including trade secrets and Section 264(2) covers breaking and entering with the intent of obtaining trade secrets.

The maximum punishment under said provisions of the Criminal Code is 6 years of imprisonment.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

See item A1 and A2, Ordinary violations of Section 19 are subject to criminal liability under the Marketing Practices Act section 30(4) on the request of the injured party. The punishment under this provision is financial penalty or imprisonment for a maximum of 1 year and 6 months.

Grave violations also constitute a violation of section 299a of the Criminal Code, which refers to section 19 of the Marketing Practices Act. The punishment under this provision is imprisonment for a maximum of 6 years.

Criminal liability under Section 263, 264 and 299a of the Criminal Code requires intent, whereas criminal liability under Section 30 of the Marketing Practices Act requires negligence; see Section 19 of the Criminal Code.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

No.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

No, a number of different types of trade secrets are recognised in Denmark. Accordingly, trade secrets within the meaning of Section 19 of the Danish Marketing Practices Act comprise (i) operating and technical secrets, e.g. engineering and application of technical equipment, drawings, receipts, etc., and (ii) commercial secrets, e.g. formation of commercial relationships, customer lists, price calculations, etc.

However, only specific and concrete information will be protected, and the categorization as a trade secret presupposes that the information in question is of significant importance to the enterprise and that only a limited number of the enterprises' employees are familiar with this information. Information known by a larger part of the employees or by the relevant sector of trade will not be considered a secret. The business itself will to a large extent have influence as to whether or not information can be considered a trade secret.

The term "trade secrets" within the meaning of the Danish Criminal Code is interpreted in line with the term in Section 19 of the Danish Marketing Practices Act. A trade secret is not per se considered intellectual property, but if the trade secret fulfils the conditions for protection under the ordinary intellectual property laws, protection under said laws is available.

The patentability of the items covered by trade secrets does not have an impact on the extent of the protection granted by law.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Yes.

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

Ordinary violations of Section 19 are subject to criminal liability on the request of the injured party; see the Marketing Practices Act, Section 30 (4). Grave violations also constitute a violation of the Criminal Code, Section 299a. It does not require the request of the injured party for the public prosecutor to commence criminal proceedings for violation of Section 299a, but in practice, such a request is always filed.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

No, the ordinary rules apply

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

No, the injured party does not have this remedy at hand. The access to obtain ex parte orders to search premises - see the Administration of Justice Act, Chapter 57a (implementing Directive 2004/48/EC on the enforcement of intellectual property rights, article 8) - only applies to the "ordinary" IP rights such as copyrights, patents, trademarks etc., not including mere trade secrets.

However, the Danish Administration of Justice Act chapter 73 covers searches by the police in criminal investigations. As part of the investigation the police may under certain conditions inter alia search premises and computer systems for misappropriated data. Danish law however, recognizes the Defendant's privilege against self-incrimination, meaning the right to remain silent. The Defendant may therefore not be required to provide information as to the whereabouts of documents and files containing such data, provided it contains a risk of self-incrimination.

It is possible to obtain an interim injunction against the misuse of trade secrets by filing an application with the Bailiff's Court of the local jurisdiction where the defendant is established. The proceedings are not ex parte, but quite fast.

The plaintiff must render probable that the defendant is misusing trade secrets, which the plaintiff can enforce. Further, the plaintiff must render probable that the defendant will continue to carry out the infringing acts and that the purpose of the action would be lost if the plaintiff had to resort to ordinary court proceedings. Finally, the plaintiff must render probable that the general rules of law on penalties and damages and possibly provision of security offered by the defendant do not provide adequate protection of the plaintiff. The Bailiff's Court may refuse to grant an injunction if the damage or inconvenience inflicted on the defendant is in obviously disproportion to the plaintiff's interest in the injunction being granted.

In practice, the plaintiff must file the application within approximately one year from learning about the infringement. If it is rendered probable that the defendant is misusing the trade secrets and will continue to do so (in the lack of an interim injunction), then the interim injunction is normally granted.

The interim injunction can be obtained also if ordinary civil proceedings have been commenced.

Violation of an interim injunction is subject to criminal sanctions under the Administration of Justice Act.

If an interim injunction is obtained, the plaintiff must commence confirmatory proceedings on the merits.

The above conditions and procedures for obtaining an interim injunction are of a general nature and are not special for violation of trade secrets.

As part of an ordinary civil case, the plaintiff can obtain a permanent injunction; see the Marketing Practices Act, Section 20 (1). The permanent injunction will normally be limited in time to 2-3 years from the commencement of the in-fringing actions - however, this is a concrete assessment based on the specific circumstances.

The plaintiff can also obtain damages and a reasonable fee from the defendant for the violation; see the Marketing Practices Act, Section 20 (2), (3) and (4).

The above remedies are cumulative.

The Danish Administration of Justice Act chapter 74 covers seizure in criminal law. Under section 801(1) (3) seizure may be made in order to ensure the injured party' claim of restitution.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Yes, under Section 30(6) of the Marketing practices Act, referring to chapter 5 of the Criminal Code.

2. If so, which type of liability arises for companies? Which penalties shall apply?

Companies can be punished by financial penalties only, see Section 25 of the Criminal Code.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

The ordinary courts adjudicate cases of liability. Cases of liability of companies entail no difference in respect to which courts may adjudicate the cases.

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

No, but if the obligation of secrecy has been expressed it may be considered an aggravating circumstance.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

No, but if the offender is a competitor or a potential competitor it may be considered an aggravating circumstance.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

Yes, provided that the proceedings regarding the civil claim for damages will not be a significanct burden to the criminal proceedings, it is possible to file a civil claim for damages under the criminal proceedings, see Section 991(2) of the Danish Administration of Justice Act. If the claim for damages is heard as part of the criminal proceedings, the civil proceedings will be stayed.

Estonia

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Yes, unjustified disclosure and use of trade secrets is criminalized in Estonia under the Penal Code [RT I 2001, 61, 364].

Violation of the above-mentioned provisions of the Penal Code is sanctioned with a fine or imprisonment for up to one year maximum. A fine may also be imposed on a corporation.

It should be noted, that the said provisions on sanctions will not be applied if the actions of the defendant also meet the criteria of more serious offences with more severe sanctions.

For more information see: Jaan Sootak and Priit Pikamäe: Karistusseadustik. Kommenteeritud väljaanne [Penal Code. The Commentary.] Juura, 2009, pp. 929 – 932.

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

The criminal provisions on breach of trade secrets are limited to cases where:

i) the person who without permission discloses or uses the business secret becomes aware of such trade secret in connection with his or her professional or official duties

and

ii) if such act was committed for commercial purposes or with the aim to cause damage.

According to the Commentary of the Penal Code the respective section does not provide a list of subjects who can be liable but refers to a person who became aware of the trade secret in connection with his or her professional or official duties. Therefore the person liable could be a member of the management board or the supervisory board, auditor, and so forth.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

If the activity of the defendant meets the criteria for other criminal offences, such as fraud, these can also be applied. A civil lawsuit can alternatively be pursued if the criteria are met. Also some violations of trade secrets only result in a civil lawsuit (see the questionnaire on Commercial & IP law).

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

The general "safe harbor" clauses of Estonian criminal law (ignorance of circumstances which constitute necessary elements of offence) apply also with abuse of trade secrets, although not very relevant in practice. The court may also opt for not sentencing the defendant (or the prosecutor can opt not to prosecute him) if the crime as a whole can be held as minor or if there are other especially weighty reasons.

It should also be noted that trade secret abuse is only penalized as an intentional crime (the respective offence requires deliberate intent regarding commercial purposes or the aim to cause damage), not when committed through negligence.

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

The necessary elements of a completed offence are:

iii) In case of disclosure – if the trade secret has been communicated to a specific person or to the public. The way of disclosure is not important. It is also not important if the other person (the public) understands or uses the trade secret;

iv) In case of use – if the offender exploits the trade secret.

Also it is not important if any damages have actually been caused, but the respective offence requires deliberate intent regarding commercial purposes or the aim to cause damage.

Therefore mere risk of dissemination or disclosure does not give rise to criminal liability.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

Only following violation of trade secrets is recognized in the Penal Code:

<u>Unjustified disclosure and use of trade secrets</u>

Under § 377 (1) of the Penal Code a person who discloses or uses a business secret of which the person became aware in connection with his or her professional or official duties without the permission of the relevant undertaking, if such act was committed for commercial purposes or with the aim to cause damage shall be punished by a pecuniary punishment or up to one year of imprisonment.

The same act, if committed by a legal person, is punishable by a pecuniary punishment.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

The Estonian law does not provide any indications if trade secrets could be perceived or protected under intellectual property law. The misuse of trade secrets under competition law, commercial law and employment law are much more extensive than under criminal law (see the questionnaire on Commercial & IP law).

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

There are no limitations as such. The Penal Code does not include a definition of trade secrets. According to the Commentary of the Penal Code the definition used in the civil case law should be followed together with the definition of trade secrets in the TRIPS Agreement, which also do not include any limitations as to the items covered by legal protection of trade secrets.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

The only requirement is that the definition of a trade secret prescribed in the TRIPS Agreement is met.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Criminal protection is provided for all intellectual property rights (copyright, patents, trademarks, designs, utility models etc.)

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

If the proprietor of a trade secret considers the infringing conduct to amount to an offence criminalized in the Penal Code, the proprietor may request the police to initiate an investigation.

The police are required to investigate the matter "if there is reason and grounds". The reason for the commencement of criminal proceedings is a report of a criminal offence or other information indicating that a criminal offence has taken place. The grounds for a criminal proceeding are constituted by ascertainment of criminal elements in the reason for the criminal proceeding.

The prosecutor can raise charges if both the objective and subjective necessary elements of an offence can be shown and if the prosecutor is convinced that the necessary evidence in the criminal matter has been collected.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

No specific evidence have to be shown, any evidence allowed under the Law of Criminal Procedure [RT I 2003, 27, 166] can be brought before a court in order to prove that an abuse of trade secrets has occurred. It is the task of the prosecutor to show that both the objective and subjective necessary elements of an offence exist.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

The holder of trade secrets may not apply or any precautionary measures, but the police investigating the matter has a range of possibilities for securing and searching for evidence (such as searches of premises for investigational purposes and seizure of computer systems if they can be held as evidence in the matter) under the Law of Criminal Procedure.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Yes, a legal person can be held responsible for an act which is committed in the interests of the legal person by its body, a member thereof, or by its senior official or competent representative.

Prosecution of a legal person does not preclude prosecution of the natural person who committed the offence.

2. If so, which type of liability arises for companies? Which penalties shall apply?

Companies may be ordered to pay a lump-sum fine that can range from 3 200 euros to 16 000 000 euros. The sum to be paid is assessed by the court in accordance with the nature and extent of the omission and the financial standing of the corporation.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

The issue of corporate liability will be determined in the same case and by the same court as the individual trade secret violation. The court will be determined according to the location where the crime has been committed.

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

Under the Penal Code a trade secret violation may be committed by a person who discloses or uses a business secret of which the person became aware in connection with his or her professional or official duties without the permission of the relevant undertaking.
Since the violation can take place on in relation to business secret of which the person became aware of in connection with his or her professional or official duties, there has to be a specific obligation to keep the information secret under the law and/or under a contract.
Since the law does not provide a list of persons who can be liable under this provision, the person liable could also be a member of the management board or the supervisory board, auditor, and so forth.
An employee is required to maintain confidentiality and refrain from using the employer's trade secrets if it is stipulated so in the employment contract. The regulation of the employment contract needs to stipulate also what information qualifies as trade secrets.
The Commercial Code prescribes the obligation of the member of the management board to preserve the business secrets of the company. The member of the management board is expected to know what such business secrets of the company are.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?
There is no such condition under the Penal Code since only an act committed by a person who discloses or uses a business secret of which the person became aware in connection with his or her professional or official duties is considered a criminal offence.
An offence committed by a competitor or potential competitor is not punishable under criminal law.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?
An aggrieved person may bring a claim for damages also in the course of a criminal proceeding. The filing of a civil action for compensation for proprietary damage in a criminal proceeding is exempt from state fees. The participants in a proceeding may submit the civil action through the Prosecutor's Office or the Investigative Body within ten days as of the date of submission of the criminal file to the participants for examination. If a criminal matter is especially extensive or complicated, the Prosecutor's Office may extend such term to up to fifteen days. After that term or if the court has refused to accept the clam, a claim may be filed with a civil court.
If there is an ongoing civil lawsuit for compensation, then the civil court will not accept the claim and vice versa, if there is an ongoing civil lawsuit for compensation in the civil court the criminal court will not accept the claim. There cannot be two parallel proceeding, and the court is obligated to refuse to hear an action if matter between the same parties concerning the same object of the action on the same basis is being heard by another court.

Finland

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Yes, business espionage (Chapter 30, Section 4), the violation (Chapter 30, Section 5) or misuse (Chapter 30, Section 6) of trade secrets and secrecy offences are criminalized under the Criminal Code. Attempts to engage in business espionage or to violate a trade secret are also punishable. Accidental violations, on the contrary, are not punishable; the act must be deliberate.

Violation of any of the above-mentioned provisions of the Criminal Code is sanctioned with a fine or imprisonment for up to two years maximum (one year for secrecy offences not penalized under Chapter 40, Section 5 of the Criminal Code). A fine may also be imposed on a corporation.

It should be noted, that the said provisions on sanctions will not be applied if the actions of the defendant also meet the criteria of more serious offences with more severe sanctions.

Chapter 30, Section 11 of the Criminal Code defines the concept of "trade secret" for the purposes of Chapter 30 of the Code as "a business or professional secret and other corresponding business information that an entrepreneur keeps secret and the revelation of which would be conductive to causing financial loss to him or her or to another entrepreneur who has entrusted him or her with the information".

Section 10 of the Unfair Business Practices Act also penalizes the intentional use or revealing of technical models or instructions (as specified in Section 4 of the Act) as abuse of technical models and instructions. This can result in a fine.

For more information see the article of Nyblin (2007), mentioned in the Commercial & IP law questionnaire. For further information, please refer also to Section A. 8. of the Commercial and IP Law Questionnaire.

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

Business espionage requires that the accused has an intention of unlawfully revealing the trade secret or unjustifiably utilizing it. Violation of a trade secret requires that the defendant has tried to obtain financial benefit for himself/herself or another or to injure another by disclosing the trade secret.

Disclosing a trade secret for one's own benefit can also result in being found guilty of misuse of trade secrets or a secrecy offence, but these crimes can also be committed by only using or disclosing the information contrary to a secrecy obligation.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

If the activity of the defendant meets the criteria for other criminal offences, such as fraud or bribery, these can also be applied. A civil lawsuit can alternatively be pursued if the criteria are met (see the questionnaire on Commercial & IP law).

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

The general "safe harbor" clauses of Finnish criminal law (ignorance concerning the elements of the crime, ignorance concerning prohibition) apply also with abuse of trade secrets, although not very relevant in practice. The court may also opt for not sentencing the defendant (or the prosecutor can opt not to prosecute him) if the crime as a whole can be held as slight or if there are other especially weighty reasons.

An indictment can only be brought if probable cause for the defendant's culpability is shown. It should also be noted that trade secret abuse is only penalized as an intentional crime, not when committed through negligence.

Trade secret violation is not punishable if carried out after two years have passed since the defendant's period of service with the employer in question has ended.

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

Attempts to engage in business espionage or to violate a trade secret can give rise to criminal liability even though the crimes would remain on the level of attempts. Liability for business espionage can arise if the defendant has acquired the trade secret in a manner set out in the Criminal Code (Chapter 30, Section 4; see question 7 below) and *intends* to use it unlawfully. In other ways, the risk of disclosure of trade secrets does not give rise to criminal liability as such.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

The following violations of trade secrets are recognized in the Criminal Code:

<u>Business espionage</u>

A person who unlawfully obtains information regarding the trade secret of another

(1) by entering an area closed to unauthorized persons or accessing an information system protected against unauthorized persons,

(2) by gaining possession of or copying a document or other record, or in another comparable manner, or

(3) by using a special technical device,

with the intention of unlawfully revealing this secret or unjustifiably utilizing it shall be sentenced, unless a more severe penalty for the act is provided elsewhere in the law, for business espionage to a fine or to imprisonment for at most two years

<u>Violation of a trade secret</u>

A person who, in order to obtain financial benefit for himself or herself or another, or to injure another, unlawfully discloses the trade secret of another or unlawfully utilizes such a trade secret, having gained knowledge of the secret

(1) while in the service of another,

(2) while acting as a member of the administrative board or the board of directors, the managing director, auditor or receiver of a corporation or a foundation or in comparable duties,

(3) while performing a duty on behalf of another or otherwise in a fiduciary business relationship, or

(4) in connection with company restructuring proceedings,

shall be sentenced, unless a more severe penalty for the act is provided elsewhere in the law, for violation of a trade secret to a fine or to imprisonment for at most two years.

Misuse of a trade secret

A person who unlawfully

(1) uses in business a trade secret that has been obtained or revealed through an act punishable under this Code or

(2) in order to obtain financial benefit for himself or herself or another reveals such a secret

shall be sentenced for misuse of a trade secret to a fine or to imprisonment for at most two years.

Secrecy Offence

A person who in violation of a secrecy duty provided by an Act or Decree or specifically ordered by an authority pursuant to an Act

(1) discloses information which should be kept secret and which he or she has learnt by virtue of his or her position or task or in the performance of a duty, or

(2) makes use of such a secret for the gain of himself or herself or another shall be sentenced, unless the act is punishable under chapter 40, section 5, for a secrecy offence to a fine or to imprisonment for at most one year.

If the offence is as a whole to be assessed as slight, the court can order that a fine is paid.

Other

As stated under question 1, intentional use or revealing of technical models or instructions has been penalized in the Unfair Business Practices Act. This criminalization is usually invoked when the information in question is not held as comprising trade secrets as such.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts

prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

If misuse of trade secrets has not been carried out intentionally, it is prohibited under the Unfair Business Practices Act, but not criminalized. The same goes for actions prohibited under the Employment Contracts Act.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

There are no limitations as such (if the definition of a trade secret under the Criminal Code is met), although it has been proposed in legal literature that trade secret misuse should often relate to document-based information, whereas information based on memory should often be held as the use of one's own professional knowledge.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

The only requirement is that the Criminal Code's definition for a trade secret is met. Information that is insignificant regarding the company's business is not to be held as a trade secret even though the company would want to keep it secret

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Criminal protection is provided for all intellectual property rights (copyright, patents, trademarks, designs, utility models etc.)

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

If the proprietor of a trade secret considers the infringing conduct to amount to an offence criminalized in the Penal Code, the proprietor may request the police to initiate an investigation. Business espionage and violation of a trade secret are criminalized also as mere attempts.

The police is required to investigate the matter if there are "reasons to suspect that a crime has been committed or is being attempted". Business espionage and violation and misuse of a trade secret, as well as secrecy offences pursuant to the Criminal Code are, however, complainant offences. They will, in other words, not be investigated by the police or the prosecutor unless the proprietor of the violated trade secret files a request for investigation.

The prosecutor can raise charges if probable cause for the culpability of the defendant has been shown.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

No specific evidence has to be shown, but it is the task of the prosecutor to show beyond reasonable doubt that said abuse has occurred.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

The holder of trade secrets may not apply or any precautionary measures, but the police investigating the matter have a range of possibilities for securing and searching for evidence (such as searches of premises for investigational purposes and seizure of computer systems if they can be held as evidence in the matter) under the Coercive Measures Act (450/1987 as amended).

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Companies can be liable for business espionage and misuse of a trade secret if a person who is part of the company's statutory organ or other management or who exercises actual decision-making authority therein has been an accomplice in an offence or allowed the commission of the offence or if the care and diligence necessary for the prevention of the offence have not been observed in the operations of the corporation.

The offence is deemed to have been committed in the operations of a company if the perpetrator has acted on the behalf or for the benefit of the company, and belongs to its management or is in a service or employment relationship with it or has acted on assignment by a representative of the company.

2. If so, which type of liability arises for companies? Which penalties shall apply?

Companies may be ordered to pay a lump-sum fine that can range from 850 euros to 850 000 euros. The sum to be paid is assessed by the court in accordance with the nature and extent of the omission or the participation of the management, and the financial standing of the corporation.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

The issue of corporate liability will be determined in the same case and by the same court as the individual trade secret violation. The court will be determined according to the location where the crime has been committed.

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

A trade secret violation penalized in the Criminal Code requires that the person committing the act is aware, or should be aware, that the information in question constitutes a trade secret. Usually such can be seen to have been met if the offender in question has been especially obligated to keep certain specific information secret,

although a specific obligation is not necessary for a trade secret violation to occur. The information in question must nonetheless constitute a trade secret (ie. the company must have an interest in keeping the information secret) for the conduct to be punishable.
There is no clear distinction in this regard between employees and persons other than employees, although it is in practice more common that employees are required to maintain confidentiality in their employment agreements. Depending on the agreement in question, it may thus be easier for the trade secret holder to show that the employee in question should have realized that the expressed information constitutes a trade secret in contrast to a situation where the offender is not an employee.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

There is no such specific condition under the Criminal Code. Of course, a competitor can also be an offender in case the criteria of the Criminal Code are met.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

A claim for damages can be brought in connection with criminal proceedings, and this is also often the case in practice. However, this only applies if a separate civil case regarding compensation has not been brought, as two parallel proceedings on the same issue cannot be held simultaneously. In this case, the proceedings instituted later shall not be held.
The Court may also either join or separate a compensation claim with the criminal proceedings related to the same issue.

France

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Yes, there is criminal liability for trade secrets violation in the French jurisdiction.

French law provides a specific protection of manufacturing secrets ('*secret de fabrication*') under article L.621-1 of the French Intellectual Property Code (hereinafter "IPC") which refers to the content of article L. 1227-1 of the French Labor Code. This offence incriminates the act of revealing or attempting to reveal a manufacturing secret by any director or employee of the company. This offence is punishable by two years of imprisonment and a fine of 30,000 Euros.

Furthermore, there are general criminal provisions that can be used before the Courts to protect trade secrets (e.g. theft, receiving or concealing stolen goods, breach of trust, disclosure of secret information by a person entrusted with such a secret, fraudulent access within an automated data processing system, supplying information to a foreign power and corruption). However, this protection is generally considered as ill-suited in view of the specific nature of trade secrets.

The provisions regarding theft (article 311-1 of the Criminal Code) apply when there is a fraudulent appropriation of a trade secret fixed in a document belonging to another person. This offence has been used by French Courts to charge a person who disclosed trade secrets (Court of cassation, 7 November 1974). This offence is punishable by three years' imprisonment and a fine of 45,000 Euros.

The provision regarding breach of trust under article 314-1 of the Criminal Code is available when there is a misappropriation of trade secrets fixed on document(s) handed over to a person and that he accepted subject to the condition of returning, redelivering or using them in a specified way. This specific offence has been applied by French Courts and especially in the 'Michelin case' to charge the employee who tried to sell trade secrets to a competitor (Correctional Court of Clermont Ferrand, 21 June 2010). This author of theoffence is liable to a prison sentence of three years and a fine of 375,000 Euros.

Article 321-1 of the Criminal Code can be used to charge the person who received information considered as a trade secret. French courts already used this offence in a trade secret violation action before the criminal courts (Court of cassation, 20 October 2010). This offence is punishable by five years' imprisonment and a fine of 375,000 Euros.

Article 226-13 of the Criminal Code applies to professional secrets and can be used to charge the person who disclosed secret information (commercial or technical) even though he was entrusted with such a secret. This offence is punishable by one year's imprisonment and a fine of 15,000 Euros.

Article 323-1 of the Criminal Code applies to charge a person who access or attempts to access fraudulently within an automated data processing system. This offence is punishable by three years' imprisonment and a fine of 45,000 Euros.

The provisions under articles 411-6 to 411-8 of the Criminal Code are available so as to charge the acts of supplying secret information to a foreign power and therefore charge

a person for espionage acts. This offence is punishable by fifteen years' of criminal detention and a fine of 225,000 Euros.

Finally, the offence of corruption is available so as to protect trade secrets when the offender proposes without right and at any time offers, promises, donations, gifts or advantages so as to obtain from any public body or administration any trade secret. This offence is punishable by ten years' imprisonment and a fine of 150,000 Euros.

Please find below the list of the relevant literature on the matter

Francis Hagel, "*The Protection of trade secret: Issues and Guidelines*", Cahiers de Droit de l'Entreprise n° 1, January 2012. Article published in an Intellectual Property Law review giving a recent overview of the issues and guidelines regarding the protection of trade secrets.

Report n°4159 on the sanctions for the violation of trade secrets, by Bernard Carayon, for the National Assembly, 11 January 2012. Report written by French Member of Parliament Bernard Carayon prior to the filing of a bill before the French National Assembly regarding the sanctions of trade secrets violations, reporting the inadequacies of the French protection of trade secrets and proposing a new legislation. This report is available in French at http://www.assemblee-nationale.fr/13/rapports/r4159.asp

Jérôme Lasserre Capdeville, "*The offence of violation of a manufacturing secret*", AJ Pénal 2011, p.459. Article published in a criminal Law review regarding the offence punished under article L.621-1 IPC.

Thibault du Manoir de Juaye, "*Trade secrets*", Revue Lamy Droit de l'Immatériel, 2010, n°65. Article published in an Intellectual Property Law review giving a recent overview of the recent decisions regarding provisions used in French Law to protect trade secrets

Proceedings of the Conference Prometheus on the legal protection of economical information – Issues and prospects, by Bernard Carayon, André Dietz, Christian Harbulot, François Hagel, Olivier de Maison Rouge Thibault du Manoir de Juaye, Bertrand Warusfel, 18 October 2010. Proceedings of a conference organised by Bernard Carayon, a French deputy, regarding the protection of trade secrets and economical information in France. Available in French at
http://www.fondation-prometheus.org/publish/Actes_du_colloque_18%20octobre_2010.pdf

Report of the workshop presided by Claude Mathon, the protection of Trade secrets: issues and propositions, by Claude Mathon and his team, 17 April 2011. General report on the protection of trade secrets, the inadequacies of French Law relating to this matter and proposing a new legislation. Available at :
http://www.claudemathon.fr/public/Secret_des_affaires_Rapport_final_17_avril_09.pdf

French report on the protection of trade secrets through IPR and Unfair Competition Law, by Jean-Pierre Stouls and his team, for the AIPPI, 17 March 2010. Report written by the French Group of the AIPPI regarding the protection in France of the violation of trade secrets, reporting the inadequacies of the French protection of trade secrets and proposing improvements.
https://www.aippi.org/download/commitees/215/GR215france_en.pdf

François Hagel, "*Secrets and Intellectual Property Law, An overview*", Lamy Droit de l'Immatériel October 2009, p.73-80. Article published in an Intellectual Property Law review giving an overview of the protection of trade secrets by Intellectual Property law.

Trade secrets in French Law, by Pierre Martin, Dedale Editions, 2009. Based on a doctoral thesis by the same author submitted in 2008.

Joanna Schmidt Szalewski, "*Know-How*", Répertoire de droit commercial Dalloz, February 2009. Section of an encyclopaedia regarding the protection in French law of Know How.

Didier Poracchia, "*Secret and confidentiality in employee/employer relationships",* Revue Sociale Lamy, Supplément, 2008. Article published in a Labour Law review regarding the protection of trade secrets in the employer's/employee's relationships.

Thibault du Manoir de Juaye, "*Economic Intelligence and Trade Secrets: the point of view of in-house counsels*", Cahiers des droits de l'entreprise n°5, September – October 2008. Article published in a Labour Law review regarding the protection of trade secrets.

Régis Fabre and Léna Sersiron, "*Appropriation or Reservation of know how*", LexisNexis Encyclopedia Patents, 4200, 28 February 2007. Section of an Encyclopaedia regarding the appropriation of know how and its protection under French Law.

Yann Paclot, "*Secret business relations, the diverse aspects of trade secret*", Revue Droit et Patrimoine, 2002, n°102. Article published in a Property Law review regarding the protection of trade secrets in business.

Christophe Caron, "*Secret business relations, Secret and Intellectual Property*", Revue Droit et Patrimoine, 2002, n°102. Article published in a Property Law review regarding the protection of trade secrets by Intellectual Property Law

François-Xavier Testu, "*Secret business relations, The contractual confidentiality",* Revue Droit et Patrimoine, 2002, n°102. Article published in a Property Law review regarding the protection of trade secrets in business by contractual obligations and agreements.

"*The legal protection of company's secrets"*, n°85, Revue Droit et Patrimoine, September 2000. Article published in a Property Law review regarding the protection of trade secrets.

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

Yes, the infringer has to pursue a specific purpose set forth by law when committing the offence regarding the specific provisions. Indeed, criminal law requires the demonstration of an intent to commit the offence (article L.121-3 of the Criminal Code).

According to article L.621-1 IPC, the employee or director of the company owning the secret must intend to reveal or attempt to reveal a manufacturing secret.

Concerning the offence of corruption, the offender must intend to propose without right and, at any time, offers, promises, donations, gifts or advantages so as to obtain from any public body or administration any distinction, employment, contract, any other favorable decision or trade secrets.

Regarding the provisions under articles 411-6 to 411-8 of the Criminal Code, the offender must have the intention to supply or make accessible to a foreign power, undertaking or organization or to an undertaking or organization under foreign control, information, documents, etc.

Under the provisions of article 323-1 of the Criminal Code, the offender must intend to fraudulently access or remain within all or part of an automated data processing system.

Article 226-13 of the Criminal Code requires that the infringer may pursue a purpose to disclose the secret information.

According to the provision under the Criminal Code prosecuting the offence of receiving stolen trade secrets, the offender must pursue the purpose of concealing, retaining or transferring a good, or act as an intermediary in the transfer of a good, knowing that that thing was obtained by a felony or misdemeanor.

Following the provisions regarding the offence of breach of trust, the infringer may pursue the purpose to misappropriate funds, valuables or any property that were handed over to him and that he accepted subject to the condition of returning, redelivering or using them in a specified way.

Finally, concerning the offence of theft, it is required to evidence the purpose of the offender to fraudulently appropriate trade secrets fixed on document(s) belonging to another person.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

Apart from the offence of violation of a manufacturing secret, there are general criminal provisions that can be invoked against an infringer before the Courts to protect trade secrets.

The provision under article 311-1 of the Criminal Code is available when there is a fraudulent appropriation of a trade secret fixed in a document belonging to another person.

Moreover, French Courts do not hesitate to charge individuals and especially employees who misappropriate trade secrets fixed on document(s) handed over to them and that they accepted subject to the condition of returning, redelivering or using them in a specified way.

Furthermore, article 226-13 of the Criminal Code applies to professional secrets and is available to charge the person who disclosed secret information (commercial or technical) even though he was entrusted with such a secret.

In addition to this offence, French Courts applied article 321-1 of the Criminal Code so as to charge the person who received information considered as a trade secret.

The provisions under articles 411-6 to 411-8 of the Criminal Code are available so as to punish the person who supplied secret information to a foreign power and therefore charge a person for espionage acts.

Additionally, the offence provided under article 323-1 of the Criminal Code is available to charge a person who accesses or attempts to access fraudulently within an automated data processing system.

Finally, the offence of corruption is available when the offender proposes without right and at any time offers, promises, donations, gifts or advantages so as to obtain from any public body or administration any trade secret.

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

French criminal law does not implement a general safe harbor provision under which, there will not be any liability. However, there are specific exceptions or defences which could be used by a party so as to avoid prosecution.

Concerning the violation of a manufacturing secret, the simple fact for a third party to use the specific know-how does not constitute a fault and a misappropriation of someone else's work. Indeed, the third party could have developed his know-how on his own independently or obtained it from another company from a legitimate holder in good faith[1]. The commercial chamber of the Court of cassation held that the only similarity between goods which are not protected by a property right does not prove the misappropriation of someone else's work or the fraudulent use of the competitor's know-how.

Furthermore, regarding criminal proceedings, there is no specific legal provision or regulation prohibiting a party to disclose to third parties exhibits/documents communicated by the adverse party/opponent during the legal proceedings.

Finally, article 414-2 of the Criminal Code exempts from punishment "*any person who has attempted to commit any of the offences set out under article* [...] *411-6* (of the Criminal Code) [...]*, if, having informed the judicial or administrative authorities, he makes it possible to prevent the offence taking place and, where relevant, to identify the other offenders"*.

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

The sole risk of dissemination or disclosure of trade secrets cannot give rise to criminal liability. Indeed, according to article 111-3 of the Criminal Code, "*No one may be punished for a felony or for a misdemeanor whose ingredients are not defined by statute, nor for a petty offence whose ingredients are not defined by a regulation*." Additionally, article 121-3 of the same code provides that "*there is no felony or misdemeanor in the absence of an intent to commit it*."

Following those articles, criminal law requires in order to give rise to criminal liability the proof of all the elements of the alleged violation. They require the show of the material and legal elements as well as the evidence of the intent of the party to commit the violation; in the absence of which, the party committing the violation is not liable.

In order to prove intent, it is necessary to give evidence that the offender was aware of his acts and that he intended to reveal the manufacturing process which he knew was secret. Thus, the communication negligently does not prove intent. It should be specified that French legislation does not require evidence of a specific intent, which can be understood as the desire to achieve a specific result.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

[1] Supreme Court, Commercial chamber, 16 May 2000, JCP E 2000. 1112, PIBD 2001. 721. III. 296

There are two types of violation of trade secrets recognized in France.

The first type concerns the specific provision under criminal law protecting manufacturing secrets.

The second type of violation concerns the general criminal law provisions that could be used to protect certain information (i.e. theft, breach of trust, receiving stolen goods, disclosure of secret information by a person entrusted with such a secret, fraudulent access within an automated data processing system, supplying information to a foreign power, corruption).

All those offences are treated differently by the law due to the fact that the material and legal elements required are different from one offence to another.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law?
Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

Due to the fact that article L.621-1 IPC only protects manufacturing secrets, the notion of trade secrets protected under criminal law does not meet the requirements provided by intellectual property law.

However, the requirements under criminal case law for the protection of trade secrets meet the requirements under the protection of manufacturing secrets.
Indeed, there is no formal requirement but three substantial conditions are required to protect either trade secrets or manufacturing secrets. In order to be protected, the (manufacturing or trade) secret must:

* be substantial,
* be secret or at least not immediately accessible/available to the public,
* constitute a competitive advantage.

There are no conducts prohibited under intellectual property law which do not result in a criminal offence.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

Yes, there are limitations as to the items. For example, article L.621-1 IPC only concerns manufacturing secrets/know-how; theft only concerns documents containing a trade secret and receiving only concerns documents containing a trade secret.
Furthermore, the disclosure of secret information by a person entrusted with such a secret only concerns the secret information given/supplied during the exercise of his/her profession and the offence of supplying information to a foreign power only regards information, processes, articles, documents, computerized data or files.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

Please find the answer to this first question in the developments under question 1.

No, the patentability of the items covered by trade secrets does not impact on the extent of the protection granted by law as long as it is not granted protection by patent law. Indeed, the requirement of secrecy is common to all actions and if the information protected under trade secrets or manufacturing secrets has been granted protection by patent law, the invention will necessarily be disclosed and therefore the requirement of secrecy will not be met anymore.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Yes, the French IPC provides for criminal protection of other IP registered IP rights (e.g. articles L.335-1 to L.335-10 (copyright law) – articles L.521-9 to L.521-13 (design and model law) - articles L.615-12 to 615-16 (patent law) - articles L.716-9 to L.716-14 (trademark law)).

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

No, the prosecution of the offender can be at the initiative of the public prosecutor and the injured party/holder of the secret by a citation, a police report summons (article 388 of the French Criminal Code) or by the filing of a complaint with the competent investigating judge (Article 85 of the French Criminal Procedure Code).

Indeed, according to article 1 of the French Criminal Procedure Code: "*Public prosecution for the imposition of penalties is initiated and exercised by the judges, prosecutors or civil servants to whom it has been entrusted by law.*
This prosecution may also be initiated by the injured party under the conditions determined by the present Code."

Yes, only certain subjects are entitled to start a proceeding and/or claim any damages which are: the injured party, the public prosecutor, certain administrations such as the Customs.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

Following articles 111-3 and 121-3 of the Criminal Code, criminal law requires in order to give rise to criminal liability the proof of all the elements of the alleged violation. They require the show of the material and legal elements as well as the evidence of the intent of the party to commit the violation. In the absence of which, the party committing the violation is not liable.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

According to article 81 of the French Criminal Procedure code, which is very general, the investigating judge can order any investigating act (which is not contrary to the rights of the defense or the provisions under the European Convention of Human Rights, especially article 6 paragraph 1) such as order to search premises, require the defendant to provide information, to cease the risk of further consequences, order a precautionary seizure of the premises …

Furthermore, following article 82-1 of the French Criminal Procedure Code, the parties may file an application to obtain such investigating steps although the investigating judge can refuse to order such step.

Please find below the said provisions.

Article 81 of the French Criminal Procedure code: "*The investigating judge undertakes in accordance with the law any investigative step he deems useful for the discovery of the truth. He seeks out evidence of innocence as well as guilt*".

Article 82-1 of the French Criminal Procedure code: "*In the course of the investigation the parties may file with the investigating judge a written and reasoned application in order to be heard or interrogated, to hear a witness, for a confrontation or an inspection of the scene of the offence, to order one of them to disclose an element useful for the investigation, or for any other step to be taken which seems to them necessary for the discovery of the truth.* [...]
The investigating judge must make a reasoned order within one month from receiving the application, when he decides not to grant it. The provisions of the last paragraph of article 81 are applicable.[...]"

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Yes, companies can be held liable for trade secrets violations.

Indeed, following article 121-2 of the Criminal Code, in order to hold liable a company, it is required that the company has a legal personality which excludes "*undisclosed partnerships*" (article 1871 Civil Code) and "*de facto partnerships*"(article 1873 of the Civil Code). Furthermore the provision requires that (i) the offence should be committed by their organs or representatives and (ii) that the offence should be committed on their account.

Please find below the provision.

Article 121-2 of the Criminal Code
"*Legal persons, with the exception of the State, are criminally liable for the offences committed on their account by their organs or representatives, according to the distinctions set out in articles 121-4 and 121-7.*
However, local public authorities and their associations incur criminal liability only for offences committed in the course of their activities which may be exercised through public service delegation conventions.
The criminal liability of legal persons does not exclude that of any natural persons who are perpetrators or accomplices to the same act, subject to the provisions of the fourth paragraph of article 121-3."

2. If so, which type of liability arises for companies? Which penalties shall apply?

Civil and criminal liability can arise for company as the offender or the accomplice of the organ or the representative which committed the offence. To prove that a legal person is an accomplice, it must be established that the organ or the representative was himself an accomplice and therefore either (i) knowingly, by aiding and abetting, facilitated the preparation or the commission of the offence or, (ii) by means of a gift, promise, threat, order, or an abuse of authority or powers, provoked the commission of an offence or gave instructions to commit it.

Regarding the offences of theft (article 311-16 of the Criminal Code), breach of trust (article 314-12 of the Criminal Code), receiving stolen goods (article 321-12 of the Criminal Code), corruption (article 323-6 of the Criminal Code), all the provisions applicable to these offences refer to article L.131-39 of the Criminal Code that provides specific penalties for legal persons.

In case the provisions do not provide a different penalty for legal persons, the penalties are the same as for the natural persons.

Article L.131-39 of the Criminal Code states as follows:

"*Where a statute so provides against a legal person, a felony or misdemeanour may be punished by one or more of the following penalties:*

1° dissolution, where the legal person was created to commit a felony, or, where the felony or misdemeanour is one which carries a sentence of imprisonment of three years or more, where it was diverted from its objects in order to commit them;

2° prohibition to exercise, directly or indirectly one or more social or professional activity, either permanently or for a maximum period of five years;

3° placement under judicial supervision for a maximum period of five years;

4° permanent closure or closure for up to five years of the establishment, or one or more of the establishments, of the enterprise that was used to commit the offences in question;

5° disqualification from public tenders, either permanently or for a maximum period of five years;

6° prohibition, either permanently or for a maximum period of five years, to make a public appeal for funds;

7° prohibition to draw cheques, except those allowing the withdrawal of funds by the drawer from the drawee or certified cheques, and the prohibition to use payment cards, for a maximum period of five years;

8° confiscation of the thing which was used or intended for the commission of the offence, or of the thing which is the product of it;

9° posting a public notice of the decision or disseminating the decision in the written press or using any form of communication to the public by electronic means. The penalties under 1° and 3° above do not apply to those public bodies which may incur criminal liability. Nor do they apply to political parties or associations, or to unions. The penalty under 1° does not apply to institutions representing workers."

Furthermore, according to article L.131-38 of the Criminal Code, "*the maximum amount of a fine applicable to legal persons is five times that which is applicable to natural persons by the law sanctioning the offence.*
Where this is an offence for which no provision is made for a fine to be paid by natural persons, the fine incurred by legal persons is €1,000,000."

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

It is the same court that will adjudicate the liability of natural persons and the liability of companies which is the Criminal Trial ('*Tribunal Correctionnel*') according to article 381 of the Criminal Procedure Code.

Regarding the violation of a manufacturing secret, the Court that will adjudicate this kind of case is the Commercial Court on the condition that the plaintiff does not make a claim for patent infringement in his action (in such case, article L.615-17 IPC adjudicates those cases to the jurisdiction of the First Instance Courts) (Court of cassation, 7 June 2011, Chlorotech v Obio Group, n°10-19.030).

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

Apart from the offences of violation of a manufacturing secret and disclosure of secret information by a person entrusted with such a secret, which requires specifically under their provisions in the Criminal Code to keep the information secret for a trade secret violation to occur, there is no such specific obligation under the other general criminal provisions (e.g. theft, receiving or concealing stolen goods, breach of trust, fraudulent access within an automated data processing system, supplying information to a foreign power and corruption).

It should be noted that even though the offence under article 411-6 to 411-8 of the Criminal code does not require such obligation, it does require that the information supplied to a foreign entity be "*liable to prejudice the fundamental interests of the nation*".

Apart from article L.621-1 IPC which provides that the offences shall be carried out by any employee or any director of the company owning the trade secret, the other provisions (e.g. theft, receiving or concealing stolen goods, breach of trust, fraudulent access within an automated data processing system and supplying information to a foreign power) do not require that the offence be committed by an employee of the company.

However, regarding the offence of corruption, the provision requires that the person committing the offence be either a person holding public authority, or discharging a public service mission or holding a public electoral mandate. Regarding the offence of disclosure of secret information by a person entrusted with such a secret, article 226-13 of the Criminal code provides that the offender shall be a person entrusted with a secret according to the law or case law (e.g. lawyers, judges, police officers, health practitioners, accountants, ministers of religion, etc.)

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

No, the offender does not have to qualify as a competitor or potential competitor of the owner of the disclosed trade secret as long as the requirements for the material, legal and moral elements of the criminal offences are met.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

Pursuant to Articles 2 and 3 of the French Criminal Procedure Code, the aggrieved person can bring a claim for damages before the criminal courts in the course of criminal proceedings.

Please find below the provisions of Articles 2 and 3 of the French Criminal Procedure Code.

Article 2

"Civil action aimed at the reparation of the damage suffered because of a felony, a misdemeanour or a petty offence is open to all those who have personally suffered damage directly caused by the offence.

The waiver of a civil action will not interrupt or suspend the exercise of the public prosecution, subject to the cases set out under the third paragraph of article 6".

Article 3

"*The civil action may be exercised at the same time as the public prosecution and before the same court.*

It is admissible for any cause of damage, whether material, bodily or moral, which ensues from the actions prosecuted".

Furthemore, according to article 5 of the French Criminal Procedure Code, it is impossible for the civil party (the aggrieved person) to bring separate claims for damages/compensation before a criminal court and a civil court. Therefore, the aggrieved party can only bring an action for compensation either before the civil court either before the criminal court.

Please find below the provisions of Article 5 of the French Criminal Procedure Code.

Article 5

"*The party who has brought his action before the competent civil court may not bring it before the court for felonies".*

Germany

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secret violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal frame work. To be more specific and have more details, please provide a list of the relevant literature on this matter.

German law provides for criminal liability for trade secret violation. The relevant provisions are scattered over a variety of laws, including the Act Against Unfair Competition, the Criminal Code, the Limited Liability Company Act, the Stock Corporation Act, the Cooperative Business Association Act, the Workplace Constitution Act, the Insurance Supervision Act, the Transformation Act, the Act on the co-Determination of Employees in Cross-Border Mergers, the Act on European Works Councils, the Act Transposing the Directive Regulations regarding the Involvement of Employees in SEs, the Public Accountants Act and the Public Disclosure Act.

Except for the provisions of the Criminal Code, the relevant provisions in the above mentioned laws constitute supplementary penal provisions.

Most of the relevant provisions which provide for criminal liability for trade secret violation have in common that the later on disclosed trade secret must have been confided or become known to the offender in course of his professional occupation for the aggrieved party. This does not necessarily require an employer-employee relationship so that, for example, also external persons like certified public accountants can be liable for punishment. However, depending on the concrete provision a certain professional relationship between the offender and the aggrieved party is generally required. As an exception to the above, the criminal liability for industrial espionage pursuant to Sec. 17(2) No. 1 Act Against Unfair Competition and the handling of unlawfully acquired trade secrets pursuant to Sec. 17(2) No .2 Act Against Unfair Competition limited to certain professionals or persons affiliated with the company. These offences can be committed by anybody

The potential penalties in the relevant provisions range from monetary fines up to three year imprisonment and, in especially serious cases, up to five years.

The general purpose of the relevant provisions is the protection of trade and business secrets against unauthorised disclosure or use. Additionally, the provisions of the Act Against Unfair Competition impose criminal penalties on the unauthorised acquirement and the unauthorised saving of trade and business secrets.

The relevant provisions which provide for criminal liability for the violation of trade secrets coherently use the term "trade and business secrets", whereas the distinction between trade secrets and business secrets is more of theoretical nature and only serves the purpose for clarification. Both terms are comprehensively used to refer to financial and company secrets and are protected in exactly the same way.

In the following, the relevant provisions which provide for criminal protection of trade secrets are synoptically presented in bilingual versions.

Act against Unfair Competition ("UWG")

Sec. 17 UWG	§ 17 UWG
Disclosure of trade and business secrets	Verrat von Geschäfts- und Betriebsgeheimnissen
(1) Whoever as the employee of a business communicates, without	(1) Wer als eine bei einem Unternehmen beschäftigte Person ein Geschäfts-

authorisation, a trade or business secret with which he was entrusted, or to which he had access, during the course of the employment relationship to another person for the purposes of competition, for personal gain, for the benefit of a third party, or with the intent of causing damage to the owner of the business shall be liable to imprisonment not exceeding three years or to a fine.

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

(3) An attempt shall incur criminal liability.

(4) In particularly serious cases the sentence shall consist in imprisonment not exceeding five years or a fine. A particularly serious case shall usually exist in circumstances where the perpetrator
1. acts on a commercial basis;
2. knows at the time of the communication that the secret is to be used abroad; or
3. himself effects a use pursuant to subsection (2), number 2, abroad.

(5) The offence shall be prosecuted upon application only, unless the criminal prosecution authority considers that it is necessary to take ex officio action on account of the particular public

oder Betriebsgeheimnis, das ihr im Rahmen des Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemand zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, mitteilt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen,
1. sich ein Geschäfts- oder Betriebsgeheimnis durch
   a) Anwendung technischer Mittel,
   b) Herstellung einer verkörperten Wiedergabe des Geheimnisses oder
   c) Wegnahme einer Sache, in der das Geheimnis verkörpert ist, unbefugt verschafft oder sichert oder
2. ein Geschäfts- oder Betriebsgeheimnis, das er durch eine der in Absatz 1 bezeichneten Mitteilungen oder durch eine eigene oder fremde Handlung nach Nummer 1 erlangt oder sich sonst unbefugt verschafft oder gesichert hat, unbefugt verwertet oder jemandem mitteilt.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter
1. gewerbsmäßig handelt,
2. bei der Mitteilung weiß, dass das Geheimnis im Ausland verwertet werden soll, oder
3. eine Verwertung nach Absatz 2 Nummer 2 im Ausland selbst vornimmt.

(5) Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die

interest in the criminal prosecution.
(6) Section 5, number 7, of the Criminal Code shall apply mutatis mutandis.

Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.
(6) § 5 Nummer 7 des Strafgesetzbuches gilt entsprechend.

Sec. 18 UWG

Use of models

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

§ 18 UWG

Verwertung von Vorlagen

(1) Wer die ihm im geschäftlichen Verkehr anvertrauten Vorlagen oder Vorschriften technischer Art, insbesondere Zeichnungen, Modelle, Schablonen, Schnitte, Rezepte, zu Zwecken des Wettbewerbs oder aus Eigennutz unbefugt verwertet oder jemandem mitteilt, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.
(3) Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.
(4) § 5 Nummer 7 des Strafgesetzbuches gilt entsprechend.

Sec. 19 UWG

Suborning and offering disclosure

(1) Whoever for the purposes of competition or for personal gain attempts to procure another person to commit a criminal offence pursuant to Section 17 or Section 18 or to incite the commission of such an offence shall be liable to imprisonment not exceeding two years or to a fine.
(2) Whoever for the purposes of competition of for personal gain offers, or accepts the offer of another person, or conspires with another person, to commit, or to incite the commission of, a criminal offence pursuant to Section 17 or Section 18 shall incur the same liability.
(3) Section 31 of the Criminal Code shall apply mutatis mutandis.

§ 19 UWG

Verleiten und Erbieten zum Verrat

(1) Wer zu Zwecken des Wettbewerbs oder aus Eigennutz jemanden zu bestimmen versucht, eine Straftat nach § 17 oder § 18 zu begehen oder zu einer solchen Straftat anzustiften, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs oder aus Eigennutz sich bereit erklärt oder das Erbieten eines anderen annimmt oder mit einem anderen verabredet, eine Straftat nach § 17 oder § 18 zu begehen oder zu ihr anzustiften.
(3) § 31 des Strafgesetzbuches gilt entsprechend.

(4) The offence shall be prosecuted upon application only, unless the criminal prosecution authority considers that it is necessary to take ex officio action on account of the particular public interest in the criminal prosecution.
(5) Section 5, number 7, of the Criminal Code shall apply mutatis mutandis.

(4) Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.
(5) § 5 Nummer 7 des Strafgesetzbuches gilt entsprechend.

Criminal Code („StGB"):

Sec. 203 StGB

Violation of Private Secrets

(1) Whosoever unlawfully discloses a secret of another, in particular, a secret which belongs to the sphere of personal privacy or a business or trade secret, which was confided to or otherwise made known to him in his capacity as a
1. physician, dentist, veterinarian, pharmacist or member of another healthcare profession which requires state-regulated education for engaging in the profession or to use the professional title;
2. professional psychologist with a final scientific examination recognized by the State;
3. attorney, patent attorney, notary, defence counsel in statutorily regulated proceedings, certified public accountant, sworn auditor, tax consultant, tax agent, or organ or member of an organ of a law, patent law, accounting, auditing or tax consulting firm in the form of a company;
4. marriage, family, education or youth counselor as well as addiction counsellor at a couselling agency which is recognised by a public authority or body, institution or foundation under public law.
4a. member or agent of a counseling agency recognized under section 3 and section 8 of the Act on Pregnancies in Conflict Situations;
5. state-recognised social worker or state-recognised social education worker; or
6. member of a private health, accident or life insurance company or a private

§ 203 StGB

Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als
1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
2. Berufspsychologen mit staatlich anerkannter wissenschaftlich Abschlußprüfung,
3. Rechtsanwalt, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,
4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater fürSuchtfragen in einer Beratungsstelle, die von

medical, tax consultant or attorney invoicing service,

shall be liable to imprisonment of not more than one year or a fine.

(2) Whosoever unlawfully discloses a secret of another, in particular, a secret which belongs to the sphere of personal privacy or a business or trade secret, which was confided to or otherwise made known to him in his capacity as a

1. public official;
2. person entrusted with special public service functions;
3. person who exercises duties or powers under the law on staff employment representation;
4. member of an investigative committee working for a legislative body of the Federation or a state, another committee or council which is not itself part of the legislative body, or as an assistant for such a committee or council; or
5. publicly appointed expert who is formally obliged by law to conscientiously fulfill his duties, or
6. person who is formally obliged by law to conscientiously fulfill his duty of confidentiality in the course of scientific research projects,

shall incur the same penalty. Particular statements about personal or material relationships of another which have been collected for public administration purposes shall be deemed to be equivalent to a secret within the meaning of the 1st sentence above; the 1st sentence above shall not apply to the extent that such particular statements are made known to other public authorities or other agencies for public administration purposes unless the law forbids it.

(2a) Subsections (1) and (2) above shall apply mutatis mutandis when a data protection officer without authorisation discloses the secret of another within the meaning of these

einer Behörde oderKörperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist.

4a. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,

5. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder
6. Angehörigen eines Unternehmens der privaten Kranken-, Unfall oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Amtsträger,
2. für den öffentlichen Dienst besonders Verpflichteten,
3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,
4. Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates, das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates,
5. öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes

provisions, which was entrusted to or otherwise revealed to one of the persons named in subsections (1) or (2) above in their professional capacity and of which he has gained knowledge in the course of the fulfilment of his duties as data protection officer.

(3) Other members of a bar association shall be deemed to be equivalent to an attorney named in subsection (1) No 3 above. The persons named in subsection (1) and the 1st sentence above shall be equivalent to their professionally active assistants and those persons who work with them in training for the exercise of their profession. After the death of the person obliged to keep the secret, whosoever acquired the secret from the deceased or from his estate shall be equivalent to the persons named in subsection (1) and in the 1st and 2nd sentences above.

(4) Subsections (1) to (3) above shall also apply if the offender unlawfully discloses the secret of another person after the death of that person.

(5) If the offender acts for material gain or with the intent of enriching himself or another or of harming another the penalty shall be imprisonment of not more than two years or a fine.

förmlich verpflichtet worden ist, oder

6. Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist,

anvertraut worden oder sonst bekanntgeworden ist. Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfaßt worden sind; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen Stellen für Aufgaben der öffentlichen Verwaltung bekanntgegeben werden und das Gesetz dies nicht untersagt.

(2a) Die Absätze 1 und 2 gelten entsprechend, wenn ein Beauftragter für den Datenschutz unbefugt ein fremdes Geheimnis im Sinne dieser Vorschriften offenbart, das einem in den Absätzen 1 und 2 Genannten in dessen beruflicher Eigenschaft anvertraut worden oder sonst bekannt geworden ist und von dem er bei der Erfüllung seiner Aufgaben als Beauftragter für den Datenschutz Kenntnis erlangt hat.

(3) Einem in Absatz 1 Nr. 3 genannten Rechtsanwalt stehen andere Mitglieder einer Rechtsanwaltskammer gleich. Den in Absatz 1 und Satz 1 Genannten stehen ihre berufsmäßig tätigen Gehilfen und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind. Den in Absatz 1 und den in Satz 1 und 2 Genannten steht nach dem Tod des zur Wahrung des Geheimnisses Verpflichteten ferner gleich, wer

das Geheimnis von dem Verstorbenen oder aus dessen Nachlaß erlangt hat.

(4) Die Absätze 1 bis 3 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.
(5) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

Sec. 204 StGB

Exploitation of the Secrets of Others

(1) Whosoever unlawfully exploits the secret of others, in particular a business or trade secret, which he is obliged to keep secret pursuant to section 203, shall be liable to imprisonment of not more than two years or a fine.

(2) Section 203 (4) shall apply mutatis mutandis.

§ 204 StGB

Verwertung fremder Geheimnisse

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein Betriebs- oder Geschäftsgeheimnis, zu dessen Geheimhaltung er nach § 203 verpflichtet ist, verwertet, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) § 203 Abs. 4 gilt entsprechend.

Limited Liability Company Act ("GmbHG"):

Sec. 85 GmbHG

Violation of the duty of confidentiality

(1) Whoever without authorisation discloses a secret of the company, in particular a trade or business secret, shall be punished by imprisonment of up to one year or by fine if such secret became known to him in his capacity as company director, member of the supervisory board or liquidator.
(2) If such offender acted material gain or with the intent to enrich himself or another person or to harm another person, the punishment shall be imprisonment of up to two years or a fine. Whoever unlawfully uses a secret of the kind specified in subsection 1 in particular a trade or

§ 85 GmbHG

Verletzung der Geheimhaltungspflicht

(1) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer ein Geheimnis der Gesellschaft, namentlich ein Betriebs- oder Geschäftsgeheimnis, das ihm in seiner Eigenschaft als Geschäftsführer, Mitglied des Aufsichtsrats oder Liquidator bekanntgeworden ist, unbefugt offenbart.
(2) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe. Ebenso wird bestraft, wer ein Geheimnis der in

business secret, which he has learned under the circumstances of subsection 1 shall be punished in the same manner.

(3) The offence shall be prosecuted only upon application of the company. If such offence is committed by a company director, the application may be made by the supervisory board and, if no supervisory board exists, by a special representative appointed by the shareholders. If such offence is committed by a member of the supervisory board, such application may be made by the management board or the liquidators.

Absatz 1 bezeichneten Art, namentlich ein Betriebs- oder Geschäftsgeheimnis, das ihm unter den Voraussetzungen des Absatzes 1 bekanntgeworden ist, unbefugt verwertet.

(3) Die Tat wird nur auf Antrag der Gesellschaft verfolgt. Hat ein Geschäftsführer oder ein Liquidator die Tat begangen, so ist der Aufsichtsrat und, wenn kein Aufsichtsrat vorhanden ist, von den Gesellschaftern bestellten besondere Vertreter antragsberechtigt. Hat ein Mitglied des Aufsichtsrats die Tat begangen, so sind die Geschäftsführer oder die Liquidatoren antragsberechtigt.

Stock Corporation Act („AktG")

Sec. 404 AktG

Violation of the duty of confidentiality

(1) Whoever without authorisation discloses a secret of the company, in particular a trade or business secret, shall be punished by imprisonment of up to one year or by fine if such secret became known to him in his capacity as:

1. a member of the management board or the supervisory board or liquidator;
2. auditor or assistant of an auditor;

in case of No. 2, however only if such act does not constitute a criminal offense pursuant to Sec. 333 of the Commercial Code.

(2) If such offender acted material gain or with the intent to enrich himself or another person to harm another person, the punishment shall be imprisonment of up to two years or a fine. Whoever unlawfully uses a secret of the kind specified in subsection 1, in particular a trade or business secret, which he has learned under the circumstances of subsection 1 shall be punished in the same manner.

§ 404 AktG

Verletzung der Geheimhaltungspflicht

(1) Mit Freiheitsstrafe bis zu einem Jahr, bei börsennotierten Gesellschaften bis zu zwei Jahren, oder mit Geldstrafe wird bestraft, wer ein Geheimnis der Gesellschaft, namentlich ein Betriebs- oder Geschäftsgeheimnis, das ihm in seiner Eigenschaft als

1. Mitglied des Vorstands oder des Aufsichtsrats oder Abwickler,
2. Prüfer oder Gehilfe eines Prüfers

bekanntgeworden ist, unbefugt offenbart; im Falle der Nummer 2 jedoch nur, wenn die Tat nicht in § 333 des Handelsgesetzbuchs mit Strafe bedroht ist.

(2) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren, bei börsennotierten Gesellschaften bis zu drei Jahren, oder Geldstrafe. Ebenso wird bestraft, wer ein Geheimnis der in Absatz 1 bezeichneten Art, namentlich ein Betriebs- oder Geschäftsgeheimnis, das ihm unter den Voraussetzungen des Absatzes 1 bekanntgeworden ist, unbefugt

(3) The offence shall be prosecuted only upon application by the company. Such application may be made by the supervisory board if a member of the management board or liquidator committed such offence; such application may be made by the management board or the liquidators if a member of the supervisory board committed such offence.

verwertet.

(3) Die Tat wird nur auf Antrag der Gesellschaft verfolgt. Hat ein Mitglied des Vorstands oder ein Abwickler die Tat begangen, so ist der Aufsichtsrat, hat ein Mitglied des Aufsichtsrats die Tat begangen, so sind der Vorstand oder die Abwickler antragsberechtigt.

Commercial Code („HGB"):

Sec. 333 HGB Commercial Code	§ 333 HGB
Violation of the duty of confidentiality	Verletzung der Geheimhaltungspflicht
(1) Whoever without authorization discloses a secret of the company, a subsidiary (Sec. 290 para. 1, 2), a jointly run enterprise (Sec. 310) or an associated enterprise (Sec. 311), in particular a trade or business secret, if such secret became known to him in his capacity as auditor or assistant to an auditor while examining the annual financial statements, a separate financial statements in accordance with § 325 subsection 2 or the consolidated financial statements, shall be punished by imprisonment of up to one year or by fine or whoever without authorization reveals a business or trade secret or any knowledge about the company, which has become known to him as an employee at a inspecting authority in accordance with § 342b subsection 1 during the examination.	(1) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer ein Geheimnis der Kapitalgesellschaft, eines Tochterunternehmens (§290 Abs. 1, 2), eines gemeinsam geführten Unternehmens (§ 310) oder eines assoziierten Unternehmens (§ 311), namentlich ein Betriebs- oder Geschäftsgeheimnis, das ihm in seiner Eigenschaft als Abschlussprüfer oder Gehilfe eines Abschlussprüfers bei Prüfung des Jahresabschlusses, eines Einzelabschlusses nach § 325 Abs. 2a oder des Konzernabschlusses bekannt geworden ist, oder wer ein Geschäfts- oder Betriebsgeheimnis oder eine Erkenntnis über das Unternehmen, das ihm als Beschäftigter bei einer Prüfstelle im Sinne von § 342b Abs. 1 bei der Prüftätigkeit bekannt geworden ist, unbefugt offenbart.
(2) If such offender acted material gain or with the intent to enrich himself or another person to harm another person, the punishment shall be imprisonment of up to two years or a fine. Whoever unlawfully uses a secret of the kind specified in subsection 1, in particular a trade or business secret, which he has learned under the circumstances of subsection 1 shall be punished in the same manner.	(2) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe. Ebenso wird bestraft, wer ein Geheimnis der in Absatz 1 bezeichneten Art, namentlich ein Betriebs- oder Geschäftsgeheimnis, das ihm unter den Voraussetzungen des Absatzes 1 bekannt geworden ist, unbefugt verwertet.
(3) The offence shall be prosecuted only upon application by the company.	

(3) Die Tat wird nur auf Antrag der Kapitalgesellschaft verfolgt.

Act on Purchasing and Trading Cooperations ("GenG")

Sec. 151 GenG	§ 151 GenG
Violation of the duty of confidentiality	Verletzung der Geheimhaltungspflicht
(1) Whoever without authorisation discloses a secret of the cooperative, in particular a trade or business secret, shall be punished by imprisonment of up to one year or by fine if such secret became known to him in his capacity as	(1) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer ein Geheimnis der Genossenschaft, namentlich ein Betriebs- oder Geschäftsgeheimnis, das ihm in seiner Eigenschaft als
1. a member of the management board or the supervisory board or liquidator;	1. Mitglied des Vorstands oder des Aufsichtsrats oder Liquidator oder
2. auditor or assistant of an auditor;	2. Prüfer oder Gehilfe eines Prüfers
in case of no. 2, however only if such act does not constitute a criminal offense pursuant to sec. 340m in conjunction with sec. 333 of the Commercial Code.	bekannt geworden ist, unbefugt offenbart, im Falle der Nummer 2 jedoch nur, wenn die Tat nicht in § 340m in Verbindung mit § 333 des Handelsgesetzbuchs mit Strafe bedroht ist.
(2) If such offender acted for material gain or with the intent to enrich himself or another person or to harm another person, the punishment shall be imprisonment of up to two years or a fine. Whoever unlawfully uses a secret of the kind specified in subsection 1 in particular a trade or business secret, which he has learned under the circumstances of subsection 1 shall be punished in the same manner.	(2) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe. Ebenso wird bestraft, wer ein Geheimnis der in Absatz 1 bezeichneten Art, namentlich ein Betriebs- oder Geschäftsgeheimnis, das ihm unter den Voraussetzungen des Absatzes 1 bekannt geworden ist, unbefugt verwertet.
(3) The offence shall be prosecuted only upon application of the cooperative. If such offence is committed by a company director, the application may be made by the supervisory board and, if no supervisory board exists, by a special representative appointed by the shareholders. If such offence is committed by a member of the supervisory board, such application may be made by the management board or the liquidators.	(3) Die Tat wird nur auf Antrag der Genossenschaft verfolgt. Hat ein Mitglied des Vorstands oder ein Liquidator die Tat begangen, so ist der Aufsichtsrat, hat ein Mitglied des Aufsichtsrats die Tat begangen, so sind der Vorstand oder die Liquidatoren antragsberechtigt.

Works Constitution Act ("BetrVG")

Sec. 120 BetrVG

Breach of secrecy

(1) Whoever, without authorization, discloses a third party's trade or business secret which the employer has expressly stated to be confidential and that has come to his knowledge while serving as
1. a member or substitute member of the works council or one of the bodies referred to in section 79 (2),
2. a representative of a trade union or employers' association,
3. an expert who has been called in by the works council under section 80 (3) or consulted by the conciliation committee under the third sentence of section 109,
3a. a consultant retained by the works council under the second sentence of section 111,
3b. personnel providing information to the works council in accordance with the third sentence of section 80 (2),
4. an employee who has been called in by the works council in accordance with the third sentence of section 107 (3) or by the finance committee under the second sentence of section 108 (2)

shall be liable to a term of imprisonment of up to one year or a fine.

(2) A similar penalty shall be imposed on any person who without being authorized to do so divulges an employee's secret and specifically a personal secret which has come to his knowledge while he was serving as a member or substitute member of the works council or one of the bodies referred to in section 79 (2) and in respect of which he is bound

§ 120 BetrVG

Verletzung von Geheimnissen

(1) Wer unbefugt ein fremdes Betriebs- oder Geschäftsgeheimnis offenbart, das ihm in seiner Eigenschaft als
1. Mitglied oder Ersatzmitglied des Betriebsrats oder einer der in § 79 Abs. 2 bezeichneten Stellen,
2. Vertreter einer Gewerkschaft oder,
3. Sachverständiger, der vom Betriebsrat nach § 80 Abs. 3 hinzugezogen oder von der Einigungsstelle nach § 109 Satz 3 angehört worden ist,
3a. Berater, der vom Betriebsrat nach § 111 Satz 2 hinzugezogen worden ist,
3b. Auskunftsperson, die dem Betriebsrat nach § 80 Abs. 2 Satz 3 zur Verfügung gestellt worden ist, oder
4. Arbeitnehmer, der vom Betriebsrat nach § 107 Abs. 3 Satz 3 oder vom Wirtschaftsausschuss nach § 108 Abs. 2 Satz 2 hinzugezogen worden ist,

bekannt geworden und das vom Arbeitgeber ausdrücklich als geheimhaltungsbedürftig bezeichnet worden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis eines Arbeitnehmers, namentlich ein zu dessen persönlichen Lebensbereich gehörendes Geheimnis, offenbart, das ihm in seiner Eigenschaft als Mitglied oder Ersatzmitglied des Betriebsrats oder einer der in § 79 Abs. 2 bezeichneten Stellen bekannt geworden ist und über das nach den

to secrecy under the provisions of this Act.

(3) Where an offender has acted for material gain or with the intention of obtaining some advantage for himself or another person or of harming any other person, the penalty shall be a term of imprisonment of up to two years or a fine. A similar penalty shall be imposed on any person who, without being authorised to do so, exploits a third party's secret and specifically a trade or business secret in respect of which he is bound to secrecy under the provisions of subsections 1 or 2.

(4) Subsections (1) to (3) shall also be applicable if the offender divulges or exploits the third-party secret after the death of the person concerned.

(5) Proceedings for the offence shall be instituted only on application by the injured party. If the injured party dies, the right to apply shall pass to the relatives in accordance with section 77 (2) Criminal Code insofar as the secret belongs to the personal sphere of the injured party; in all other cases it shall pass to the heirs. Where the offender divulges the secret after the death of the party concerned, the second sentence of this subsection shall apply, mutatis mutandis

Vorschriften dieses Gesetzes Stillschweigen zu bewahren ist.

(3) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe. Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein Betriebs- oder Geschäftsgeheimnis, zu dessen Geheimhaltung er nach den Absätzen 1 oder 2 verpflichtet ist, verwertet.

(4) Die Absätze 1 bis 3 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tode des Betroffenen unbefugt offenbart oder verwertet.

(5) Die Tat wird nur auf Antrag des Verletzten verfolgt. Stirbt der Verletzte, so geht das Antragsrecht nach § 77 Abs. 2 des Strafgesetzbuches auf die Angehörigen über, wenn das Geheimnis zum persönlichen Lebensbereich des Verletzten gehört; in anderen Fällen geht es auf die Erben über. Offenbart der Täter das Geheimnis nach dem Tode des Betroffenen, so gilt Satz 2 sinngemäß.

<u>Insurance Supervision Act („VAG"):</u>

Sec. 138 VAG

Violation of the duty of confidentiality

(1) A person who, except for the cases under section 333 of the Commercial Code or section 404 of the Stock Corporation Act, discloses any secret of the insurance undertaking without being authorised to do so, in particular any business or trade secret which has come to his knowledge in his capacity as
   1. auditor or assistant to an auditor in accordance with section 341k in conjunction with section 319 of the Commercial Code,
   2. member of the board of directors

§ 138 VAG

Verletzung der Geheimhaltungspflicht

(1) Wer, abgesehen von den Fällen des § 333 des Handelsgesetzbuchs oder des § 404 des Aktiengesetzes, ein Geheimnis des Versicherungsunternehmens oder Pensionsfonds (§ 112 Abs. 1 Satz 1), namentlich ein Betriebs- oder Geschäftsgeheimnis, das ihm in seiner Eigenschaft als
   1. Prüfer oder Gehilfe eines Prüfers nach § 341k in Verbindung mit § 319 des Handelsgesetzbuchs,
   2. Mitglied des Vorstands oder des

or supervisory board or liquidator,

shall be liable to imprisonment for a term not exceeding one year, or to a fine. The same applies to persons who work for a protection fund in accordance with § 133.

(2) If the offender acts for a consideration or with the intent to enrich himself or another person or to harm another person he shall be punished with imprisonment for a term not exceeding two years or by imposing a fine. Subject to punishment shall also be any person who makes use of a secret of the kind described under subsection 1 above, in particular any business or trade secret which came to his knowledge as specified under subsection 1 above.

(3) The offence shall only be prosecuted at the request of the insurance undertaking. If a member of the board of directors or a liquidator has committed the offence the supervisory board shall be entitled to make the request, if a member of the supervisory board has committed the offence the board of directors or the liquidator shall be entitled to make the request.

Aufsichtsrats oder Liquidator bekanntgeworden ist,

unbefugt offenbart, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. Dasselbe gilt für die gemäß § 133 für einen Sicherungsfonds tätigen Personen.

(2) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe. Ebenso wird bestraft, wer ein Geheimnis der in Absatz 1 bezeichneten Art, namentlich ein Betriebs- oder Geschäftsgeheimnis, das ihm unter den Voraussetzungen des Absatzes 1 bekanntgeworden ist, unbefugt verwertet.

(3) Die Tat wird nur auf Antrag des Versicherungsunternehmens oder Pensionsfonds (§ 112 Abs. 1 Satz 1) verfolgt. Hat ein Mitglied des Vorstands oder ein Liquidator die Tat begangen, so ist der Aufsichtsrat, hat ein Mitglied des Aufsichtsrats die Tat begangen, so sind der Vorstand oder die Liquidatoren antragsberechtigt.

<u>Transformation Act („UmwG"):</u>

Sec. 315 UmwG

Breach of duty of confidentiality

(1) Any person who without authorization discloses a secret of a legal entity involved in a reorganization, namely a business or trade secret, which has come to his/her knowledge in his/her capacity as

1. a member of the representative body, a shareholder or a partner authorized to represent the company, a member of a supervisory board or a liquidator of this or another legal entity involved in the reorganization;
2. a merger, division or transfer

§ 315 UmwG

Verletzung der Geheimhaltungspflicht

(1) Mit Freiheitsstrafen bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer ein Geheimnis eines an einer Umwandlung beteiligten Rechtsträgers, namentlich ein Betriebs- oder Geschäftsgeheimnis, das ihm in seiner Eigenschaft als

1. Mitglied des Vertretungsorgans, vertretungsberechtigter Gesellschafter oder Partner, Mitglied eines Aufsichtsrats oder Abwickler dieses oder eines anderen an der Umwandlung beteiligten Rechtsträgers,
2. Verschmelzungs-, Spaltungs-

auditor or an assistant of such an auditor,

shall be liable to a term of imprisonment not exceeding one year or to affine if the offence is in the case of No. 1 not subject to a penalty in Sec. 85 German Limited Liability Companies Act, Sec. 404 German Stock Corporation Act, Sect. 151 German Cooperative Societies Act or Sec. 138 German Insurance Supervisory Act and, in the case of No. 2, Sec. 333 German Commercial Code.

(2) In the event that the offender acts for a consideration or with the intent to enrich himself/herself or any other person or cause damage to any other person, the punishment shall be a term of imprisonment not exceeding two years or a fine. Any person who makes unauthorised use of a secret of the kind referred to in Paragraph 1, namely a business or trade secret, which has come to his/her knowledge on the conditions of Paragraph 1 shall be liable to equal punishment.

(3) The offence shall only b e prosecuted at the request of any of the legal entities involved in the reorganization. In the event that a member of a representative body, a shareholder or a partner authorised to represent the legal entity or a liquidator has committed the offence, application may be filed also by a supervisory board or a shareholder or a partner not being authorized to represent that legal entity. In the event that a member of a supervisory board has committed the offence, application may be filed also by the members of the board of directors, the shareholders or the partners authorized to represent the legal entity or the liquidators.

oder Übertragungsprüfer oder Gehilfe eines solchen Prüfers

bekannt geworden ist, unbefugt offenbart, wenn die Tat im Falle der Nummer 1 nicht in § 85 des Gesetzes betreffend die Gesellschaften mit beschränkter Haftung, § 404 des Aktiengesetzes, § 151 des Genossenschaftsgesetzes oder § 138 des Versicherungsaufsichtsgesetzes, im Falle der Nummer 2 nicht in § 333 des Handelsgesetzbuchs mit Strafe bedroht ist.

(2) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe. Ebenso wird bestraft, wer ein Geheimnis der in Absatz 1 bezeichneten Art, namentlich ein Betriebs- oder Geschäftsgeheimnis, das ihm unter den Voraussetzungen des Absatzes 1 bekannt geworden ist, unbefugt verwertet.

(3) Die Tat wird nur auf Antrag eines der an der Umwandlung beteiligten Rechtsträger verfolgt. Hat ein Mitglied eines Vertretungsorgans, ein vertretungsberechtigter Gesellschafter oder Partner oder ein Abwickler die Tat begangen, so sind auch ein Aufsichtsrat oder ein nicht vertretungsberechtigter Gesellschafter oder Partner antragsberechtigt. Hat ein Mitglied eines Aufsichtsrats die Tat begangen, sind auch die Mitglieder des Vorstands, die vertretungsberechtigten Gesellschafter oder Partner oder die Abwickler antragsberechtigt.

Act Concerning the Implementation of the EU-Regulation on the European Economic Interest Group ("EWIVAG")

Sec. 14 EWIVAG	§ 14 EWIVAG

Violation of obligation to secrecy

(1) Whoever, without authorization, discloses a secret of the organization, in particular a trade or business secret, which has come to his knowledge in his capacity as managing director or liquidator, shall be punished by imprisonment of up to one year or by fine.

(2) If such offender acted material gain or with the intent to enrich himself or another person or to harm another person, the punishment shall be imprisonment of up to two years or a fine. Whoever unlawfully uses a secret of the kind specified in subsection 1 in particular a trade or business secret, which he has learned under the circumstances of subsection 1 shall be punished in the same manner.

(3) The offence shall only be prosecuted upon request. The application must be submitted by special representatives who are appointed by the members.

Verletzung der Geheimhaltungspflicht

(1) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer ein Geheimnis der Vereinigung, namentlich ein Betriebs- oder Geschäftsgeheimnis, das ihm in seiner Eigenschaft als Geschäftsführer oder Abwickler bekanntgeworden ist, unbefugt offenbart.

(2) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe. Ebenso wird bestraft, wer ein Geheimnis der in Absatz 1 bezeichneten Art, namentlich ein Betriebs- oder Geschäftsgeheimnis, das ihm unter den Voraussetzungen des Absatzes 1 bekanntgeworden ist, unbefugt verwertet.

(3) Die Tat wird nur auf Antrag der Vereinigung verfolgt. Antragsberechtigt sind von den Mitgliedern bestellte besondere Vertreter.

Act on the participation of employees in a European Company ("SCEBG")

§ 47 SCEBG

Penal provisions

(1) Whoever
1. uses a business or trade secret contrary to sec. 43 subsection 2, also in connection with subsection 4, or
2. abuses a European Cooperative Society contrary to sec. 45 sentence 1 to withdraw employees participation rights or to withhold these,

shall be punished by imprisonment of up to two years or by fine.

(2) Whoever
1. discloses a business or trade

§ 47 SCEBG

Strafvorschriften

(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer
1. entgegen § 43 Abs. 2, auch in Verbindung mit Abs. 4, ein Betriebs- oder Geschäftsgeheimnis verwertet oder
2. entgegen § 45 Satz 1 eine Europäische Genossenschaft dazu missbraucht, Arbeitnehmern Beteiligungsrechte zu entziehen oder vorzuenthalten.

(2) Mit Freiheitsstrafe bis zu einem Jahr

secret contrary to sec. 43 subsection 2, also in connection with subsection 4,
2. impedes, influences or interferes the activities listed in sec. 46 No. 1 or No. 2 or
3. discriminates or favors a person named in sec. 46 No. 3

shall be punished by imprisonment of up to one year or by fine.

(3) If the offender acts in the cases covered by subsection 2 No. 1 for material gain or with the intent of enriching himself or a third person or of harming another person the penalty shall be imprisonment not exceeding two years or a fine.

(4) The offence shall only be prosecuted upon request. In the cases covered by subsection 1 no. 2 and subsection 2 No. 2 and No.3 the application shall be submitted by the special negotiating body, the SCE works council, the majority of employee representatives in conjunction with a procedure for the information and consultation, each member of the supervisory or administrative body, a union that represents the company and the management.

oder mit Geldstrafe wird bestraft, wer
1. entgegen § 43 Abs. 2, auch in Verbindung mit Abs. 4, ein Betriebs- oder Geschäftsgeheimnis offenbart,
2. entgegen § 46 Nr. 1 oder 2 eine dort genannte Tätigkeit behindert, beeinflusst oder stört oder
3. entgegen § 46 Nr. 3 eine dort genannte Person benachteiligt oder begünstigt.

(3) Handelt der Täter in den Fällen des Absatzes 2 Nr. 1 gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

(4) Die Tat wird nur auf Antrag verfolgt. In den Fällen des Absatzes 1 Nr. 2 und des Absatzes 2 Nr. 2 und 3 sind das besondere Verhandlungsgremium, der SCE-Betriebsrat, die Mehrheit der Arbeitnehmervertreter im Rahmen eines Verfahrens zur Unterrichtung und Anhörung, jedes Mitglied des Aufsichts- oder Verwaltungsorgans, eine im Unternehmen vertretene Gewerkschaft sowie die Leitungen antragsberechtigt.

Act on European Works Councils ("EBRG")

§ 47 EBRG

Penal provisions

(1) Whoever uses a business or trade secret contrary to sec. 35 subsection 2 sentences 1 or 2, each also in connection with subsection 3, shall be punished by imprisonment of up to two years or by fine.

(2) The offence shall only be prosecuted upon request.

§ 43 EBRG

Strafvorschriften

(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer entgegen § 35 Absatz 2 Satz 1 oder 2, jeweils auch in Verbindung mit Absatz 3, ein Betriebs- oder Geschäftsgeheimnis verwertet.

(2) Die Tat wird nur auf Antrag verfolgt.

Act on Co-determination of Employees ("MgVG")

Sec. 34 MgVG

§ 34 MgVG

Penal provisions

(1) Whoever uses a business or trade secret contrary to sec. 31 subsection 2, also in connection with subsection 4, shall be punished by imprisonment of up to two years or by fine.

(2) Whoever
1. discloses a business or trade secret contrary to sec. 31 subsection 2, also in connection with subsection 4,
2. influences, impedes or interferes the activities listed in sec. 33 No. 1 or No. 2 or
3. discriminates or favores a person named in sec. 33 No. 3

shall be punished by imprisonment of up to one year or by fine.

(3) If the offender acts in the cases covered by subsection 2 No. 1 for material gain or with the intent of enriching himself or a third person or of harming another person the penalty shall be imprisonment not exceeding two years or a fine.

(4) The offence shall only be prosecuted upon request. In the cases covered by subsection 2 No. 2 and No. 3 the application shall be submitted by the special negotiating body, each member of the supervisory or administrative body, a union that represents the company and the management.

Strafvorschriften

(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer entgegen § 31 Abs. 2, auch in Verbindung mit Abs. 4, ein Betriebs- oder Geschäftsgeheimnis verwertet.

(2) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer
1. entgegen § 31 Abs. 2, auch in Verbindung mit Abs. 4, ein Betriebs- oder Geschäftsgeheimnis offenbart,
2. entgegen § 33 Nr. 1 oder 2 eine dort genannte Tätigkeit behindert, beeinflusst oder stört oder
3. entgegen § 33 Nr. 3 eine dort genannte Person benachteiligt oder begünstigt.

(3) Handelt der Täter in den Fällen des Absatzes 2 Nr. 1 gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

(4) Die Tat wird nur auf Antrag verfolgt. In den Fällen des Absatzes 2 Nr. 2 und 3 sind das besondere Verhandlungsgremium, jedes Mitglied des Aufsichts- oder Verwaltungsorgans, eine im Unternehmen vertretene Gewerkschaft sowie die Leitungen antragsberechtigt.

<u>Act Regulating the Profession of Auditors ("WiPro")</u>

Sec. 133b WiPrO

Unauthorized utilization of third-party professional and trade secrets

(1) Using a third-party secret in violation of § 66b Section 2 is punishable by imprisonment of up to two years or a punitive fine.

(2) The offence shall only be prosecuted upon request.

§ 133b WiPrO

Unbefugte Verwertung fremder Betriebs- oder Geschäftsgeheimnisse

(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer entgegen § 66b Abs. 2 ein fremdes Geheimnis verwertet.

(2) Die Tat wird nur auf Antrag verfolgt.

Sec. 133c WiPrO	§ 133c WiPrO
Unauthorized Revealing of Third-party Professional or Trade Secrets	Unbefugte Offenbarung fremder Betriebs- oder Geschäftsgeheimnisse
(1) Revealing a third-party secret in violation of § 66b Section 2 is punishable by imprisonment of up to one year or a punitive fine.	(1) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer entgegen § 66b Abs. 2 ein fremdes Geheimnis offenbart.
(2) If such offender acted material gain or with the intent to enrich himself or another person or to harm another person, the punishment shall be imprisonment of up to two years or a fine.	(2) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.
(3) The offence shall only be prosecuted upon request.	(3) Die Tat wird nur auf Antrag verfolgt.

Company Disclosure Act ("PublG")

Sec 19 PublG	§ 19 PublG
Violation of confidentiality	Verletzung der Geheimhaltungspflicht
(1) Whoever without authorization discloses a secret of the company (executive board, part of senior management), in particular a trade or business secret, which has come to his knowledge in his capacity as auditor pursuant to this act or as assistant of such an auditor, shall be punished by imprisonment of up to one year or by fine.	(1) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer ein Geheimnis des Unternehmens (Konzernleitung, Teilkonzernleitung), namentlich ein Betriebs- oder Geschäftsgeheimnis, das ihm in seiner Eigenschaft als Prüfer nach diesem Gesetz oder als Gehilfe eines solchen Prüfers bekanntgeworden ist, unbefugt offenbart.
(2) If such offender acted material gain or with the intent to enrich himself or another person or to harm another person, the punishment shall be imprisonment of up to two years or a fine. Whoever unlawfully uses a secret of the kind specified in subsection 1 in particular a trade or business secret, which he has learned under the circumstances of subsection 1 shall be punished in the same manner.	(2) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe. Ebenso wird bestraft, wer ein Geheimnis der in Absatz 1 bezeichneten Art, namentlich ein Betriebs- oder Geschäftsgeheimnis, das ihm unter den Voraussetzungen des Absatzes 1 bekanntgeworden ist, unbefugt verwertet.
(3) The offence shall be prosecuted only upon application of the company (executive board, part of senior management).	(3) Die Tat wird nur auf Antrag des Unternehmens (Konzernleitung, Teilkonzernleitung) verfolgt.

Concerning relevant literature on this matter, the following articles might give a good overview on German law providing for criminal liability for trade secret violation:

a) Mayer, Geschäfts- und Betriebsgeheimnis oder Geheimniskrämerei? (Trade secrets or secretiveness?), GRUR 2011, 884 et seq.

This article summarizes the requirements and the scope of protection of Sec. 17 of the Act Against Unfair Competition, which is the most important provision concerning the protection of trade secrets under German law. The author therefore describes the constituent elements of the provision and comments on the most relevant aspects and problems in regard to Sec. 17 of the Act Against Unfair Competition.

b) Rützel, Illegale Unternehmensgeheimnisse? (Illegal trade secrets?), GRUR 1995, 557 et seq.

The author considers the question of whether illegal secrets should be regarded as trade secrets or if only secrets that are coincide with the law should be protected by the law. In his explanations he takes many provisions into consideration which serve the protection of trade secrets, such as Sec. 17 of the Act Against Unfair Competition or Sec. 203 German Criminal Code.

c) Kiethe/Hohmann, Der strafrechtliche Schutz von Geschäfts- und Betriebsgeheimnissen (The protection of trade secrets under criminal law), NStZ 2006, 185 et seq.

In this paper the author describes the protection of trade secrets under criminal law and explains the most relevant provisions and its elements. Furthermore the author points out the importance of the protection of trade secrets as German companies suffer billions of Euros of damage every year as a result of industrial espionage.

d) Mautz/Löblich, Nachvertraglicher Verrat von Betriebs- und Geschäftsgeheimnissen (Post-contractual disclosure of trade secrets), MDR 2000, 67 et seq.

This article provides an overview over the legal protection of trade secrets regarding the violation through former employees involving problems of the procedural enforcement.

e) Többens, Die Straftaten nach dem Gesetz gegen den unlauteren Wettbewerb (Criminal offenses in the context of the Act Against Unfair Competition), WRP 2005, 552 et seq.

In this article, the author summarizes the protection of trade secrets stipulated by the Act Against Unfair Competition and simultaneously provides a comprehensive overview of the statutory offences.

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily peruse to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantage from use)?

As a subjective element Sec. 17 Act Against Unfair Competition requires that the infringer must have acted either for competition purpose, for personal gain, for the benefit of a third party or with the intent of causing damage to the owner of the business.

Acting for the purposes of competition is to be assumed if it is objectively appropriate and covered by the intention of the infringer to promote the sale or purchase of a competitor to the disadvantage of the business owner. Acting for personal gain is any action to achieve direct or indirect, material or immaterial personal advantages. Acting for the benefit of a third party is to be assumed if it is directed to achieve any type of advantage for a third party, regardless if it is based on an unselfish motivation of the infringer. The intent of causing damage to the owner of the business requires that the infringer acts target-orientated to cause material or immaterial damages.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

German law ensures the protection of trade secrets by the supplementary penal provisions listed above (c.f. Question 1). The violation of these provisions constitutes a misdemeanor, threatened by imprisonment or by a fine, and can lead to criminally prosecution. In particular in the case of industrial espionage pursuant to Sec. 17 (2) No. 1 Act Against Unfair Competition, the violation of trade secrets can entail further criminal offences like theft of unlawful appropriation.
Besides their function as criminal offences, the provisions which provide for criminal protection of trade secrets can constitute the basis for civil law claims in conjunction with civil law provisions.

4. Do the relevant provisions establish any "save harbour" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "fair use", "just cause", "de minimis threshold")?

The relevant provisions which provide for criminal protection of trade secrets do not contain any "save harbour" clauses or specific conditions under which the offender may not be prosecuted, such as "fair use", "just cause", "de minimis threshold".

However, the disclosure of a trade secret can be, in principle, legally justified based on the principles of necessity according to Sec. 34 Criminal Code. Pursuant to Sec. 34 Criminal Code, an act can be justified if it is committed to avert an imminent danger to life, limb, freedom, honour, property or another legal interest of the offender or any other person which cannot otherwise be averted if the protected interest substantially outweighs the one interfered with. In this context, a justification of the disclosure of trade secrets is discussed in the legal literature, in particular, if the offender acts in order to protect its own assets and legal interests but also in connection with whistle blowing.

Furthermore, the disclosure of trade secrets can be justified if the disclosing person is legally obliged to render information or to testify in course of criminal proceedings.

5. May the sole risk of dissemination or disclosure give rise to criminal liability?

Under German law, the sole risk of dissemination or disclosure does not give rise to criminal liability. The relevant provisions which provide for criminal protection of trade secrets refer to the attempt of the disclosure of trade secrets as the earliest moment of criminal liability. The liability for attempt as well as the beginning of the attempt is ruled in the Criminal Code.

According to Sec. 22 Criminal Code, an offender attempts to commit an offence if he/she takes steps which will immediately lead to the completion of the offence as envisaged by the offender. Therefore, the criminal liability of an attempt begins at the latest when the offender starts to carry out at least one of the objective elements of the offence. Mere acts preparatory to the commission of the offence have to be differentiated from the attempt and, principally, remain unpunished. In connection with most of the relevant provision which provide for criminal protection of trade secrets, the offender must take steps, as envisaged by him, which will immediately lead to the disclosure or non-authorized use of the trade secret.

Sec. 19(1) and (2) Act against Unfair Competition constitute an exemption to the above mentioned principles. The provision is aimed on the extension of the criminal protection of trade secrets by including certain preparatory acts. Sec. 19(1) Act against Unfair Competition imposes penalties on the unsuccessful attempt to procure another person to commit the disclosure of trade secrets pursuant to Sec. 17 Act against Unfair Competition or to commit the non-authorized use or communication of models pursuant

to Sec. 18 Act against Unfair Competition. Furthermore, pursuant to Sec. 19(2) Act against Unfair Competition, it is a punishable offence to offer or to accept the offer of another person or to conspire with another person to commit a criminal offence pursuant to Section 17 or Section 18 Act against Unfair Competition.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

Most of the provisions which protect against the violation of trade secrets sanction the unauthorized disclosure or use of trade secrets committed by certain professionals and require that the offender must have obtained the trade secret in course of its professional activities or responsibilities.

For example, Sec. 17(1) of the Act Against Unfair Competition protects against trade secret violation by employees of a company and requires that the employee was entrusted or granted access to the trade secret during the course of the employment. The term "employee" is interpreted in a broad sense and includes, beside typical employer-employee relationships, also dependent services providers who provide services to the company without carrying risks of profits and losses. Other provisions embrace certain professionals who typically act as secret carriers or often get in touch with secret information such as attorneys, accountants but also legal representatives of private juristic persons. A punishable offence is not committed if the knowledge of the trade secret is acquired before entering into or after the end of the professional relationship or if it is acquired only in course of private matters.

An exception to the above is Sec. 17(2) No. 1 UWG of the Act Against Unfair Competition which provides for protection of trade secrets against industrial espionage. Unlike the other relevant provisions, the group of persons who may commit the offence is not limited to certain professionals or persons affiliated with the company. The offence of industrial espionage can be committed by anybody. As the prohibited act, Sec. 17(2) No. 1 Act Against Unfair Competition denominates the unauthorized procurement or saving of trade and business secrets either by using technical means, creating an embodied communication of the secret or by removing an item in which the secret is embodied.

A further exception to the above is Sec. 17(2) No. 2 of the Act Against Unfair Competition which, like Sec. 17(2) No. 1 Act Against Unfair Competition, is not limited to certain professionals or persons affiliated with the company but can be committed by anybody. Sec. 17(2) No. 2 of the Act Against Unfair Competition sanctions the handling of unlawfully acquired trade secrets and requires a punishable underlying violation of trade secrets. Subject of the protection of Sec. 17(2) No. 2 of the Act Against Unfair Competition are trade secrets that the offender either

- acquired through communication of an employee pursuant to Sec. 17(1) Act against Unfair Competition (i.e. all legal requirement of Sec. 17(1) Act against Unfair Competition must be fulfilled by the employee, in particular, the communication must had taken place at a time when this employee was employed at the relevant company),

- or through an own or a third parties act of industrial espionage pursuant to Sec. 17(2) No. 1 Act against Unfair Competition,

- or otherwise acquired or saved the trade secret in an unauthorized manner.

The prohibited act is the unauthorized use of the trade secret, whereas the term "use" means every exploit of the secret knowledge or information through its application or implementation conforming to the purpose of the secret in practice.

In all cases of trade secret violation sanctioned by Sec. 17 UWG of the Act Against Unfair Competition, the offender must have acted either for the purpose of competition, or in self-interest, in the interest of a third party or with the intent to afflict damage on the owner of the business. The threatened punishment is identical, regardless which alternative of trade secret violation pursuant to Sec. 17 of the Act Against Unfair Competition.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

German criminal law provisions as well as the intellectual property law provisions refer to an identical notion of trade secrets and coherently use the term "trade and business secrets" (as regards the definition of the term "trade and business secrets", reference is made to Question 9). The parallelism of the criminal law provisions and the intellectual law provision is furthermore determined by the fact that the criminal law provisions, in particular, Sec. 17 of the Act Against Unfair Competition build the basis for civil law claims, including intellectual law claims, such as injunctive relief and compensation claims. Hence, a violation of the criminal law provisions implies civil law liability.

Sec. 4 No. 9 lit. c Act Against Unfair Competition, as a civil law provision, builds a separate basis for civil law claims against the violation of trade secrets which simultaneously results in criminal offences. Sec. 4 No. 9 lit. c of the Act Against Unfair Competition prohibits the offer of products that are replicas of products of a competitor if the copyist dishonestly obtained the knowledge or documents needed for the replicas. It is generally recognized that dishonest obtaining in the sense of Sec. 4 No. 9 lit. c Act Against Unfair Competition include all acts punishable under criminal law provisions which provide for protection of trade secrets, in particular, Sec. 17 and 18 Act Against Unfair Competition. Furthermore, also Sec. 4 No. 9 lit. c of the Act Against Unfair Competition requires that the information obtained are secret. If the information is public knowledge dishonesty is excluded. Consequently, there are no conducts prohibited under intellectual property law which do not result in criminal offences.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

The relevant German provisions which provide for criminal protection of trade secrets contentiously refer to the term "trade and business secrets". The distinction between trade secrets and business secrets is more of theoretical nature and only serves the purpose for clarification. Both terms are comprehensively used to refer to financial and company secrets and are protected in exactly the same way. The central term of trade and business secrets is not defined by law. According to consistent case law, the concept of trade and business secrets covers all information

- which are connected to the business and

- which are not in the knowledge of the public domain but only available to a limited group of persons and

- for which the company owner has communicated the intention to keep the information secret and

- which is subject of the company owner's objectively legitimate economic interest in observing secrecy.

As those four important criteria determine if information can be regarded as a trade secret they shall be explained in more depth hereafter:

(1) Information connected to the business

Firstly only such information is protected which relates to the relevant business, so that only information can be protected which relates to the company's sphere and not solely to the private sphere of the owner or the employees. Equally information assigned to other companies or the general market can not be considered as trade secrets.

(2) Not public knowledge

Secondly the information must not be public knowledge, so it must not belong to the public domain but only a restricted group of people. The owner of the secret must therefore maintain control over this group of people and ensure that others are excluded from the knowledge. Otherwise the knowledge can not be regarded as secret. The notion of the group of people can not be generally specified as this depends on the relevant circumstances of the individual case. Generally speaking the information cannot be regarded as a trade secret any more when it becomes known to wider circles with the consequence that the secret is lost. Information is part of the pubic knowledge when the knowledge can be acquired by normal means in a way that the interested average salesman can acquire the information without mayor difficulties and the aid of honest means.

Passing the information to another party does however not lead to the loss of the secret as long as this party is bound to confidentiality.

(3) Expressively kept secret

Thirdly the owner of the secret must have the intention to keep the specific knowledge as a secret, which distinguishes trade secrets from information that is simply not known. The company owner will either have to be expressively declared or to be contained in the nature of the information itself.

(4) Legitimate commercial interest

Lastly the company owner must have a legitimate interest in keeping the information secret, which is the case when the information could have an impact on the competitiveness of the company so that common knowledge of the information could haul the competitor's business or weaken the own one.

As long as these four cumulative requirements are met, there is no limitation as to the items of the information protected as trade and business secret, in particular, whether it is more technology related, customer related or concerns the internal organization of the company.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

As described above (c.f. Question 9), trade secrets have to meet four specific requirements in order to avail themselves of the relevant legal protection. Under German law, all information is considered trade secrets that is (1) connected to the business which is (2) not public knowledge, and that (3) shall be expressively kept secret for the purpose of economic interest, whereas (4) the business owner needs to have a legitimate commercial interest in keeping the information secret. The patentability of the items covered by trade secrets does not impact on the extent of the protection granted by law.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

German law provides for criminal protection of registered trademarks (national trademarks, IR-marks with designation in Germany as well as CTMs), registered patents, registered utility models, registered designs and registered variety denominations. Furthermore, German law provides for criminal protection of certain unregistered IP rights, namely, unregistered national trademarks which have acquired prominence due to use, unregistered trademark which are well-known within the meaning of Article 6-bis of the Paris Convention, trade designations, appellations of geographical origin as well as of copyrights.

In this context, the most important provisions are Sec. 143 of the Trademark Act, Sec. 142 of the Patent Act, Sec. 25 of the Act on designs and Utility Models, Sec 14 of the design Act and Sec. 106 of the Copyright Act. The potential penalties in the relevant provisions range from monetary fines up to three year imprisonment and, in especially serious cases, up to five years.

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

If Sec. 17 to 19 Act Against Unfair Competition are violated, criminal prosecution against the offender are initiated by the public prosecution office only upon application of the aggrieved party and, additionally, if the public prosecution office considers the criminal prosecution to be in the public interest. The public interest can be assumed on basis of general preventive reasons or special preventive reasons, for example, if a criminal prosecution can prevent further damages from the aggrieved party. If the public prosecution office denies a public interest the aggrieved party can bring private prosecution against the offender before the criminal court. Beside that, criminal prosecution can be initiated ex officio and without application of the of the aggrieved party if the criminal prosecution authority considers that it is necessary to take ex officio action on account of the particular public interest. The particular public interest is usually only assumed if essential public interests are endangered or violated.

In the case of the violation of other provisions than Sec. 17 to 19 of the Act Against Unfair Competition, criminal prosecution against the offender are initiated by the public prosecution office only upon application of the aggrieved party; ex officio action is foreclosed. If the aggrieved party demands for criminal prosecution but criminal prosecution authority considers the offender's guilt to be of a minor nature and there is no public interest in the prosecution, the public prosecution office can dispense with prosecution with the approval of the court. In this situation, the aggrieved party foreclosed from initiating private prosecution.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

In the case of violation or abuse of trade secrets, the general rules of evidence according to the Code of Criminal Procedure are applicable. The guiltiness of the offender must be fully proved with evidence by witnesses, documentary evidence, evidence by inspection or expert evidence. It is not required to present specific evidence which rise above that in order to prove an abuse of trade secrets.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade

secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

Under German law, criminal investigation proceedings are guided by the public prosecution authority. Therefore, it is the public prosecutor who supervises and conducts all steps and actions in order to gather the relevant evidence. In this context, the public prosecution authority can for example order searches of dwellings or of other premises, seize documents and other items and examine the accused persons. In course of criminal proceedings, the aggrieved party is not entitled to apply for an ex parte order in order to gather or secure relevant evidence. The aggrieved party is also not entitled to apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets or for a precautionary seizure to avoid the continuation of the offence and the perpetuation of the consequences thereof. The aforesaid also applies if the aggrieved party brings private prosecution against the offender in the case of a violation of trade secrets pursuant to Sec. 17 – 19 of the Act Against Unfair Competition.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

No, German law does not provide for criminal liability of legal persons. Criminal prosecution can only be directed against individuals and only individuals can be liable to prosecution.

2. If so, which type of liability arises for companies? Which penalties shall apply?

Not applicable

3. Which court may adjudicate cases of liability of companies for such trade secrets violation?

Not applicable

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

As already mentioned in the Answer to Question 7 of the Criminal Law Questionnaire, most of the provisions which protect against the violation of trade secrets sanction the unauthorized disclosure or use of trade secrets committed by certain professionals and require that the offender must have obtained the trade secret in course of its professional activities or responsibilities. However, this does not mean that the offender has to be imposed in any case with (contractual) obligations of confidentiality which the offender violates when disclosing the trade secret.
For example, Sec. 17(1) of the Act Against Unfair Competition, as one of the most important criminal law provision against violation of trade secrets, protects against trade secret violation by employees of a company and requires that the employee was entrusted or granted access to the trade secret during the course of the employment. The term "employee" is interpreted in a broad sense and includes, beside typical employer-employee relationships, also dependent services providers who provide

services to the company without carrying risks of profits and losses. In this context, it is irrelevant whether or not an employee in the sense of Sec. 17(1) of the Act Against Unfair Competition Law is imposed with specific obligation to keep secret information obtained in course of its professional activities or responsibilities.
Other provisions, like for example Sec. 203 Criminal Code, Sec. 85 Limited Liability Company Act or Sec. 404 Stock Corporation Act, embrace certain professionals or representatives who typically act as secret carriers or often get in touch with secret information, such as attorneys, accountants but also legal representatives of private juristic persons. In the case of these provisions the specific obligation of professional discretion is functionally caused. A further going expressively imposed obligation of confidentiality is not necessary.
As an exception to the above, Sec. 17(2) No. 1 and No. 2 of the Act Against Unfair Competition do not require a special relation between the offender and the aggrieved person but can be committed by anybody.
Sec. 17(2) No. 1 of the Act Against Unfair Competition provides for protection of trade secrets against industrial espionage. Unlike the other relevant provisions, the group of persons who may commit the offence is not limited to certain professionals or persons affiliated with the company. The offence of industrial espionage can be committed by anybody. As the prohibited act, Sec. 17(2) No. 1 of the Act Against Unfair Competition denominates the unauthorized procurement or saving of trade and business secrets either by using technical means, creating an embodied communication of the secret or by removing an item in which the secret is embodied.
Also Sec. 17(2) Nr. 2 of the Act Against Unfair Competition is not limited to certain professionals or persons affiliated with the company but can be committed by anybody. Sec. 17(2) Nr. 2 of the Act Against Unfair Competition sanctions the handling of unlawfully acquired trade secrets and requires a punishable underlying violation of trade secrets.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

As far as criminal proceedings are concerned, the offender of a trade secret violation does not need to qualify as a competitor or potential competitor of the owner of the disclosed trade secret.
As already mentioned in the Answer to Question 1 of the Criminal Law Questionnaire, most of the relevant provisions which provide for criminal liability for trade secret violation have in common that the later on disclosed trade secret must have been confided or become known to the offender in course of his professional occupation for the aggrieved party. This does not necessarily require an employer-employee relationship so that, for example, also external persons like certified public accountants can be liable for punishment. However, depending on the concrete provision a certain professional relationship between the offender and the aggrieved party is generally required. As an exception to the above, the criminal liability for industrial espionage pursuant to Sec. 17(2) No. 1 of the Act Against Unfair Competition and the handling of unlawfully acquired trade secrets pursuant to Sec. 17(2) No. 2 of the Act Against Unfair Competition limited to certain professionals or persons affiliated with the company. These offences can be committed by anybody.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

Under German law, the aggrieved person cannot bring a claim for damages in course of criminal proceedings. Damages claims can only be asserted by the aggrieved person in course of a - legally independent - civil lawsuit against the offender of the trade secret violation.

Greece

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Greek law provides for criminal liability in cases of trade secrets violation. More specifically:

(i) Article 16 of L. 146/1914 on unfair competition.

"A punishment of imprisonment for a term not exceeding six months and a fine (not exceeding three thousand drachmas[1]), or either of these penalties, shall be imposed upon any employee, worker or trainee of a commercial or industrial establishment or enterprise who, during the term of his employment, without authorization, communicates to third parties secrets of the establishment or the enterprise that have been confided to him by virtue of his employment relationship, or have been otherwise brought to his knowledge, if he does so for purposes of competition, or with the intention of damaging the proprietor of the establishment or the enterprise.

The same punishment shall be imposed also upon anyone who, without authorization, makes use of, or communicates to third parties, for purposes of competition, such secrets, if his knowledge of them has been gained through one of the communications designated in the preceding section, or through his own acts in violation of the law or the principles of morality".

In light of articles 18 and 53 of the Greek Penal Code[2], the crime designated in article 16 of L. 146/1914 is a misdemeanor. The potential penalty for the offender is imprisonment for a term ranging from 10 days up to 6 months and/or a fine not exceeding 3.000 drachmas (8,80 Euros).

(ii) Article 17 of L. 146/1914 on unfair competition.

"The punishment of the preceding Article shall be imposed upon anyone who, without authorization, makes use of, or communicates to third parties the models or technical standards that have been confided to him in the course of business, and in particular drawings, prototypes, patterns, samples or instructions".

The crime designated in this article is a misdemeanor, while the potential penalty for the offender is imprisonment for a term ranging from 10 days up to 6 months and/or a fine not exceeding 3.000 drachmas (8,80 Euros).

[1] In the above provision, drachmas were not converted into Euros. For your convenience, please note that 3.000 drachmas correspond to 8.80 Euros

[2] **Article 18** of the Greek Penal Code provides that "any act punished by the penalty of death or incarceration, is a felony. Any act punished by imprisonment or fine or restriction in a special youth detention facility, is a misdemeanor. […]".
Article 53 of the Greek Penal Code provides that "the duration of imprisonment is longer than ten days but does not exceed five years".

(iii) Article 18 par. 2 of L. 146/1914 on unfair competition.

"The punishments provided in Article 16, reduced by half, shall apply to anyone who, for purposes of competition, attempts to induce another to commit an act in violation of the provisions of Article 16 section 1 and of Article 17.

The crime designated in this article is a misdemeanor, while the potential penalty for the offender is imprisonment for a term ranging from 10 days up to 3 months and/or a fine not exceeding 1.500 drachmas (4,40 Euros).

(iv) Article 370B of the Greek Penal Code.

"1. Any person who, acting in an unfair manner, copies, imprints, uses, discloses to a third party, or in any way violates data or computer programs, which constitute State, scientific or professional secrets, or secrets of an enterprise of the public or private sector, is punished by imprisonment for a term of at least three months. As secret is also considered any information which its legal owner, out of reasonable interest, treats as confidential, especially when he has taken measures in order to prevent third parties to take knowledge of it.

2. If the offender is in the service of the owner of the data, and if the secrets are of great financial significance, imprisonment of at least 1 year shall be imposed.

3. […]

4. The actions provided in paragraphs 1 and 2 are prosecuted further to the filing of a complaint".

The crime designated in this article is a misdemeanor, while the potential penalty for the offender is: for the crime of paragraph 1, imprisonment for a term ranging from 3 months up to 5 years; for the crime of paragraph 2, imprisonment for a term ranging from 1 year to 5 years.

Apart from the above, the following provisions also aim to the protection of secrets in general (official secrets, professional secrets), including trade secrets. The following provisions differ from the ones designated above, in that they establish, for example, specific qualities for the offender, they do not aim to the protection of trade secrets only, and, finally, refer to acts committed for purposes other than competition.

(i) Article 13 par. 4 and 5, and Article 17 par. 3 of L. 1767/1988 on Works Councils of enterprises.

Art. 13 par. 4: "The employer is not obliged to provide the Works Councils with information related to issues that are considered to be secrets according to the current legislation, such as the bank secrecy, the legal professional privilege, issues of national security or patents".

Art. 13 par. 5: "The members of the Works Councils are obliged not to communicate to third parties, without the employer's authorization, information related to the issues designated in the previous paragraph, or information of high importance for the enterprise, the disclosure of which would cause harmful consequences for the competitiveness of the enterprise".

Art. 17 par. 3: "The provision of article 16 of L. 146/1914 shall also apply to the members of the works councils, for a term of 5 years after the termination of their

employment, in case they violate their duty of confidentiality, provided in art. 13 par. 5 of this law".

The crime designated in these articles is a misdemeanor and the potential penalty for the offender is imprisonment for a term ranging from 10 days up to 6 months and/or a fine not exceeding 3.000 drachmas (8,80 Euros).

(ii) Article 63 par. 1 section a' of L. 2190/1920 on Societe Anonyme.

"Any civil servant, who supervises Societes Anonymes and does not keep absolute confidentiality of any and all things he observed/noted during the operation of the company, shall be punished by imprisonment".

The crime designated in this article is a misdemeanor and the potential penalty for the offender is imprisonment for a term ranging from 10 days up to 5 years.

(iii) Article 63C par. 2 of L. 2190/1920 on Societe Anonyme.

"Any auditor of a societe anonyme who does not keep absolute confidentiality of any and all things he observed/noted during the operation of the company, shall be punished by imprisonment of maximum three (3) months".

The crime designated in this article is a misdemeanor and the potential penalty for the offender is imprisonment for a term ranging from 10 days up to 3 months.

(iv) Article 252 of the Greek Penal Code (Violation of Official Secrecy).

"1. Any civil servant who, beyond the cases analyzed in articles 248 (*Violations by post office employees)*, 249 (*Violations by employees of the Telegraphic Service)*, 250 (*Violations by employees of Telecommunication Service)* and 251 (*Violation of judicial confidentiality),* in violation of his duties, communicates to a third party:

(a) anything that came to his knowledge strictly due to his Service, or

(b) any document which has been confided to him or to which he has access due to his Service, shall be punished by imprisonment of at least three (3) months, if he has committed one of the above actions in order to gain a personal benefit, or to damage the State or someone else.

2. Anyone who serves, by virtue of a relation of any kind, to the Political Bureau of the Prime Minister, of the Ministers or the Deputy Ministers, especially as an associate specialist, special advisor, administrator, official on secondment or official to which certain duties have been assigned, contractor, and/or as a member of working groups or committees, and communicates to others: a) any information which came to his knowledge strictly due to his Service or b) any document which has been confided to him or to which he has access due to his Service, shall be punished by imprisonment of at least six (6) months. If he commits said act in order to gain a personal benefit or to create a benefit for someone else or to harm the State or someone else, shall be punished by imprisonment of at least one (1) year and a fine, ranging from 100.000 up to 500.000 Euros.

3. The penalties of the preceding paragraphs shall also apply to any third party who makes use of the information or the document, knowing its source, in order to gain a personal benefit, to create a benefit for someone else, or to harm the State or someone else.

Use of the information or the document within the necessary limits, which takes place for the satisfaction of a reasonable interest for the notification of the public, does not constitute an illegal act".

The crime designated in this article is a misdemeanor, while the potential penalty for the offender is: for the crime of paragraph 1, imprisonment for a term ranging from 3 months up to 5 years; for the crime of paragraph 2 section (a), imprisonment for a term ranging from 6 months up to 5 years; for the crime of paragraph 2 section (b), imprisonment for a term ranging from 1 year up to 5 years and a fine ranging from 100.000 up to 500.000 Euros; for the crime of paragraph 3, the penalties of paragraphs 1 or 2 shall apply accordingly.

(v) Article 371 of the Greek Penal Code (Violation of professional confidentiality).

"1. Any cleric, lawyer and legal assistant of any kind, notary, doctor, midwife, nurse, pharmacist or other person to whom, due to his profession or capacity, others usually confide their private secrets, as well any assistant of the above mentioned persons, who discloses the private secrets that have been confided to him or came to his knowledge due to his profession or capacity, shall be punished by a fine or by imprisonment of maximum 1 year.

2. The same punishment shall be imposed upon anyone who, following and due to the death of one of the persons designated in par. 1, possesses documents or notes of the dead, relative to his profession or capacity, and discloses private secrets out of such documents or notes.

3. Legal prosecution starts only further to the filing of a complaint.

4. If the offender aimed to the performance of his duty or to the preservation of a legal - or, for any other reason, justified - substantial interest, either public or his own, or of someone else, which could not be otherwise preserved, his act is not considered to be illegal and does not entail any punishment".

The crime designated in this article is a misdemeanor, and the potential penalty for the offender is a fine ranging from 150 up to 15.000 Euros[3], or imprisonment for a term ranging from 10 days up to 1 year.

(vi) Article 390 of the Greek Penal Code (Breach of trust).

"Anyone who damages knowingly someone else's property, the management of which has been entrusted to him (totally or partially or only with regards to a specific action) by virtue of a law or a legal act, shall be punished by imprisonment of at least three (3) months. In case the damage caused to the property exceeds the amount of fifteen thousand (15.000) Euros, the offender shall be punished by incarceration of maximum ten years".

It should be clarified that this article establishes a general criminal liability for cases of breach of trust on behalf of persons that have been entrusted with the management of another's property. Especially with regards to trade secrets violation, this article may apply in cases where, for instance, the legal representative or a member of the Board of Directors of a legal entity violates the trade secrets of such legal entity, and provided that the application of the "lex specialis" (art. 16 section [b] of L. 146/1914) is not possible because its requirements are not met.

[3] Article 57 of the Greek Penal Code provides that "unless special provisions provide differently, the amount of the fine may not be less than 150 Euros, nor higher than 15.000 Euros.

The crime designated in section (a) of this article (390 of Greek Penal Code) is a misdemeanor, while the potential penalty for the offender is imprisonment for a term ranging from 3 months up to 5 years. The crime designated in section (b) of this article is a felony, and the potential penalty for the offender is incarceration for a term ranging from 5 to 10 years[4].

With regards to the legal value protected under the above criminal legal framework, it should be noted that in general, trade secrets are protected under their quality as legal values having an economic value. Trade secrets are considered to be intangible assets, connected with their owner with a proprietary/economic relationship, and constitute part of his property. More specifically:

The acts designated in articles 16 and 17 of L. 146/1914 constitute on the one hand cases of financial crimes and, on the other hand, crimes against the goods of individuals, among which the property is also included.

The legal value protected under Art. 252 of the Greek Penal Code is the proper operation of the Public Service and, in particular, the interest of the State for the observance of the obligation of confidentiality with regards to official secrets, as well as the interest of individuals who may be harmed by the violation of the official confidentiality obligation.

With regards to articles 370B and 371 of the Greek Penal Code, it should be noted that both of them are included in the section of Penal Code which refers to the "Violation of Secrets". In particular, the legal value protected under article 370B is, according to one opinion of the legal theory, the property in its broad sense, given that digital data referring to e.g. research and analysis results, lists of customers, business plans, etc, express/embody an economic value; according to another opinion of the legal theory, the legal value protected under this provision is the information itself (which has been saved in a digital form). On the other hand, the legal values protected under article 371 are the individual and trade secrets, as well as the trust of the public towards certain professionals.

The legal value protected under article 390 of the Greek Penal Code, is the property, which includes any and all goods belonging to one person, which have an economic value.

Finally, the legal value protected under articles 63 par. 1 section a and 63C par. 2 of L. 2190/1920, is trade secrets themselves.

List of Literature available on the matter.

(i) G.N. Michalopoulos, "*Unfair Competition",* (edited by Nik. K. Rokas), Nomiki Vivliothiki, Athens, 1996, pp. 401-416.

This reference provides a definition of the legal concept of "secrets", lists the categories of secrets and analyzes their protection under articles 16 – 18 of L. 146/1914 of Unfair Competition. Reference is also made to other legal provisions which, although not aiming directly and exclusively to the protection of trade secrets, are part of the legal framework for the protection of secrets. Finally, it analyzes how trade secrets are treated in the Greek Codes of Civil and Penal Procedure.

(ii) Anastasia Ant. Voudrisli, "*Trade Secrets and their protection under Greek law",* Aristotle University of Thessaloniki, Thessaloniki 2008, pp. 1 – 34 and 52 – 58.

This reference defines the elements of the legal concept of "trade secrets" and points out the differences between trade secrets and patents, intellectual property works and bank

[4] Article 52 par. 3 of the Greek Penal Code provides that "the duration of temporary incarceration does not exceed 20 years and may not be less than 5 years [….]".

secrets. It also defines the legal nature of trade secrets and the persons who are obliged to respect their confidentiality; it also analyzes protection of trade secrets under L. 146/1914 and article 370B of the Greek Penal Code.

(iii) Lambros E. Kotsiris, "*Competition Law – Unfair and Free",* Sakkoulas Publications, 4th Edition, May 2001, pp. 309 – 323,

which makes reference to the economic and legal importance of trade secrets, defines the legal concept of trade secrets and analyzes their protection under L. 146/1914 on unfair competition.

(iv) Mich. – Theod. Marinos, "*Unfair Competition"*, Sakkoulas Publications Dikaio & Oikonomia, 2nd Edition, Athens 2009, pp. 243 – 250,

which analyzes the legal definition of trade secrets, and sets the legal framework for their protection on the basis of L. 146/1914 on unfair competition. Reference is also made to articles 252, 370, 371 and 390 of the Greek Penal Code, as ways to preserve the economic value of trade secrets.

(v) Anthoula P. Papadopoulou, "*Trade Secrets",* Sakkoulas Publications, 2007, pp. 1 – 191 and 236 – 252,

which makes reference to the "secret" as a legal value protected by law. Furthermore, it defines the legal concept of trade secrets and lists the elements of such legal concept; it also lists the categories of trade secrets (commercial secrets, confidential information, industrial secrets and know-how). It makes reference to computer programs and databases and to their protection as trade secrets and intellectual property works, as well as to the reasons which made necessary the legal protection of trade secrets. The author also makes a comparative analysis of trade secrets and patents, intellectual property works and other types of secrets, such as bank secrets and stock exchange secrets. Reference is also made to the legal nature of trade secrets and to the duration of their protection. Finally, an analysis of legal protection of trade secrets is provided, on the basis of L. 146/1914, L. 1767/1988 on works councils, and on art. 370 B of the Greek Penal Code.

(vi) Christos Milonopoulos, "*The penal protection of software under Greek law",* Poinika Chronika, Volume of year 1988, pp. 3 – 27,

which analyzes the ways of violation of software and the possible ways for its protection, on the basis of the provisions of the Greek Penal Code, of intellectual property law and of unfair competition law.

(vii) Aggelos Konstandinidis, "*The obligation to testify and Trade Secrets in criminal trials*", Research Institute of Procedural Studies, Volume B', Sakkoulas Publications, 1991, pp. 104 – 134,

which defines the legal concept of trade secrets and analyzes the legal framework for their protection on the basis of articles 16 – 18 of L. 146/1914. It also makes reference to the conflict between the obligation to testify and the protection of trade secrets, given that L. 146/1914 does not specifically provide for this matter. Furthermore, it analyzes the duty of confidentiality on behalf of the employees, according to the provisions of L. 1767/1988 on Works Councils and makes reference to the conflict between such duty and the obligation for testimony. The author also comments on the constitutional base of "secrecy".

(viii) Irini Vassilaki, "*Software piracy and articles 16-17 of L. 146/1914",* Nomiko Vima 1988, pp. 1338 – 1344,

which refers to the problem of software piracy and deals with the protection of software in the framework of the articles 16 and 17 of L. 146/1914.

(ix) Evaggelos Perakis, "*The law of Societe Anonyme",* Volume 2, Nomiki Vivliothiki, 3rd Edition, 2010, pp. art. 63 of L. 2190/1920, pp. 2128 – 2134 and art. 63C of L. 2190/1920, pp. 2143 – 2149,

which provides an analysis of said articles of L. 2190/1920.

(x) Aristotelis Charalambakis – Ioannis Giannidis, "*Penal Code and Case Law",* Sakkoulas Publications Dikaio & Oikonomia, Athens 2009, art. 252, pp. 950 – 953, art. 370, pp. 1620 – 1623, art. 371, pp. 1625 – 1628, art. 390, pp. 1813 – 1820,

where an analysis of the articles of Greek Penal Code is available.

(xi) Michail Margaritis, "*Penal Code",* Sakkoulas Publications Dikaio & Oikonomia, Athens 2003, art. 252, pp. 665 – 667, art. 370B, pp. 1024 – 1026, art. 371, pp. 1027 – 1032, art. 390, pp. 1181 – 1186,

Where an analysis of the articles of Greek Penal Code is available.

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

Some of the above mentioned legal provisions establish specific requirements as to the purposes that the offender must pursue, in order to be charged with violation of trade secrets. More specifically:

In art. 16 section (a) of L. 146/1914, the offender must act for purposes of competition, or with the intention of damaging the proprietor of the establishment or the enterprise to which the trade secrets relate. These two elements do not need to be cumulative, but only one of them (purpose of competition or intention of damaging the proprietor of the establishment or the enterprise) is enough for the offender to be charged for violation of trade secrets on the basis of this provision.

In particular, the "*purpose of competition*" that the offender must pursue in this case, consists of two separate elements:

(a) The conduct of the offender must be objectively suitable to serve the purpose of competition - i.e. to enhance the competitiveness of the offender or of a third party - while a relation of competition is also necessary. In other words, the acts of the offender must be objectively suitable to have an impact in competition and enforce competitors, with regards e.g. to their position in the market, to their revenue, etc. Furthermore, in order for an act to be suitable to have an impact in competition, the injured party and its competitors need to be connected with a relation of competition. This is due to the fact that competition acts may be committed only by competitors, who have the same or similar customers and engage in the same or similar market - in terms of location and type of merchandise or services - or where the competitors belong to the same or close economic level and aim to the same or similar type of customers, suppliers, etc; the possibility of a competitor (evaluated by an objective point of view) to expand his commercial activities and thus, aims to the same body of customers, is enough to constitute a relation of competition.

(b) Intention of competition, i.e. intention to enhance the competitiveness of the offender or of a third party. Commitment of an act on behalf of a competitor, which is objectively suitable to enhance his or someone else's competitiveness, has led to the creation of a presumption that there is actually intention of competition.

With regards to the "*damage of the proprietor of the establishment or the enterprise*", it should be noted that it may also be indirect, meaning that it also includes cases where a third party gains a benefit in the competition.

In art. 16 section (b) of L. 146/1914, it is established that the offender must act for purposes of competition.

In art. 18 par. 2 of L. 146/1914, it is established that the offender must act for purposes of competition.

In art. 252 of the Greek Penal Code, it is established that the offender must act in order to gain a personal benefit, or to damage the State or someone else. The benefit or damage may be either direct or indirect; it must not necessarily have an economic nature, but it may also be a moral damage.

All other criminal provisions do not establish any specific requirement as to the purposes that the offender must pursue in order to be charged.

However, it should be noted that in all cases, the offender must act intentionally, and not by negligence.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

Violation of trade secrets may in some cases establish commitment of other crimes as well, e.g. violation of Intellectual Property law (where the trade secret fulfils the requirements to be also protected as an intellectual property work), embezzlement, theft, extortion, acceptance of a product of crime, etc. Furthermore, violation of article 252 of the Greek Penal Code may also constitute passive bribery.

However, the issue as to whether violation of trade secrets entails other criminal offences as well, is something that must be examined and evaluated on a case per case basis.

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

Legal/legitimate obtainment of the secret. In general, it could be argued that violation of trade secrets refers to the illegal way of obtainment of such secrets. Such violation is possible either in cases of disclosure, or in cases of appropriation or use of trade secrets for purposes other than the agreed. Therefore, persons who did not obtain the secret in an unfair/illegal manner are not prosecuted. Fair/lawful means of obtainment of a secret may be an independent invention, reverse engineering, observation of a product which is publicly available, etc.

"Reverse engineering" is the procedure of determining the nature and the essence of the product or service, by examining/testing the final product/service. Reverse engineering does not constitute an illegal act, provided that the product, from which the procedure of reverse engineering started, was obtained legally and that such reverse engineering was not in any way forbidden.

Testimony before the Court. Trade secrets are not in principal protected against the witness's obligation to testify before a Court. More specifically, in Greece, the trade secrets of a witness are not protected. Article 209 of the Greek Code of Penal Procedure provides that *"if someone is legally called to testify as a witness on a case, he cannot refuse to do so, unless he falls within one of the exceptions expressly provided in this Code".* Article 212 of the same Code provides for some categories of professionals, who may not testify in the framework of criminal proceedings[5]. Said article, which determines exhaustively such professionals, does not include persons who are holders of trade secrets. In light of this, an employee of an enterprise for instance, does not have the right to refuse to testify in the framework of criminal proceedings regarding the trade secrets of such enterprise, despite the fact that art. 16 par. 1 of L. 146/1914 establishes his obligation for confidentiality. The same also applies for the owner of the enterprise, in case he is called to testify upon matters related to the trade secrets of his enterprise.

Circumstances excluding the criminality of the act. Article 20 of the Greek Penal Code sets the requirements for the lift of the illegal character of an act. On the basis of this article, the illegal character of the act of trade secrets violation is lifted in cases where the offender exercised a right or fulfilled an obligation imposed by the law.

Authorization. Finally, disclosure or use of trade secrets is not illegal and punishable if it does not take place without authorization, i.e. *without a legal right*. Such legal right may exist e.g. in cases where the owner of the trade secret has given his authorization, or where reasons of public order impose an obligation for disclosure of trade secrets.

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

[5] Art. 212 of Greek Code of Penal Procedure provides that: "1. Criminal proceedings shall be annuled if the following persons testify in pre-trial or trial proceedings: (a) clerics regarding the matters of which they took knowledge during a confession, (b) counsels, technical consultants and notaries, regarding the matters that have been confided to them by their clients; counsels and technical consultants shall evaluate, based on their conscience, whether and to what extent they must testify on other matters of which they took knowledge by occasion of their profession, (c) doctors, pharmacists and their assistances, as well as midwives, regarding anything that has been confided to them during their profession, unless other laws establish their obligation to announce such confided information to the Authorities, and (d) civil servants, regarding matters that constitute diplomatic or military secrets or secrets related to the security of the State, unless the competent Minister, either following an application of the Judicial Authority or of the parties of the case, or ex officio, provides his authorization.
2. The prohibition established in par. 1 sections (a), (b) and (c) continues to apply even if the persons to whom the prohibition refers, have been released – by the person who confided such confidential information to them - from their obligation to keep confidentiality. 3. All the above witnesses are obliged to declare under oath to the person who asks for their testimony, that, if they testified, they would violate the secrets mentioned in paragraph 1. [...]".

In general, the sole risk of dissemination or disclosure of trade secrets may not give rise to criminal liability. In such a case, the owner of the trade secret may apply before civil Courts and ask for interim measures, claiming that there is a case of emergency and/or that such interim measures are necessary in order to prevent an imminent danger, i.e. the disclosure and/or use of his trade secrets.

Especially with regards to criminal/penal law, it should be noted that the risk of dissemination or disclosure of trade secrets could result in criminal liability, only in the framework of the legal concept of "attempt". In such a case, reduced penalty would be imposed to the offender. However, in order for someone to be punished for "attempt of trade secrets violation", he should have committed an act which could be considered at least as "beginning of implementation" of trade secrets violation; acts of preparation of the crime (like, for instance, memorization of a secret) are, in principle, not prosecuted.

It should also be mentioned that article 18 par. 2 of L. 146/1914 provides specifically for criminal liability of anyone attempting to induce someone else to commit the act of articles 16 section (a) or 17.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

Violation of trade secrets could be categorized as follows:

I. Depending on the personal qualities of the infringer/offender:

- *Violation by employees.*

(a) Article 16 par. 1 of L. 146/1914. The offender in this provision may only be an employee, worker or trainee of a commercial or industrial establishment or enterprise. The term employee is interpreted broadly and includes any person who provides any kind of services, either on a part-time or a full-time basis, irrespectively of whether he receives payment (standard salary or a profit share) or not. In this broad sense, the cleaning personnel as well as the general manager of the enterprise are also considered as "employees". However, the members of the Board of Directors of the legal representatives of a company may not in principal be considered as "employees", unless they receive payment for their services, on the basis of an agreement with the company. It should also be noted that this provision applies only *during* the employment agreement of the "employee", "worker" or "trainee". (Following the termination of the employment agreement, application of this provision is not possible; in such a case, art. 16 par. 2 may apply, provided of course that all other requirements established in this paragraph are met).

(b) Article 370B par. 2 of the Greek Penal Code. The second paragraph of article 370B, according to which the offender is in the service of the holder of the data or computer programs, constitutes an aggravated circumstance of the basic crime of par. 1.

(c) Articles 13 par. 5 in combination with 17 par. 3 of the L. 1767/1988. The offender in this provision may only be a member of the Works Councils of an enterprise, i.e. an employee of the enterprise to which the trade secrets refer.

(d) Article 390 of the Greek Penal Code. The offender in this case may be any person (trustee, manager) who takes care of or has been entrusted with the management of one's property. The quality of the trustee or manager may derive from a legal act (e.g. a

mandate, a power of attorney, an employment agreement, etc), or by the law (e.g. the manager/representative of a legal entity, the managing director, the Board of Directors of a Societe Anonyme, the trustee in bankruptcy, etc).

- *Violation by third parties.*

(a) Articles 16 par. 2 of L. 146/1914.

(b) Art. 18 par. 2 of L. 146/1914,

(c) Article 370B par. 1 of the Greek Penal Code.

In all these provisions, any person, irrespectively of his quality, may be the offender.

- *Violation by third parties, connected to the enterprise – owner of the secrets.*

(a) Article 17 of L. 146/1914. In this case, the offender may be only a third party (and not an employee), related with the owner of the trade secrets in the course of business. The term "relation in the course of business" is also interpreted broadly, so as to include any contractual or non-contractual relation. It should be noted that persons having with the owner of the trade secrets a relation of other kind, such as friends, family, etc, are not subject to the application of this provision.

- *Violation by professionals.*

(a) Article 371 of the Greek Penal Code. In this provision, the offender may be any person to whom others confide their secrets because of the nature of his profession, as well as the assistants of such professionals.

(b) Article 63 C par. 2 of L. 2190/1920. In this case, the offender may only be an auditor, who performs audits in a societes anonymes.

- *Violation by civil servants.*

(a) Article 252 of the Greek Penal Code.

(b) Article 63 par. 1 section a, of L. 2190/1920.

In both of the above provisions, the offender may only be a civil servant.

II. Depending on the items covered by trade secrets:

- *Violation of trade secrets in general.*

Article 16 sections (a) and (b) of L. 146/1914, Articles 370B, 252, 371 and 390 of Greek Penal Code, Articles 13 and 17 of L. 1767/1988, and Articles 63 par. 1 section a and 63C par. 2 of L. 2190/1920 aim to the protection of trade secrets in general. However, the following should also be noted:

Article 370B of Greek Penal Code protects trade secrets in the form of data or computer programs, i.e. secrets saved in the memory of a computer (e.g. customer base). It is clear that in case of secret computer data or programs, the offender violates the provisions of L. 146/1914, as well as the article 370B of the Greek Penal Code. However in such a case, the provision of article 370B of the Greek Penal Code, being "lex specialis", will apply.

Article 252 of Greek Penal Code protects any kind of secrets of which the civil servant took knowledge strictly due to his service, which may also include trade secrets.

Article 371 of Greek Penal Code aims to the protection of secrets of individuals, which may also include trade secrets.

- *Violation of models and technical standards.*

Article 17 of L. 146/1914 protects only models and technical standards. "Models" are the objects that are used as such for the manufacturing of new things, and may be of a technical or non-technical nature. "Technical Standards" are the oral or written instructions upon a technical matter. The law makes an indicative reference to such technical standards: drawings, prototypes, patterns, samples or instructions.

III. Apart from art. 390 section (b) of Greek Penal Code, law treats all the above crimes as misdemeanors, while the crime of art. 390 section b of Greek Penal Code is a felony.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

Although in the framework of Trips Agreement, implemented with Greek Law no 2290/1995, "undisclosed information" falls within the concept of "intellectual property", under Greek Law, trade secrets, per se, are not classified as intellectual property rights.

Indeed, both trade secrets and intellectual property works are the result of one's intellectual work and it is possible that a trade secret is also protected under the provisions of Intellectual Property law. More specifically, both intellectual property works and trade secrets do not need to be "published" in order to be protected and, furthermore, the owner of the secret or the intellectual property work does not have to follow a formal/administrative registration procedure, in order to obtain a right upon the secret and/or the work (as opposed to patents or trademarks). However, there are significant differences between a trade secret and an intellectual property work. More specifically:

The important thing in a trade secret is the information that the trade secret contains, i.e. the content of the secret, and not the form by which the secret is expressed. On the contrary, what is important in an intellectual property work is the specific form by which this intangible asset (work) is expressed. A concept, as well as the form by which it is expressed with regards to a product or a service, even if not yet finalized, can constitute a trade secret, but cannot constitute an intellectual property work.

Furthermore, an intellectual property work requires more elements, which are not necessary in a trade secret: originality, which is essential for a work in order to be protected as an intellectual property work, is not necessary in trade secrets. More specifically, a trade secret needs to be original, only to the extent that justifies the fact that it is not known to others. In this framework, even a simple idea may constitute a

basis for the development of a result that can be treated as secret. On the other hand, an intellectual property work must be original, in order to be protected under intellectual property law. Although Greek law does not specifically define the term "originality", Greek jurisprudence and theory require that the specific work has the element of the "personal intellectual creation" and that the author's personality is reflected therein. An intellectual property work is original as a way of expression of the individual mind, when it is the result of the personal contribution and represents some individuality. Another criterion applied also by Greek Courts, is the criterion of "statistical uniqueness", according to which a work is original when, under the same circumstances, no other author would create the same work. Thus, the originality required for a work to constitute an intellectual property work, is far more extensive than the originality required for a trade secret, which is necessary only to the extent that justifies its secrecy, i.e. that it is not known to others.

In view of the above, it could be argued that, in case a trade secret meets all requirements of an intellectual property work, but cannot be protected as a trade secret (e.g. because it has become known to others), it may be protected under the provisions of intellectual property law, provided of course that it has been violated in one of the ways provided by that law.

With regards to the ways of violation, it should also be noted that violation of a trade secret does not necessarily constitute at the same time a violation of an intellectual property work. For instance, violation of an intellectual property work requires a reproduction of the material carrier containing the work, and not just the use or disclosure of information included therein. On the contrary, the sole unfair use or disclosure to a third party of the information included therein is enough to constitute violation of a trade secret.

Please also note that Article 66 of Greek Copyright Law (Law 2121/1993) which provides for penal sanctions available in copyright infringement cases has a rather broad scope, applying in cases of violation of any and all rights / powers deriving from protected "intellectual property" works. According to said provision, anyone, who - without having the right and in violation of the provisions of either Greek Copyright Law or provisions of multiparty international conventions on the protection of intellectual property ratified by law - records, reproduces, distributes, possesses with an intent to distribute, uses, presents to the public, publicly performs, broadcasts through radio or television by any means and generally exploits the work which is the subject matter of intellectual property or imports copies or infringes or violates the author's right to decide on the presentation of the work to the public and to present it without any alterations and/ or additions or cuts, is punished by imprisonment of at least one year and a fine (pecuniary penalty) ranging from 2.900 to 15.000 Euros. Therefore it becomes evident that, in principle, there are no conducts prohibited under intellectual property law which do not result in criminal offenses.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

Although Greek Law does not provide for a specific definition of "trade secrets", Greek legal theory and jurisprudence have developed the legal concept of trade secrets. According to the most generally acknowledged definition, as "trade secret" is considered any information that relates to a specific enterprise, which is known only to a specified number of persons bound by confidentiality, and which, according to the will of the owner of the enterprise having a reasonable economic interest, must remain secret.

According to the theory of "will", the most crucial element is the will of the owner for such fact to remain secret. On the other hand, according to the theory of "interest", the most crucial element is the existence of an economic interest for preserving confidentiality. The most prevailing (as correct) is the "combination" theory which requires both elements, i.e. the subjective element of the will of the owner as well as the objective element of the economic interest.

In general, as "trade secret" is considered any fact/information of any kind, which is connected to the operation of the enterprise in any level whatsoever (organization, production, etc), and the economic/commercial value of which depends on its confidentiality, which is necessary for the exploitation of such information by the enterprise in order to enhance its competitive lead.

The term "trade secret" is broad enough and includes any commercial secret, any confidential information, any industrial secret, and know-how (commercial know-how and industrial know-how).

Therefore, trade secrets may indicatively include instructions, models, lists of customers and/or suppliers, technological methods, marketing methods, methods for the production of new products, plans for the expansion of business in the future, codes, ways of book keeping, business methods, correspondence, quotations to customers, etc.

In view of the above, it is evident that there are no limitations as to the items covered by legal protection of trade secrets, as long as those items fulfil the above requirements.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

In general, a trade secret must meet the following requirements in order to be treated as such and enjoy legal protection:

(a) Secrecy. The secrecy of a fact/information ensures its economic/commercial value and the competitive lead of its owner in the market. As "secret" is considered anything which is not known to others, apart from a small number of persons connected to the owner of the secret and controlled by him. The owner of a secret must want to treat it as such and to keep its secrecy. In this respect, the owner of the secret evaluates the information as secret and takes reasonable measures in order to safeguard its secrecy. The will of the owner to treat an information as secret, may be expressed either expressly, or even indirectly (resulting from the circumstances of each case).

Any secret that is disclosed cannot be treated as secret anymore and may not enjoy legal protection.

(b) Result of work. A trade secret is the result of research and work of one or more persons, aiming to improve the position of an enterprise in the field of competition. Therefore, when it comes to information, for which no work has been performed and no capacity was needed, such information cannot be considered inaccessible for third parties, cannot attribute to its owner a lead in competition and thus, may not constitute a secret.

(c) The connection between the secret and the enterprise. Such connection is necessary in order for secret information to be considered as trade secrets. More specifically, not

any secret information constitutes a trade secret: it has to be part of the internal organizational value of the enterprise, the use of which attributes to the enterprise a competitive lead in the market.

(d) The economic interest of the enterprise. An enterprise may not unduly claim protection of secrets and demand the observance of confidentiality, when it does not serve its interests. Economic interest of the enterprise is deemed to exist when the secret information is important and has an impact on the competitive capacity of the enterprise, while its disclosure might lead to the damage of the enterprise or to the enhancement of competitors. It should of course be noted that the economic interest of the secret's owner should be legitimate, since illegal secrets do not justify the owner's legal interest and, thus, are not protected.

- As already pointed out, in order for a trade secret to enjoy legal protection, it has to be kept as a secret. On the contrary, in order for a patent to be protected as such, it has to be disclosed through the relevant official registration procedure. In cases where a trade secret fulfils the requirements provided for the grant of a patent (i.e. is patentable), it is up to its owner to decide whether he wants to proceed to its registration as a patent and enjoy the relevant legal protection, or he prefers to keep its secrecy and treat it as a trade secret. He may of course treat it as a secret for a specific period of time (until he finalizes its form, content, etc), and afterwards seek for its official registration as a patent. Therefore, the requirements for legal protection of trade secrets (secrecy) and patents (disclosure through the official registration procedure) are different and, therefore, the two systems of legal protection cannot apply at the same time. It is thus clear that the patentability of a trade secret does not impact on the extent of its protection by virtue of the above mentioned legal framework.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Greek Law 1733/1987 "Technology Transfer, Inventions and Technological Innovation", which refers to patents, does not provide for direct criminal protection of patents. However, art. 17 par. 7 of said Law provides that "anyone who places on products or on their wrapping, or on any kind of commercial documents destined for the public, or on other relevant means of publishing and advertising, a false statement that the objects in question are protected by a patent, shall be punished by imprisonment of maximum one year, and/or by a fine of at least 50.000 drachmas*".

Additional criminal protection on the basis of the provisions on forgery and fraud may also be possible.

(* 50.000 drachmas correspond to 146,74 Euros).

With regards to utility models, the same L. 1733/1987 applies and thus, utility models may be protected in a criminal basis in the same way as patents.

Industrial designs are regulated by L. 2417/1996 and by Presidential Decree 259/1997. Article 28 par. 2 of said Presidential Decree refers to article 17 par. 7 of L. 1733/1987 for possible criminal protection of industrial designs.

With regards to trademarks, Greek Law 2239/1994 provides specifically for their criminal protection. More specifically, article 28 of said law stipulates the following: "1. Imprisonment of at least three months and/or a fine of at least 200.000 drachmas* shall be imposed upon anyone who a) alters a trademark or knowingly uses an altered trademark, b) knowingly affixes to the undertaking's products or to articles of the undertaking's trade, a trademark of which he is not the owner, c) imitates a trademark, in whole or in part, without alteration, with the purpose of misleading purchasers, or knowingly uses such a trademark, d) knowingly sells or offers for sale or disseminates goods bearing a trademark that constitutes an alteration or imitation of another trademark, e) uses a trademark contrary to the provisions of article 19, f) uses as a trademark the emblems and symbols of the Greek State or of authority or religious symbols. 2. The provisions of paragraph 1 of this article shall also apply to service marks".
(**200.000 drachmas correspond to 586,95 Euros).*

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

Violation of trade secrets is in principal prosecuted further to the filing of a penal complaint on behalf of the holder of the right to file such a complaint (indeed, articles 16 – 18 of L. 146/1914 and articles 370B and 371 of the Greek Penal Code specifically provide that the acts described therein can be prosecuted further to the filing of a penal complaint). The person who is entitled to file the penal complaint is the person who is the holder of the legal value violated by the illegal act, in this case the owner of the trade secret. In case of death of the trade secret's owner, the right to file a penal complaint passes on to his heirs. If the owner of the trade secret is a legal entity, the person entitled to file the penal complaint on behalf of the legal entity is the person who legally represents such entity.

According to Greek Penal Code, the penal complaint must be filed within a specific deadline and, more specifically, within 3 months from the date on which the person entitled to do so took knowledge of the illegal (already committed) act, as well as of the person(s) who committed it, or of one of the accomplices.

On the other hand, with regards to the acts described in articles 252 and 390 of the Greek Penal Code and in articles 63 par. 1 section (a) and 63C of L. 2190/1920, it should be noted that they are prosecuted ex officio. Of course, even in these cases, the Public Prosecutor needs to be informed of the illegal act. In this framework, the right to report such illegal act lies with the injured party, or with anyone else who took knowledge of such act in any way whatsoever.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

In order to prove that an illegal act (in this case violation of trade secrets) has been committed, any type of evidence may be brought before Court. According to Greek Code of Penal Procedure, the main types of evidence are (indicatively) the following: indications, inspection of a place or a thing, the conduct of an expert's report, admission of guilt on behalf of the defendant, witnesses and documents. However, means of evidence which have been obtained illegally are not taken in consideration by the Court.

All means of evidence will be evaluated by the Court, in order to determine whether the illegal act has been committed or not.

In view of the above, there is not any specific evidence that the injured party will have to produce before the Court in order to prove abuse of his trade secrets.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

Application for such ex parte provisional Court orders is possible only in civil proceedings, through an application for interim measures, in cases of emergency and/or imminent danger. In the framework of such interim measures applications, the injured party may also request that the offender ceases violation of trade secrets and desists from such actions in the future.

In the framework of criminal proceedings, the injured party may file a penal complaint and ask from the police officers (acting as inquiry officers) to visit the residence/premises of the offender/defendant, in order to conduct any and all acts necessary for the certification of the illegal action (finding of evidence) and to track down the offender. In the framework of this procedure, the police officers can confiscate anything which proves the illegal action (documents, computer systems, etc). Given that, according to the Greek Code of Penal Procedure, inquiry actions normally require the prior written order of the district attorney, such "ex parte" raid is possible in cases where the obtainment of the district attorney's order will delay the proceedings and, as a result, crucial evidence could be lost, removed or altered, while the certification of the illegal action might either be cancelled, or become more difficult.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Greek law does not provide for criminal liability of legal entities. Criminal liability according to Greek law is only possible for natural persons. Therefore, criminal liability may apply only on the legal representatives of a legal entity.

2. If so, which type of liability arises for companies? Which penalties shall apply?
In Greek law, companies are subject only to civil liability, while criminal liability, as mentioned above, is only possible for natural persons.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

The civil (and not penal, as clarified above) Courts are competent to adjudicate civil liability of companies in cases of trade secret violations.

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

In general, in order for a trade secret violation to occur, the information/fact/document/etc (which constitutes the object of the crime), must be secret. A piece of information/document, etc, is considered to be secret and confidential, in cases where there is a confidentiality clause referring to it. Such confidentiality clause may be either expressly agreed or may derive from the circumstances. In cases where the information is not considered to be confidential (either because it has not been accompanied by an - express or implied by the circumstances – confidentiality clause, or because it is easily and freely accessible by everyone, or because its owner provided his authorization for its disclosure) the crime of trade secrets violation is not committed.

There is not any distinction, in this respect, between employees of the company owning the secret and any other persons other than employees. Therefore, in order for a trade secret violation to occur (either by employees or by any other person) it is important that the disclosed information – object of the crime - is actually a secret; and in order for the information to constitute a secret, it has to be accompanied by a confidentiality clause, which may be either expressly agreed, or implied by the circumstances.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

In cases or articles 16 section (b) and 18 of L. 146/1914 of Unfair Competition, the offender has to qualify as a competitor or potential competitor of the owner of the disclosed trade secrets. More specifically, said articles define that the offender must act "for purposes of competition". (As analyzed in our answer to Question A2 of Criminal Law Questionnaire, the "*purpose of competition*" reasonably entails that there is a relation of competition between the offender and the injured party and that the offender intends to compete the injured party.)

In case of article 16 section (a) of the same law, the offender must either qualify as a competitor of the owner of the disclosed trade secrets ("act for purposes of competition"), or act with the intention of damaging the proprietor of the establishment or the enterprise to which the disclosed secrets relate.

In cases of the other legal provisions of trade secrets violation mentioned in the Criminal Law Questionnaire (Art. 17 of L. 146/1914, Art. 370B of the Greek Penal Code, Art. 13 & 17 of L. 1767/1988, Articles 63 par. 1a and 63C par. 2 of L. 2190/1920, and Articles 252, 371 and 390 of the Greek Penal Code), the offender does not need to qualify as a competitor of the owner of the disclosed trade secrets, in order to be prosecuted on the basis of such provisions.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

According to article 63 of the Greek Code of Penal Procedure "*the civil claim for damages occurred by reason of the crime and for the restitution of moral damages, may be brought before the penal Court by the persons entitled to this according to the provisions of the civil code. […]".*

Article 65 of the same Code provides that: "*1. The penal Court may not deal with the civil claim in cases where it decides that the defendant must not be prosecuted or in cases where it dismisses the defendant for any reason whatsoever. 2. The Penal Court which deals with a civil claim, is obliged to decide upon it. As an exemption, in cases where the claimed amount is higher than 44 Euros, the Penal Court may remit the civil claim to the civil Courts, if it decides that further evidence is required. […]".*

Article 66 of the same Code provides that: "*1. The civil claim which has been filed before a civil Court may be brought before the penal Court, provided that the civil Court has not issued its first-grade decision. 2. If the plaintiff claiming damages exercises his abovementioned right, then he cannot continue the proceedings before the civil Courts, with the exception of the cases mentioned in article 65".*

In view of the above provisions, the aggrieved person may bring a claim for damages in the course of criminal proceedings. In such a case, the aggrieved person may not continue civil proceedings - if he has also filed his claim before civil Courts. However, it should be noted that it is rather uncommon for the aggrieved persons to bring their civil claim for damages before the penal Courts in the course of criminal proceedings, given that the penal Courts will most probably remit the civil claim to the civil Courts, on grounds of further required evidence. One more reason for the reluctance of the aggrieved parties to bring their civil claims (for damages) before the penal Courts, is that the penal Court may deal with the civil claim, only when it condemns the defendant.

What usually happens is the following: the aggrieved parties file their civil claim for restitution of moral damages (and not for compensation of property damage) before the penal Court, asking for a very small amount (usually 44 Euros), without prejudice to claim any other amounts before civil Courts further to the filing of a civil action (in practice, the filing of the action for damages before the civil Court usually takes place at the same time with the filing of the penal complaint). In these cases the penal Courts, if they decide to condemn the defendant, grant the civil claim (moral damages) of the aggrieved parties for the amount of 44 Euros, and the aggrieved parties seek payment of further amounts (compensation & the rest of moral damages, if any) through their civil action against the defendant before the competent civil Courts.

Hungary

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Hungarian legislation contains a general criminal provision relating to the infringement of trade secrets. Article 300 of the Hungarian Criminal Code protects trade, bank, securities, fund, insurance and occupational retirement and trade secrets.

Article 300 of the Criminal Code: *"(1) Any person who is under the obligation to keep confidential bank, securities, fund, insurance or occupational retirement secrets, and who makes available any bank, securities, fund, insurance or occupational retirement secret to an unauthorized person for financial gain or advantage or by causing pecuniary injury to others,further the person who illegally acquires, uses, or publishes a business secret for financial gain or advantage or by causing pecuniary injury to others is guilty of a felony punishable by imprisonment for up to three years."*

The new proposal of the Criminal Code[1] contains a separate provision relating to the violation of trade secrets but it primarily has the same wording as the currently applicable provision.

The Criminal Code does not contain a specific definition relating to trade secrets. The definition of trade secrets as provided for in Article 81 of the Civil Code (see Questionnaire A. point 2.1) is applicable to the definition of trade secrets used in the criminal law context.

The aim of the criminal protection is to protect the interest in the lawful and reliable functioning of competition and fair trading practices.

The following short description of relevant cases (with precedent value) relate to infringement of the trade secrets:

-BH 2002.176 - Employment relationship:
A company employee working in a T-shirt manufacturing factory unduly obtained and later used the description of a manufacturing method and stole the mold used for the screen painting of the T-shirts. The court assessed that the activity resulted in the crime of trade secret violation. Obtaining the mold alone does not qualify as a trade secret violation, since for that the actual breach of trade secret has to be established as well. In the present case several copies were made from the mold, which were used to produce counterfeit products, thus the court held that this actual use of the mold qualified the activity as trade secret violation.

-BH 2005.49 - The former licensee of the patent (the producer and distributor of the product) after the expiration of the patent and know-how license agreement used the technology learnt and continued to manufacture the product. The court assessed the infringement of business secret as in the license agreement the patentee has taken all the necessary steps to protect its invention by adopting appropriate provisions to protect its trade secret.

The following literature is connected to the infringement of trade secrets:

[1] The final proposal of the Criminal Code is not accepted yet.

- Béla Busch: The criminal protection of trade secret (In "In memoriam Pálinkás György", Rejtjel Kiadó, Budapest, 2007) (Busch Béla: Az üzleti titok büntetőjogi védelme. Pálinkás György emlékkönyv, Rejtjel Kiadó, Budapest, 2007)

- The Hungarian Criminal Law (edited by Ferenc Nagy, Hvg/orac kiadó, 2009.)
A Magyar Büntetőjog Különös Része (szerkesztette Nagy Ferenc, Hvg/orac Kiadó, 2009.)

In addition to the general provision on the violation of trade secrets, the Criminal Code also provides special provisions relating to criminal protection of IP rights. We will discuss this issue bellow at question 9.

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

We have to analyze the relevant part of Article 300 of the Criminal Code to answer this question: the relevant part of the provision provides that *"the person who illegally acquires, uses or publishes a business secret for financial gain or advantage or by causing pecuniary injury to others" has committed trade secret violation. .*

Pursuant to Hungarian law this offence may only be committed with intent.

There are two elements in the provision which influence the determination of the intention needed in order to establish this offence:
The first element is that the offence was committed *"for financial gain or advantage".* According to Hungarian criminal law this element requires specific intent (*dolus directus*) from the person committing the offence. However, in this case it is not a requirement that the offender acquires any financial gain as a result of committing the crime.

The second element of the offence that it was committed is *"by causing pecuniary injury to others".* Obviously, this element requires actual loss caused for classifying as an offence. Thus, according to Hungarian law this element of the offence can be committed with conditional intention (*dolus eventualis*) as well.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

The consequences of trade secret violation entail both criminal and civil liability. In the framework of a related criminal procedure a civil claim for damages which is based on an act giving rise to criminal proceedings can be decided by the same court as well. However, a civil lawsuit may be initiated separate from the criminal procedure.

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "fair use", "just cause", "de minimis threshold")?

Article 300 (2) of the Criminal Code contains the definition of "safe harbors" according to which a prosecutor can not be sanctioned for infringement of trade secrets. This "safe harbor" concept is connected to greater social goals which serve to justify the infringement of trade secrets.

Article 300 (2) of the Criminal Code:
"No punishment shall apply on the grounds of breach of trade secret against any person:

a) who fulfills the duties prescribed in a separate Act governing the publication of public information and information to be made available in the public interest; or
b) who fulfills the duties subject to the reporting obligation prescribed in the Act on the Prevention and Combating of Money Laundering and Terrorist Financing or who initiates such action, even if the report he filed in good faith has proved to be unfounded;
c) who fulfills the duties subject to the reporting obligation prescribed by law in connection with insider trading, market manipulation and the fight against terrorism, or who initiates such action, even if the report he filed in good faith has proved to be unfounded."

The regulations for "safe harbors" provided for in the Criminal Code are based on relevant European Union regulations. Pursuant to the regulations of the Criminal Code, the offender of a trade secret violation cannot be sanctioned if:

a. fulfills his obligations pursuant to the regulations of the act on disclosure of public information or information of public interest;

b. fulfills his reporting obligations pursuant to the regulations of the act on prevention of the use of the financial system for the purpose of money laundering and terrorist financing, or initiates such reporting, even in case the reporting made in good faith was unfounded; or

c. fulfills his reporting obligations pursuant to the regulations of the act on insider dealing, market manipulation or combating terrorism or initiates such reporting, even in case the reporting made in good faith was unfounded. (see more in detail below under point 6)

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

No, the sole risk of dissemination or disclosure of trade secrets does not give rise to criminal liability.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

The following types of behavior are punishable as a criminal offence: acquiring, using, publishing, communicating the business secret to others or making it available to an unauthorized person. The above mentioned behaviors do not preclude each other, as these activities can be carried out individually or simultaneously as well.

We can distinguish two groups of infringement of trade secrets. The first group contains the infringement of trade secrets which are sanctioned by Article 300 of the Criminal Code. The second group contains the infringement of trade secrets which are not sanctioned by Article 300 of the Criminal Code ("safe harbors", see also point 4).

In the first group, the Criminal Code does not specify the personal qualities of the infringer or the type of items covered by trade secrets. The offender or the conspirator of the crime can be anybody.

In the second group, the Criminal Code does specify the personal qualities of the infringer or the type of items covered by trade secrets. When we are considering the second group we must take into account the following three factors which are:

1. The subject of trade secret: public information.

Special personal qualification defined by Act CXII of 2011 on Information Autonomy and Freedom of Information:

- data processor: shall mean a natural or legal person or unincorporated organization that is engaged under contract in the processing of personal data on behalf of a controller of the data, including when contracting is ordered by virtue of law;
- data disseminator shall mean a body having public service functions, that shall publish data received from the data source on a website.

The above mentioned persons must publish any information that is of public interest even if it qualifies as trade secret.

2. The subject of trade secret: information of insider dealing or market manipulation.

Special personal qualification defined by Act CXX of 2001 on the Capital Market:
-the persons engaged in investment services, activities auxiliary to investment services, and commodity exchange services (Article 205).

If the above mentioned persons notice any information, fact or circumstance that may suggest insider dealing or market manipulation then that person must disclose the information to the authority even if that information is defined as trade secret.

3. The subject of trade secret: information of personal data or transaction

Special personal qualification defined by Act CXXXVI of 2007 on the Prevention and Combating of Money Laundering and Terrorist Financing:

a) the provision of financial services or in activities auxiliary to financial services;
b) the provision of investment services, in activities auxiliary to investment services or in providing investment fund management services;
c) the provision of insurance services, insurance agency or occupational retirement provision;
d) the provision of commodity exchange services;
e) the service of accepting and delivering international postal money orders;
f) the provision of real estate agency or brokering and any related services;
g) the provision of auditing services;
h) the provision of accountancy (bookkeeping), tax consulting services whether or not certified, or tax advisory activities under agency or service contract;
i) the operation of a casino, electronic casino or card room, or card game within the framework of distance gambling;
j) the trading in precious metals or articles made of precious metals;
k) the trading in goods, involving a cash payment in the amount of three million six hundred thousand forints or more;
l) the provision of voluntary mutual insurance fund services;
m) the provision of legal counsel or notary services (Article 1).

If the above mentioned persons notice any information, fact or circumstance that may suggest money laundering or terrorist financing then that person must disclose the information to the authority even if that information is defined as trade secret.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

The criminal law provisions meet the requirements provided by intellectual property law.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

There is no limitation relating to items as described in the question. Anything included in the definition of trade secrets under the Civil Code is under criminal protection.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

As mentioned in our answer to question 1 above, criminal law does not provide a definition of trade secret but relies on the definition as prescribed by Art. 81 (2) of the Civil Code. Consequently no additional specific requirements are needed to obtain the relevant legal protection beyond those prescribed by Article 81 of Civil Code (see also A 2.1. answer). If the item is patentable but not registered as patent, then general rules on trade secrets apply.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

In addition to the general protection of trade secrets the Criminal Code provides special protection relating to registered IP rights.

The following criminal acts may be distinguished as follows:

i. Plagiarism

Article 329 of Criminal Code:
"(1) Any person who:
a) connotes as his own the intellectual product of another person and thereby causes financial injury to the right-holder of record;
b) misusing his position, office or membership at an economic operator makes the utilization of an intellectual product of another person, or the enforcement of rights associated therewith, conditional upon being given a share from the fee received for, or from the profits or proceeds generated by such product;
is guilty of a felony punishable by imprisonment for up to three years."

(2) For the purposes of this Article 'intellectual works' shall mean literary, scientific and artistic works, inventions, plant varieties, product designs, industrial designs, topographies of microelectronic semiconductors, and other innovations.

ii. Violation of Industrial Design Rights

Article 329/D of Criminal Code:
"(1) A person who violates the right of the holder of a patent, plant variety, certification of supplementary protection, trademark, geographical indication, design rights, utility models or topographies conferred on the basis of an act, promulgated international convention or Community legislation by imitating or copying the subject matter of protection, and thereby causing financial injury, is guilty of a misdemeanor punishable by imprisonment of up to two years.
(2) The punishment for a felony shall be imprisonment for up to three years if the violation of industrial design rights:
a) results in substantial financial injury;
b) is committed in a pattern of business operation.
(3) The punishment shall be:
a) imprisonment of up to five years if the violation of industrial design rights results in particularly considerable financial injury;
b) imprisonment between two to eight years if the violation of industrial design rights results in particularly substantial financial injury."
iii. False Marking of Goods

Article 296 of Criminal Code:
"(1) Any person who produces a product with distinctive appearance, packaging, labeling or name, from which a competitor or his product having distinctive features can be recognized, and who does so without the consent of such competitor, or who acquires such product for the purpose of placing it on the market, is guilty of a felony punishable by imprisonment for up to three years.
(2) The punishment shall be imprisonment between one to five years if the criminal offense is committed in respect of products of substantial quantity or value."

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

The offender may be prosecuted either at the sole initiative of the Public Prosecutor or the initiative of holder as injured party. If the procedure is initiated by the Public Prosecutor there is no need for any statement from the holder as a injured party.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?
There is no special evidentiary requirement relating to the burden of proof in a criminal procedure; however, all the elements of the criminal act must be substantiated.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

The prosecutor and the police are in charge of the investigative procedure. Thus, they carry out the necessary investigation. However, the holder of the trade secret as an injured party has a right to propose such investigative action but it is at the discretion of the authority to decide if it intends to initiate an investigative action or not.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Under Hungarian laws, only private individuals may be held criminally liable. However, a company may also be liable for violation of the criminal law under certain circumstances. Pursuant to the Act CIV of 2001 on Criminal Sanctions against legal persons, various sanctions can be applied against a legal person if the following conditions are met: a crime has been committed (i) intentionally; (ii) for the purpose of achieving a material advantage for the benefit of the legal person or the crime has resulted in such a benefit; and (iii) by the chief executive, duly authorized representative of the legal person, an employee, executive, procurist a member of the supervisory board or a person authorized by them within the scope of activity of the legal person or the crime has been committed by a member or employee within the scope of activity of the legal person if the person entitled to supervise such persons could have prevented such an act.

Further, sanctions can also be applied against a legal person if the crime results in a benefit for the legal person and the chief executive, the duly authorized representative of the legal person, the employee, the executive, procurist or a member of the supervisory board are aware that a crime has been committed.

2. If so, which type of liability arises for companies? Which penalties shall apply?

Criminal sanctions applicable to legal persons are as follows:

(i) the termination of the legal person's activity;
(ii) the restriction of the scope of the legal person's activity; and
(iii) a fine (ranging from HUF 500,000 (approximately EUR 2,000) to three times the material advantage / benefit which was intended to be gained or was actually gained by committing the crime).

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

The same court is entitled to make decisions relating to criminal liability of a legal person as criminal liability of a private individual.

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

No specific obligation for protection of information is necessary for a trade secret violation to occur.

From a criminal law point of view there is no difference regarding whose information should be kept secret.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

No, the offender shall not need to qualify as a competitor of the owner of the disclosed trade secret.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

Yes. According to Articles 54 and 335 of the Criminal Procedure Code (Act XIX. of 1998), the aggrieved person may assert civil law claims in criminal procedure.
The ongoing civil lawsuit for compensation will neither be dismissed nor stayed as a consequence of asserting civil law claim in criminal procedure, however they might influence each other with respect to the actual amount to be recovered as a consequence of the trade secret violation.
If the criminal procedure ends without establishing the offence, it is obviously not possible for, the aggrieved person to assert any civil law claims during the criminal procedure. However, due to the different legal base in a civil law procedure the aggrieved person may still recover damages if the trade secret violation can be established according to civil law rules.

Ireland

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

There is no criminal liability for trade secrets violation in Ireland[1].

Ancillary offences exist which may arise in the case of violating trade secrets depending on the circumstances of the violation and these are discussed below. If documents or other items are taken in the process of violating trade secrets it may amount to theft – although trade secrets are not considered to be property[2] and so if no physical materials are taken this offence does not apply.

Criminal offences exist for certain infringements of intellectual property rights, which may arise in the case of trade secrets violations depending on the nature of the trade secrets (discuseed at Question 11). Criminal sanctions in the form of committal proceedings may also be imposed in the event that a person breaches a Court Order where they have obtained civil remedies for trade secrets violation, such as injunctions (discussed in the Commercial and IP Law Questionnaire) or pursuant to a criminal investigation.

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

Not applicable.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

As discussed at Question 1, the violation of trade secrets may entail a number of ancillary criminal offences, depending on the way in which the violation is effected or if the violation is in breach of a Court Order affecting the trade secrets.

The following are the most likely criminal offences to arise in the case of trade secrets violations in Ireland.

(i). Disclosure of personal data obtained without authority

Section 22 of the Data Protection Acts 1988 and 2003, as amended, states:

(1) A person who:

[1] An offence exists under Section 55(5) of the Air-Raid Precautions Act 1939 but is of little practical significance. Section 5(5) states:
"(5) If any person who in compliance with the provisions of this section or of a warrant issued thereunder is admitted into a factory, workshop or workplace discloses to any person any information obtained by him in the factory, workshop or workplace with regard to any manufacturing process or trade secret, he shall, unless such disclosure was made in the performance of his duty, be guilty of an offence under this section and shall be liable on summary conviction thereof to a fine not exceeding five hundred pounds or at the discretion of the court to imprisonment for a term not exceeding twelve months".

[2] Oxford v Moss (1979) 68 Cr App Rep 183

(a) obtains access to personal data, or obtains any information constituting such data, without the prior authority of the data controller or data processor by whom the data are kept, and

(b) discloses the data or information to another person,

shall be guilty of an offence.

(ii). Unauthorised accessing of data

Section 5 of the Criminal Damage Act 1991 states:

(1) A person who without lawful excuse operates a computer

(a) within the State with intent to access any data kept either within or outside the State, or
(b) outside the State with intent to access any data kept within the State,

shall, whether or not he accesses any data, be guilty of an offence and shall be liable on summary conviction to a *fine not exceeding £500 or imprisonment for* a *term not exceeding* 3 *months or both.*

(2) Subsection (1) applies whether or not the person intended to access any particular data or any particular category of data or data kept by any particular person.

(iii). Unlawful use of a computer

Section 9 of the Criminal Law (Theft and Fraud Offences) Act 2001 states:

(1) A person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another, is guilty of an offence.

(2) A person guilty of an offence under this section is liable on conviction on indictment to a fine or imprisonment for a term not exceeding 10 years or both".

(iv). Theft

Section 4 Criminal Justice (Theft and Fraud Offences) Act 2001 states:

(1) Subject to section 5, a person is guilty of theft if he or she dishonestly appropriates property without the consent of its owner and with the intention of depriving its owner of it.

(5) In this section—

''appropriates'', in relation to property, means usurps or adversely interferes with the proprietary rights of the owner of the property;

''depriving'' means temporarily or permanently depriving.

(v). Criminal infringement of intellectual property rights

Please see response to Question 11.

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may

not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

Not applicable.

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

Not applicable.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

Not applicable.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

Criminal law does not deal with the notion of trade secrets.

Trade secrets are generally treated under the law of confidence, as opposed to intellectual property law. As indicated above, there is no direct criminal liability for a breach of confidence (such as, for example, dissemination of confidential business information).

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

Not applicable, as trade secrets do not directly benefit from the protection of criminal law.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

Not applicable, as trade secrets do not directly benefit from the protection of criminal law.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Criminal Protection exists for copyright, trade mark and design rights. There is currently no criminal protection for patents in Ireland.

Section 140 of the Copyright and Related Rights Act 2000 makes it a criminal offence to infringe copyright:

(1) A person who, without the consent of the copyright owner—
(a) makes for sale, rental or loan,
(b) sells, rents or lends, or offers or exposes for sale, rental or loan,
(c) imports into the State, otherwise than for his or her private and domestic use,
(d) in the course of a business, trade or profession, has in his or her possession, custody or control, or makes available to the public, or

(e) otherwise than in the course of a business, trade or profession, makes available to the public to such an extent as to prejudice the interests of the owner of the copyright, a copy of a work which is, and which he or she knows or has reason to believe is, an infringing copy of the work, shall be guilty of an offence.
(2) In this section ''loan'' means a loan for reward and in particular does not include a loan to a family member or friend for private and domestic use, and ''lends'' shall be construed accordingly.
(3) A person who—
(a) makes,
(b) sells, rents or lends, or offers or exposes for sale, rental or loan,
(c) imports into the State, or
(d) has in his or her possession, custody or control, an article specifically designed or adapted for making copies of a work, knowing or having reason to believe that it has been or is to be used to make infringing copies, shall be guilty of an offence.

(4) A person who—
(a) (i) makes,
(ii) sells, rents or lends, or offers or exposes for sale, rental or loan,
(iii) imports into the State, or
(iv) has in his or her possession, custody or control, a protection-defeating device, knowing or having reason to believe that it has been or is to be used to circumvent rights protection measures, or
(b) provides information, or offers or performs any service, intended to enable or assist a person to circumvent rights protection measures, shall be guilty of an offence.
(5) Where copyright is infringed by—
(a) the public performance of a literary, dramatic or musical work,
(b) the playing or showing in public of a sound recording, artistic work, original database or film, or
(c) broadcasting a work or including a work in a cable programme
service, the person who caused the work to be so performed, played, broadcast, included in a cable programme service or shown shall be guilty of an offence where he or she knew or had reason to believe that the copyright in the work would be infringed.
(6) An offence shall not be committed under subsection (1) or (5) by the undertaking of an act which under this Part may be undertaken without infringing the copyright in a work.
(7) A person guilty of an offence under subsection (1), (3) or (4) shall be liable—
(a) on summary conviction, to a fine not exceeding £1,500 in respect of each infringing copy, article or device, or to imprisonment for a term not exceeding 12 months, or both, or
(b) on conviction on indictment, to a fine not exceeding £100,000, or to imprisonment for a term not exceeding 5 years, or both.
(8) A person guilty of an offence under subsection (5) shall be liable—
(a) on summary conviction, to a fine not exceeding £1,500 in respect of such offence or to imprisonment for a term not exceeding 12 months, or both, or
(b) on conviction on indictment, to a fine not exceeding £100,000, or to imprisonment for a term not exceeding 5 years, or both.

Section 92 of the Trade Mark Act 1996 makes it a criminal offence to infringe a trade mark registration.

(1) Subject to the provisions of subsection (3), it shall be an offence for any person—
(a) to apply a mark identical to or nearly resembling a registered trade mark to goods or to material used or intended to be used for labelling, packaging or advertising goods,
(b) to sell, let for hire, offer or expose for sale or hire or distribute—
(i) goods bearing such a mark, or

(ii) material bearing such a mark which is used or intended to be used for labelling, packaging or advertising goods,
(c) to use material bearing such a mark in the course of a business for labelling, packaging or advertising goods, or
(d) to possess in the course of a business goods or material bearing such a mark with a view to doing any of the things mentioned in paragraph (a) to (c),
when that person is not entitled to use the mark in relation to the goods in question or authorised by a person who is so entitled.

(2) Subject to the provisions of subsection (3), it shall be an offence for any person to possess in the course of a business goods or material bearing a mark identical to or nearly resembling a registered trade mark with a view to enabling or assisting another person to do any of the things mentioned in subsection (1) (a), (b) or (c), knowing or having reason to believe that the other person is not entitled to use the mark in relation to the goods in question or authorised by a person who is so entitled.
(3) Any person who contravenes the provisions of subsection (1) or (2) shall be guilty of an offence if, but only if that person acts with a view to gain, for himself or another, or with intent to cause a loss to another and it shall be a defence for a person charged with an offence under subsection (1) to show that he believed, on reasonable grounds, that he was entitled to use the trade mark in relation to the goods in question.
(4) A person who commits an offence under this section shall be liable—
(a) on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding £1,000, or to both;
(b) on conviction on indictment to imprisonment for a term not exceeding five years or to a fine not exceeding £100,000, or to both.

Section 66 of the Industrial Design Act 2001 makes it a criminal offence to infringe an industrial design.

(1) A person who without the licence of the registered proprietor
of a design and while the design right is in force—
(a) uses, otherwise than for his or her private and domestic use,
(b) makes for sale or rent,
(c) sells or rents, or offers or exposes for sale or rent,
(d) imports into the State, otherwise than for his or her private and domestic use,
(e) exports, or
(f) in the course of a business, trade or profession, has in his or her possession, custody or control, a product which is, and which he or she knows or has reason to believe is, an infringing product, shall be guilty of an offence.

(2) A person who—
(a) makes,
(b) sells or rents, or offers or exposes for sale or rent,
(c) imports into the State, or
(d) has in his or her possession, custody or control, an article specifically designed or adapted for applying to or incorporating in a product a design, knowing or having reason to believe that it has been or is to be used to make infringing products, shall be guilty of an offence.
(3) An offence shall not be committed under subsection (1) by the undertaking of an act which under this Act may be undertaken without infringing the design right.
(4) A person guilty of an offence under this section shall be liable—
(a) on summary conviction, to a fine not exceeding €1,905 (£1,500) in respect of each infringing product or article, or to imprisonment for a term not exceeding 12 months, or both, or
(b) on conviction on indictment, to a fine not exceeding €127,000 (£100,000), or to imprisonment for a term not exceeding 5 years, or both.

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

Not applicable.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

Not applicable.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [In criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

Violation of trade secrets does not attract criminal liability and cannot of itself give rise to criminal proceedings.

However, if criminal proceedings arose in respect of ancillary offences, ex parte orders can be applied for by An Garda Síochána (the Irish Police). An Garda Síochána may obtain search warrants in respect of offences under the Criminal Law (Theft and Fraud Offences) Act 2001 and Criminal Damage Act 1991 and seizure orders in respect of offences under Criminal Law (Theft and Fraud Offences) Act 2001.

The Data Protection Acts 1988 and 2003 provide that a court may order the forfieture (or destruction or erasure) of any data material connected with the commission of an offence under that Act.

Section 13 of the The Criminal Damage Act 1991 states:

(1) If a judge of the District Court is satisfied by information on oath of a member of the Garda Síochána that there is reasonable cause to believe that any person has in his custody or under his control or on his premises any thing and that it has been used, or is intended for use, without lawful excuse-
(a) to damage property belonging to another,
(b) to damage any property in a way likely to endanger the life of another or with intent to defraud, or
(c) to access, or with intent to access, data, the judge may issue a search warrant mentioned in subsection (2).
(2) A search warrant issued under this section shall be expressed and operate to authorise a named member of the Garda Síochána, accompanied by such other members of the Garda Síochána as may be necessary, at any time or times within one month of the date of issue of the warrant, to enter if need be by force the premises named in the warrant, to search the premises and any persons found therein, to seize and detain anything which he believes to have been used or to be intended for use as aforesaid and, if the property concerned is data or the search warrant has been issued on a ground referred to in subsection (1) (c), to operate, or cause to be operated by a person

accompanying him for that purpose, any equipment in the premises for processing data, inspect any data found there and extract information therefrom, whether by the operation of such equipment or otherwise.
(3) The Police (Property) Act, 1897, shall apply to property which has come into the possession of the Garda Síochána under this section as it applies to property which has come into the possession of the Garda Síochána in the circumstances mentioned in that Act.
(4) A person who-
(a) obstructs or impedes a member of the Garda Síochána acting under the authority of a search warrant issued under this section, or
(b) is found on or at the premises specified in the warrant by a member of the Garda Síochána acting as aforesaid and who fails or refuses to give the member his name and address when required by the member to do so or gives him a name or address that is false or misleading, shall be guilty of an offence and shall be liable on summary conviction- (i) in the case of an offence under paragraph (a), to a fine not exceeding £1,000 or imprisonment not exceeding 12 months or both, and (ii) in the case of an offence under paragraph (b), to a fine not exceeding £500".

Section 48 of the Criminal Justice (Theft and Fraud Offences) Act 2001 states:

(1) This section applies to an offence under any provision of this Act for which a person of full age and capacity and not previously convicted may be punished by imprisonment for a term of five years or by a more severe penalty and to an attempt to commit any such offence.
(2) A judge of the District Court, on hearing evidence on oath given by a member of the Garda Siocnene, may, if he or she is satisfied that there are reasonable grounds for suspecting that evidence of, or relating to the commission of, an offence to which this section applies is to be found in any place, issue a warrant for the search of that place and any persons found there.
(3) A warrant under this section shall be expressed and shall operate to authorise a named member of the Garda Siocnene, alone or accompanied by such other persons as may be necessary-
(a) to enter, within 7 days from the date of issuing of the warrant (if necessary by the use
of reasonable force), the place named in the warrant,
(b) to search it and any persons found there,
(c) to examine, seize and retain any thing found there, or in the possession of a person present there at the time of the search, which the member reasonably believes to be evidence of or relating to the commission of an offence to which this section applies, and
(d) to take any other steps which may appear to the member to be necessary for preserving any such thing and preventing interference with it.
(4) The authority conferred by subsection (3)(c) to seize and retain any thing includes, in the case of a document or record, authority-
(a) to make and retain a copy of the document or record, and
(b) where necessary, to seize and, for as long as necessary, retain any computer or other storage medium in which any record is kept.
(5) A member of the Garda Siochene acting under the authority of a warrant under this section may-
(a) operate any computer at the place which is being searched or cause any such computer to be operated by a person accompanying the member for that purpose, and
(b) require any person at that place who appears to the member to have lawful access to the information in any such computer- (i) to give to the member any password necessary to operate it, (ii) otherwise to enable the member to examine the information accessible by the computer in a form in which the information is visible and legible, or
(iii) to produce the information in a form in which it can be removed and in which it is, or can be made, visible and legible.

(6) Where a member of the Garda Siocnene has entered premises in the execution of a warrant issued under this section, he may seize and retain any material, other than items subject to legal privilege, which is likely to be of substantial value (whether by itself or together with other material) to the investigation for the purpose of which the warrant was issued.
(7) The power to issue a warrant under this section is in addition to and not in substitution for any other power to issue a warrant for the search of any place or person.
(8) In this section, unless the context otherwise requires- "commission", in relation to an offence, includes an attempt to commit the offence; "computer at the place which is being
searched" includes any other computer, whether at that place or at any other place, which is lawfully accessible by means of that computer,' "place" includes a dwelling; "thing" includes an instrument (within the meaning of Part 4), a copy of such instrument, a document or a record".

Section 31 of the Data Protection Acts 1988 and 2003 states:

(1) A person guilty of an offence under this Act shall be liable—
(a) on summary conviction, to a fine not exceeding €3,000, or
(b) on conviction on indictment, to a fine not exceeding €100,000.
(2) Where a person is convicted of an offence under this Act, the court may order any data material which appears to the court to be connected with the commission of the offence to be forfeited or destroyed and any relevant data to be erased.

Remedies available to holders in civil actions are discussed in the Commercial and IP Law Questionnaire.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Not applicable.

2. If so, which type of liability arises for companies? Which penalties shall apply?

Not applicable.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

Not applicable.

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

Not applicable. There is no criminal liability for trade secrets violation in Ireland.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

Not applicable. There is no criminal liability for trade secrets violation in Ireland.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

Not applicable. There is no criminal liability for trade secrets violation in Ireland.

Italy

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Under Section 623 of Italian Criminal Code whoever, having known by reason of his *status*, function, job or art, any information that is intended to remain secret concerning scientific discoveries or inventions, or industrial applications, discloses it to others or makes use thereof for its own or others' profit, shall be imprisoned up to two years.

The legal value protected by such provision lies with the companies' right to exploit the investments and the business information internally developed for gaining a competitive edge on the relevant market.

Notwithstanding the violation of trade secrets may most likely be committed by company's employees, most of scholars and case law consider that also persons other than employees, such as the company's agents, consultants, contractors, may be charged with the offence provided for under Section 623.

For more details, please refer to the following literature:

- Giampiero Azzali, *"Prove penali e segreti",* Giuffrè, Milano, 1967.
- Giovanni Cocco, *"La tutela penale delle creazioni intellettuali",* in Astolfo Di Amato (eds.), "*Trattato di diritto penale dell'impresa – Il diritto penale industriale*", pp. 260-307, CEDAM, Padova 1993.
- Benedetta Franchini Stufler, "*Studi sull'evoluzione economica e giuridica del know-how e della sua tutela*", Rivista di diritto industriale, No. 6, 2005.
- Nicola Mazzacuva, "*La tutela penale del segreto industriale*", Giuffrè, Milano 1979.
- Alberto Crespi, "*La tutela penale del segreto"*, Priulla, Palermo 1952.
- Alberto Alessandri, "*Riflessi penalistici sull'innovazione tecnologica",* Giuffrè, Milano 1984.
- Sergio Kostoris, *"Il segreto come oggetto della tutela penale",* CEDAM, Padova 1964.

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

Section 623 forbids two different conducts: disclosure and use of secret information.
As to the first type of conduct, it is expressly specified that secret information has to be used for the offender's own profit or for the profit of third parties for the offence to be committed. According to some scholars, the profit that the offender must obtain has to be construed as a competitive advantage detrimental to the interest of the holder of the secret information. However, certain authors (*See* Alessandri, *supra note*) and the recent case law consider any types of advantage (including moral advantage) as sufficient to give rise to a violation of trade secrets (*See* Supreme Court of Cassation, ruling No. 39656 of 8 October 2010).

With respect to the second type of conduct, Section 623 does not require the offender to obtain profit as a result of disclosure of confidential information. In fact, when the information to be kept secret is disclosed to third parties, anyone who receives that information may be able to use it as he prefers. In that case, the sole disclosure is *per se* detrimental to the holder, since the information that he intended to keep secret becomes of public domain, having no regard the type of use the information is subject to.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

Depending upon certain circumstances, the conduct under Section 623 may also result in the offence of misappropriation or embezzlement provided for by Section 646 of Criminal Code. According to this provision, however, only money or tangible personal property may be subject to misappropriation or embezzlement. Therefore, since information is an immaterial good, a concurrence of offences involving violation of trade secrets and misappropriation may comes about only in case the information to be kept secret is incorporated into tangible personal property (*See* Supreme Court of Cassation, ruling No. 20647 of 11 May 2010).

It has to be noted that a revelation of trade secrets under Section 623 does not necessarily result in unfair competition. An act of unfair competition may occur only in case the offence is committed by a competitor of the holder of the secrets.

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

Criminal provisions often establish certain conditions that offences have to meet in order to be punished. Unlike other provisions, Section 623 does not provide for any safe harbor clause, as no exemption applies to the offender. As opposed to other offences, the violation of trade secrets does not require that the holder of the secret information suffers any harm as a consequence thereof (according to some scholars, there is a legal presumption that the mere disclosure of use of a confidential information is detrimental to the holder and harms the legal values protected under the relevant provisions).
Also, the lack of a "just cause" does not constitute a requirement for the offence to be prosecuted.

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

The sole risk of a violation of trade secrets does not entail any consequence from a criminal point of view.

According to most of scholars (*See* Mazzacuva, *supra*), even the mere attempt to reveal confidential business information may give rise to the offence provided for under Section 623 of Criminal Code.
Generally speaking, in fact, the conduct constituting the said offence consists of a range of actions aimed at revealing secret information to unauthorized third parties, including, without limitation, (i) misappropriation of samples of materials, (ii) description of the innovative technical solution, (iii) unauthorized copying of documents, provided that it is intended to the revelation thereof (*See* Cocco, *supra,* p. 304).
It is indeed debated whether the misappropriation or the illegal acquisition of documents containing confidential information amounts to an attempt to reveal trade secrets under Section 623. Section 621, in fact, prohibits the revelation of the content of secret documents. This provision, in particular, assumes that the offender has illegally acquired such documents prior to disclosing their content but does not establish any specific

prohibition in this respect. Therefore, according to an author (*See* Mazzacuva, *supra*, p. 128), since Section 621 generally applies to any secret information embodied in documents (including trade secrets), the acquisition of documents containing business confidential information may not constitute an attempt to revelation of trade secrets pursuant to Section 623.
On the contrary, another author (*See* Cocco, *supra*) has pointed out that the provision under Section 621 refers to information illegally acquired by the offender, whereas Section 623 assumes that the offender normally handles information that he is obliged to keep secret; in addition, the offence under Section 623 is more specific than that prohibited under Section 621 and, thus, the latter shall not apply. On these grounds, it has been concluded that the acquisition or the misappropriation of documents containing business confidential information may amount to an attempt to revelation of trade secrets, provided that the offender is actually intended to disclose or use that information accordingly.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

Apart from Section 623 of Criminal code, other provisions establish criminal penalties for any person who discloses certain secret information that he/she has known in the course of his/her job.

According to Section 326, whoever, in his capacity as public official or civil servant, discloses any information in connection to his quality that is intended to be kept secret or uses such information may be charged with violation of a secret pertaining to his quality.
Among the others, the information that the public official/civil servant is obliged not to disclose may amount to a trade secret. In such a case, Section 326 shall apply, as it is more specific and provides for a more serious penalty than Section 623, and thus prevails over it in accordance with the general principles of Italian criminal law.

Also, Section 325 punishes whoever, in his capacity as public official or civil servant, uses, for his own or third parties' profit, any scientific discoveries or inventions or industrial applications pertaining to his quality that are intended to be kept secret. It becomes clear that the scope of Section 326 does not include the use of trade secrets by a public official/civil servant.

When it comes to the handling of trade secrets by a public official/civil servant, therefore, conducts such as the use and the disclosure of secrets pertaining to the quality of the wrongdoer fall within Section 326. Under certain circumstance, the secret may also shape as a trade secret; in such a case, any conducts consisting in the disclosure or the use thereof will be punished in accordance to Section 326. These cases may be kept separate from those where a trade secret is held by a public official/civil servant. In the latter, the trade secret does not pertain to the quality of the wrongdoer and any disclosure or use fall within the specific scope of Section 325.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

Section 98, Paragraph 1, of Industrial Property Code defines secret information as any information that
-is *secret*, in the sense that it is not generally well-known or easily accessible for experts and operators;
-has an *economic value* in so far it is kept secret;

-is subject to *measures* which are reasonably proper to keep it *confidential*.

In addition to that, Paragraph 2 specifies that secret information includes any data relating to tests or other confidential data whose elaboration entails a significant effort, and the submission of which is required for the placement on the market of certain types of products.

With respect to the scope of Section 623 of Criminal Code, it is a common opinion amongst scholars that trade secrets include any business information that the holder has an interest protected by law to exploit in order to gain a competitive advantage.

The extent to which business information constitutes trade secrets does not depend on the will of the holder thereof, but has to be determined in accordance with an actual interest to keep secret the information internally developed by the holder that may allow him to gain a competitive advantage. The will of the holder of the information to keep it secret, therefore, does not suffice to provide it with the relevant legal protection; rather, Italian Criminal law requires an objective interest.

It is a controversial issue whether scientific discoveries and inventions and industrial applications to which the confidential information refers have to meet certain criteria such as originality, novelty (*See contra* Supreme Court of Cassation, ruling No. 25008 of 18 May 2001) and suitability for industrial use.

As to originality, the discovery, invention or application is supposed to present certain features which entail a progress in the relevant field if compared with the previous state of the art. It has to be pointed out that not all the authors believe that originality is necessary, since the commitment to keep the information secret may depend on the interest of the holder to gain an advantage by the exclusive exploitation of a discovery, invention or application, regardless of the originality thereof.

With respect to novelty, this requirement is commonly understood to refer to the lack of a prior public dissemination. The main issue in connection to the requirement of novelty concerns the threshold above which certain information may be considered to be of public domain within the community of experts in the relevant field.

Please see point 10 for details about suitability for industrial use of scientific discoveries and inventions.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

With respect to secrets regarding inventions, scholars have specified that the use or the disclosure of information relating to some elements or components (including researches), even if they do not suffice for the completion of an invention, may result in a violation of Section 623 of Criminal Code (*See* Supreme Court of Cassation, ruling No. 25174 of 7 June 2005).
The first stages of research are excluded from the scope of protection. All the inventions in contrast to law, public order and public morality may not be protected as secrets pursuant to Section 623.

According to some scholars (*See* G. Cocco, *supra*), *know-how*, meant as technical rules governing industrial processes and activities, does not fall within the scope of protection of Section 623, as it does not *per se* pertain to an innovative content. However, the recent case law has ruled the opposite (*See* Supreme Court of Cassation, ruling No. 25008 of 18 May 2001).

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

With respect to the requirements that the information has to meet in order to qualify as trade secret, please refer to Paragraph A.8.
Once an invention is patented, any related information becomes of public domain. Normally, the holder of trade secrets aims at keeping all the relevant information confidential as long as possible, in order to gain the maximum competitive advantage by reserving the right to the exclusive exploitation of an invention, a discovery or an application.

However, prior to the patenting of an invention, the relevant information may nevertheless be subject to the legal protection provided for under Section 623 of the Criminal Code.

The Supreme Court of Cassation has specified that patentability of discoveries and inventions does not constitute a requirement for confidential information to be protected as trade secrets. Thus, even if the inventions and discoveries to which information refers are not eligible for patentability, any relevant information may nevertheless qualify as trade secret and avail itself of the related legal protection (*See* Supreme Court of Cassation rulings No. 11965 of 18 February 2010 – No. 25174 of 7 June 2005), provided that the concerned discoveries and inventions meet (at least) the requirement of novelty.

Unlike industrial applications, scientific discoveries and inventions covered by trade secrets are not required to be suitable for industrial use. Obviously, only those discoveries and inventions which meet this requirement may be patented.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Section 473 of Italian Criminal Code establishes criminal penalties for anyone infringes or alters trademarks, distinguishing marks, patents, design and industrial models, or uses counterfeit or altered trademarks, distinguishing marks, patents, design and industrial models.

Trade secrets may only be in connection, as specified above, to patents. However, once an invention is patented, the relevant information becomes of public domain and the holder reserves the exclusive right to use the patent for a limited period of time.

According to Italian case law, if a person other than the holder of a trade secret files with the competent office a request to patent an invention by using information thereon that is intended to be kept secret, he may be charged with revelation of trade secrets pursuant to Section 623 of Criminal Code. The same shall apply in case the invention is later patented.

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

A proceeding against whoever commits (or is suspected of having committed) the offence under Section 623 of Criminal Code may be started only once the holder of a

trade secret (normally, in person of the legal representative of the company) file with the Public Prosecutor's Office a specific report of offence. After having received a report of offence, the Public Prosecutor will start an investigation. Preliminary investigations may result in the dismissal of the case or in the charge of one or more persons with the relevant offence. In the latter case, the person in charge with violation of trade secrets may be brought to trial.
Claims for damages arising from the revelation may be filed within the criminal trial. In such a case, if a lawsuit for damages related to the offence has already been filed before a civil court, it will be dismissed. On the contrary, if a claim for damages is filed with a civil court after the starting of a criminal trial, the civil lawsuit will be suspended until a final judgment is delivered by the criminal court.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

The holder of a trade secret may not provide any specific evidence on the revelation of business confidential information. The Public Prosecutor may call witnesses and ask for the submission of documents, in order to prove that the defendant committed the offence.
Examination of witnesses called by parties usually takes the most important phase of criminal trials. It is most likely to happen that, when technical issues are at stake, the judge appoints an expert to examine the most critical aspects and acquire the elements which are necessary to evaluate the liability of the person in charge with the offence.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

Holders of trade secrets may not apply for *ex parte* orders, as they are not considered to be party in the trial. However, according to Section 244 of Italian Code of Criminal Procedure, the Public Prosecutor may ask the judge to grant a search order regarding premises, goods and persons, provided that it is essential for researching the effects of the offence (or the so called "traces of crime").
Also, the Judge, pursuant to Section 247, may order to carry out body searches, when they are necessary for finding the *corpus delicti* ("body of the crime") or other goods in relation to the crime.
Additionally, under 253 the Judge may order the seizure of the *corpus delicti* or the other goods in relation to the crimes, including, without limitation, correspondence, electronic data, files, documents.

Furthermore, even in the course of preliminary investigations, the Public Prosecutor may ask the Judge for the seizure of any goods in relation to the offence, when the free circulation thereof may result, under certain conditions, in the continuation of the offence or the perpetuation and/or aggravation of its consequences (*See* Section 321 of Italian Code of Criminal Procedure).

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Italian law on companies' criminal liability (Legislative Decree No. 231 of 8 June 2001) does not provide for liability of companies in case the offence under Section 623 of Criminal Code is committed by a person in connection to it.

2. If so, which type of liability arises for companies? Which penalties shall apply?

Not applicable

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

Not applicable

Japan

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Yes. In Japan, there is criminal liability for trade secret violation. The potential penalties are imprisonment with work and fine. This criminal liability is to protect (i) the interests of owners of trade secret, and (ii) the public interests for fair competition.

The following is a list of related literature:

- Shoen Ono/Nobuo Matsumura, " New Overview of the Unfair Competition Prevention Act (*Shin Husei Kyousou Bousi Hou Gaisetsu*)" (Seirin-shoin, 1st edition, 2011)
- Ministry of Economy, Trade and Industry "Guidelines for Management of Trade Secret" (first publicized on January 30, 2003, last revised on December 1, 2011)
- Office of Intellectual Property Policy in Ministry of Economy, Trade and Industry "Regarding Amendment to the Unfair Competition Prevention Act" (in 2009. http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/0602fukyouhoitibukaisei.pdf)
- Division of Intellectual Property Policy in Committee for Industrial Structure (*Sangkyo Kozo Shingikai*), "Regarding Direction of Re-review of Criminal Sanction concerning Trade Secret" http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/set.eigyohimitsu.pdf

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

Yes, relevant articles of the UCPA prescribing criminal sanctions establish such requirements pertaining to the purposes as "for a purpose of acquiring an illicit gain or causing injury to a holder." For your reference, please find below the English translation of relevant provisions.

	English Translation
Article 21 (1) of the Unfair Competition Prevention Act	Any person who falls under any of the following items shall be punished by imprisonment with work for not more than ten years, a fine of not more than ten million yen, or both:
(i)	a person who, for a purpose of acquiring an illicit gain or causing injury to a holder, acquires a trade secret by an act of fraud or others (which means an act of deceiving, assaulting, or intimidating a person; hereinafter the same shall apply in this Article) or an act violating control obligations (which means an act of stealing a property, trespassing on a facility, making an unauthorized access [an act of unauthorized access prescribed in Article 3 of the Unauthorized Computer Access Act (Act No. 128 of 1999)], or violating the control of

	a trade secret maintained by its holder in any other way; hereinafter the same shall apply in this Article);
(ii)	a person who uses or discloses a trade secret acquired by an act of fraud or others or an act violating control obligations for a purpose of acquiring an illicit gain or causing injury to such holder;
(iii)	a person to whom a trade secret was disclosed by its holder, and who, for a purpose of acquiring an illicit gain or causing injury to such holder, takes possession the trade secret by any of the following methods through an act of breaching of the duty to keep safe custody of the trade secret: (a) embezzling a medium containing a trade secret (which means a document, a picture or a data storage medium containing a trade secret; hereinafter the same shall apply in this item) or an object embodied a trade secret; (b) reproducing information contained in a medium containing a trade secret or an object embodied a trade secret; or (c) not deleting statement or information contained in a medium containing a trade secret that is to be deleted and disguising the said statement or information as deleted.
(iv)	a person to whom a trade secret was disclosed by its holder, and who, for a purpose of acquiring an illicit gain or causing injury to such holder, through an act of breaching of the duty to keep safe custody of the trade secret, uses or discloses it which is taken possession of by any of the methods prescribed by (a) through (c) in the preceding item breaching the duty to keep safe custody of the trade secret:
(v)	a person who is an officer (which means a director, operating officer, managing partner, secretary, auditor, or an equivalent person to them; the same shall apply in the following item) or an employee of a trade secret holder from whom a trade secret has been disclosed, and, for a purpose of acquiring an illicit gain or causing injury to such holder, uses or discloses it in breach of the duty to keep safe custody of the trade secret (except for a person prescribed in the preceding item);
(vi)	a person who is an officer or an employee of a trade secret holder from whom a trade secret has been disclosed, and, for a purpose of acquiring an illicit gain or causing injury to such holder, offers to disclose it in breach of the duty to keep safe custody of the trade secret or receives a request to use or disclose it while in office, and uses or discloses it after leaving the job (except for a person prescribed in item 4);
(vii)	a person who, for a purpose of acquiring an illicit gain or causing injury to such holder, uses or discloses a trade secret acquired by disclosure which is an offence prescribed in item 2 or the preceding three items;
(2)	Any person who falls under any of the following items shall be punished by imprisonment with work for not more than five years or a fine of not more than five million yen, or both.
(i)	a person who, for a wrongful purpose, commits any act of unfair competition listed in Articles 2(1)(i) or (xiii);
(ii)	a person who, for a purpose of acquiring an illicit gain through the use of reputation or fame pertaining to another person's famous indication of goods or business or for injuring said reputation or fame, commits any act of unfair competition listed in Article 2(1)(ii);
(iii)	a person who, for the purpose of acquiring an illicit gain, commits any act of unfair competition listed in Article 2(1)(iii)
(iv)	a person who, for a purpose of acquiring an illicit gain or causing injury

	to the user of technological restriction measures in business, commits any act of unfair competition listed in Article 2(1)(x) or (xi);
(v)	a person who misrepresents information on goods or with respect to services, or in an advertisement thereof or in a document or correspondence used for a transaction related thereto, in a manner that is likely to mislead the public as to the place of origin, quality, contents, manufacturing process, use, or quantity of such goods, or the quality, contents, purpose, or quantity of such services (except for a person prescribed in item 1);
(vi)	a person who violates a protective order; or
(vii)	a person who violates any provision of Articles 16, 17, or 18(1).
(3)	The offenses prescribed in paragraph 1, and item 6 of the preceding paragraph may not be prosecuted without a complaint.
(4)	The offenses prescribed in item 2 or items 4 to 7 of paragraph 1 shall also apply to a person who committed them outside Japan for a trade secret that had been kept within Japan at the time of the act of fraud or others, or the act violating control obligations, or at the time the trade secret was disclosed by its holder.
(5)	The offense prescribed in item 6 of paragraph 2 shall also apply to a person who committed it outside Japan.
(6)	The offense prescribed in item 7 of paragraph 2 (limited to the part pertaining to Article 18(1)) shall be governed by Article 3 of the Penal Code (Act No. 45 of 1965).
(7)	The provisions of paragraphs 1 and 2 shall not preclude application of penal provisions under the Penal Code or any other acts.
Article 22 (1) of the Unfair Competition Prevention Act	When a representative of a juridical person, or an agent, employee or any other of a juridical person or an individual has committed a violation prescribed in any of the provisions of items 1, 2 or 7 of paragraph 1 or paragraph 2 of the preceding Article with regard to the business of said juridical person or said individual, not only the offender but also said juridical person shall be punished by a fine of not more than three hundred million yen, or said individual shall be punished by the fine prescribed in the relevant Article:
(2)	In the case referred to in the preceding paragraph, a complaint filed against said offender pertaining to an offense prescribed in items 1, 2 and 7 of paragraph 1 and item 6 of paragraph 2 of the preceding Article shall also be effective against the juridical person or the individual, and a complaint filed against the juridical person or the individual shall also be effective against said offender.
(3)	The period of prescription of a penalty of fine to be imposed a judicial person or individual pursuant to the provisions of paragraph 1 in regard to an act of violation of items 1, 2 or 7 of paragraph 1 or paragraph 2 of the preceding Article shall be the same as that for the offenses prescribed in the provisions of the preceding Article.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

As you can see from our answer to Question A-1 above, a mere disclosure of the trade secret is not sufficient for a criminal charge. For a criminal charge, certain purposes and other requirements of any of each listed trade secret violation, which are set forth in Article 21(1)(i) – (vii), should be met. In addition, the punishment from (i) to (vii) are all the same. In this sense, there is a single layer of the criminal offences of trade secret violation and we do not recognize "other criminal offences."

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a *"fair use*", *"just cause", "de minimis threshold"*)?

Article 19(1)(vi) exempts from the enforcement the following act:

"*The act of a person, who has acquired a trade secret through a transaction (limited to a person who, at the time of acquiring such trade secret, had no knowledge that there had been an improper disclosure of such trade secret or that such trade secret had been acquired through wrongful acquisition or improper disclosure, and such lack of knowledge was not based on gross negligence), using or disclosing the trade secret within the scope of authority acquired through such transaction*"

This exemption includes criminal sanction as well as civil remedies. This could be a "safe harbor" in certain cases. However, we are not aware of a broader safe harbor such as "*fair use,*" "*just cause*" or "*de minimis threshold.*"

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

As you can see in the English translation of Article 21(1)(i) – (vii) of the UCPA set forth in our answer to Question A-1 above, each sub-article (Article 21(1)(i) – (vii)) requires that one of the listed patterns of a trade secret violation is completed. Therefore, criminal sanction is not applicable to an attempt or preparation of the violation of trade secret. In the general principle under the Penal Code in Japan, unless expressly stated in the statutes, an attempt or preparation of crimes cannot be subject to criminal charges (Article 44 of the Penal Code).

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

With respect to the type of items (or subject matters) covered by trade secrets, there is no difference or categorization with respect to criminal sanction.

With regard to the personal qualities of the infringer, Article 21(1)(iii) – (vi) requires that the infringer has certain relationship with the holder of trade secret (such as an employee). This criminal offence depends on the "personal qualities."

We are not aware of other categorizations with respect to criminal sanction.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

The definition of trade secret is same in the contexts of civil remedies and criminal sanction.

On the other hand, as set forth in Answer to Question A-2 above, the requirements to be met for criminal charges (Article 21(1)(i) – (vii)) are more strict than for civil remedies (Article 2(1)(iv) – (ix)). The notable differences are as follows:

(a) State of Mind

The requirements to be met for criminal charges include the specific purpose: a purpose of acquiring an illicit gain or causing injury to a holder. On the other hand, the requirements to be "unfair competition," which enable civil remedies against trade secret infringement, can be met when the infringer knows or does not know with gross negligence, for example, the fact that the information had been acquired through wrongful acquisition, when he / she disclosed or used the trade secret at issue.

(b) Method to acquire trade secret

The requirements about the method to acquire trade secret are not exactly same for the civil remedies and criminal charges.

Under Article 2(1)(iv), to meet "unfair competition" of this article, a trade secret should be acquired by theft, fraud, duress or other wrongful means (hereinafter referred to as "acts of wrongful acquisition"), or a trade secret so acquired should be used or disclosed.

On the other hand, under Article 21(1)(i), trade secret should be acquired by an act of fraud or others (which means an act of deceiving, assaulting, or intimidating a person; hereinafter the same shall apply in this Article) or an act violating control obligations (which means an act of stealing a property, trespassing on a facility, making an unauthorized access, or violating the control of a trade secret maintained by its holder in any other way to meet this criminal charge based upon this sub-article).

The "acts of wrongful acquisition" in Article 2(1)(iv) can be interpreted more broadly than act of fraud or others in Article 21(1)(i), although it depends on the facts, and the scope is not crystal clear. To say the least, the scope of such acquisition is broader in civil remedies.

In addition, the acquisition of trade secret breaching certain obligations with a holder (e.g., an employment agreement) can be the matter in both criminal charges and civil remedies.

8. Are there any limitations as to the items (i.e., documents, know-how, ideas) covered by legal protection of trade secrets?

There is no such limitation.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

The definition of trade secret is provided in Article 2(6) of the UCPA and there are three (3) requirements to become trade secret: (i) usefulness; (ii) keeping secret; and (iii) not being publicly known. These requirements should be met in order to avail of the protection as trade secret. There is no different definition in the context of civil remedies or criminal sanction.

The patentability of the items is not relevant to the extent of the protection as trade secret in principle. The patentability of the items, however, can be considered when we review the requirement of usefulness.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Yes. The following acts, respectively, provides criminal sanctions to an infringement of intellectual property right subject to each act:

- the Patent Act
- the Utility Model Act
- the Design Act
- the Trademark Act
- the Copyright Act
- the Act Concerning the Circuit Layouts of a Semiconductor Integrated Circuit
- the Plant Variety Protection and Seed Act

For your reference, please find below the punitive provisions of the Patent Act and Trademark Act.

	English Translation
Article 196 of the Patent Act	(Crime of infringement) An infringer of a patent right or exclusive license (excluding one who has committed an act that shall be deemed to constitute infringement of a patent right or an exclusive license under Article 101) shall be punished by imprisonment with work for a term not exceeding ten years or a fine not exceeding 10,000,000 yen or combination thereof.
Article 101 of the Patent Act	(Acts Deemed to constitute infringement) The following acts shall be deemed to constitute infringement of a patent right or an exclusive license: (i) where a patent has been granted for an invention of a product, acts of producing, assigning, etc., importing or offering for assignment, etc. any product to be used exclusively for the producing of the said product as a business; (ii) where a patent has been granted for an invention of a product, acts of producing, assigning, etc., importing or offering for assignment, etc. any product (excluding those widely distributed within Japan) to be used for the producing of the said product and indispensable for the resolution of the problem by the said invention as a business, knowing that the said invention is a patented invention and the said product is used for the working of the invention; (iii) where a patent has been granted for an invention of a product, acts of possessing the said product for the purpose of assigning, etc. or exporting it as a business; (iv) where a patent has been granted for an invention of a process, acts of producing, assigning, etc., importing or offering for assignment, etc. any product to be used exclusively for the use of the said process as a business; and (v) where a patent has been granted for an invention of a process, acts of producing, assigning, etc., importing or offering for assignment, etc. any product (excluding those widely distributed within Japan) to be used for the use of the said process and indispensable for the resolution of the problem by the said invention, knowing that the said invention is a patented invention and the said product is used for the working of the invention as a business; (vi) where a patent has been granted for an invention of a process of producing a product, acts of possessing the product produced by the said process for the purpose of assigning, etc. or exporting it as a business.
Article 196-2	Any person who has committed an act that shall be deemed to

of the Patent Act	constitute infringement of a patent right or an exclusive license under Article 101 shall be punished by imprisonment with work for a term not exceeding five years or a fine not exceeding 5,000,000 yen or combination thereof.
Article 197 of the Patent Act	(Crime of fraud) Any person who has obtained a patent, a registration of extension of the duration of a patent right or a trial decision by means of a fraudulent act shall be punished by imprisonment with work for a term not exceeding three years or a fine not exceeding 3,000,000 yen.
Article 198 of the Patent Act	(Crime of false marking) A person(s) who fails to comply with Article 188 shall be punished by imprisonment with work for a term not exceeding three years or a fine not exceeding 3,000,000 yen.
Article 188 of the Patent Act	(Prohibition of false marking) It shall be prohibited for a person to do the following acts: (i) putting a mark of patent or a mark confusing therewith on or in a non-patented product or the packaging thereof; (ii) assigning, etc. or displaying for the purpose of assignment, etc. a non-patented product or the packaging thereof on or in which a mark of a patent or a mark confusing therewith is put; (iii) giving in an advertisement an indication to the effect that a non-patented product is related to a patent or an indication confusing therewith for the purpose of having the product produced or used, or assigning, etc. the product; or (iv) giving in an advertisement an indication to the effect that a non-patented process is related to a patent or an indication confusing therewith for the purpose of having the process used, or assigning or leasing the process.
Article 199 of the Patent Act	(Crime of perjury, etc.) (1) A witness, an expert witness or an interpreter who has sworn under this Act and made a false statement or given an expert opinion or interpretation to the Patent Office or the court commissioned thereby shall be punished by imprisonment with work for a term between three month and ten years. (2) Where a person who has committed the crime in the preceding paragraph has made a voluntary confession before a certified copy of the judgment on the case has been served or a trial decision has become final and binding, the punishment may be reduced or exculpated.
Article 200 of the Patent Act	(Crime of divulging secrets) A present or former official of the Patent Office who has divulged or appropriated any secret relating to an invention claimed in a pending patent application that has become known to him/her in the course of performing his/her duties shall be punished by imprisonment with work for a term not exceeding one year or a fine not exceeding 500,000 yen.
Article 200-2 of the Patent Act	(Crime of breach of protective order) (1) A person who fails to comply with a protective order shall be punished by imprisonment with work for a term not exceeding five years or a fine not exceeding 5,000,000 yen or combination thereof. (2) The prosecution of the crime under the preceding paragraph may not be initiated unless a complaint is filed.

	(3) The crime under paragraph (1) shall apply to a person who commits the crime outside Japan.
Article 201 of the Patent Act	(Dual liability) (1) Where a representative of a juridical person or an agent, employee or other worker of a juridical person or an individual has committed in the course of performing his/her duties for the juridical person or individual, any act in violation prescribed in the following items, in addition to the offender, the juridical person shall be punished by a fine as provided in the corresponding item and the individual shall be punished by a fine as provided in the Article prescribed in the corresponding item: (i) Article 196, Article 196-2 or 200-2(1), a fine not exceeding 300 million yen; and (ii) Article 197 or 198, a fine not exceeding 100 million yen. (2) In the case of the preceding paragraph, the complaint under Article 200-2(2) against the offender shall have effect on the juridical person or individual and the complaint against the juridical person or individual shall have effect on the offender. (3) Where a fine is imposed on a juridical person or individual under Article 200-2(1) with regard to a violation of Article 196, 196-2 or 200-2(1), the period of prescription shall be governed by the same rules as for crimes in the provisions thereof.
Article 78 of the Trademark Act	(Crime of infringement) An infringer of a trademark right or an exclusive right to use (excluding one who has committed an act that shall be deemed to constitute infringement of a trademark right or an exclusive right to use under Article 37 or Article 67) shall be punished by imprisonment with work for a term not exceeding ten years or a fine not exceeding 10,000,000 yen or combination thereof.
Article 37 of the Trademark Act	(Acts deemed to constitute infringement) The following acts shall be deemed to constitute infringement of a trademark right or an exclusive right to use: (i) the use of a trademark similar to the registered trademark in connection with the designated goods or designated services, or the use of the registered trademark or a trademark similar thereto in connection with goods or services similar to the designated goods or designated services; (ii) the possession for the purpose of assignment, delivery or export of the designated goods, or goods similar to the designated goods or designated services, affixed with the registered trademark or a trademark similar thereto on the goods or their packages; (iii) the possession or importation of articles affixed with the registered trademark or a trademark similar thereto, that are used in the course of the provision of designated services or services similar to the designated services or the designated goods by a person who receives the said services, for the purpose of the provision of the said services through use of the said articles; (iv) the assignment, delivery, or possession or importation for the

	purpose of assignment or delivery of articles affixed with a registered trademark or a trademark similar thereto, that are used in the course of the provision of designated services or services similar to the designated services or the designated goods by a person who receives the said services, for the purpose of causing the provision of the said services through use of the said products; (v) the possession of products indicating the registered trademark or a trademark similar thereto, for the purpose of using the registered trademark or a trademark similar thereto in connection with the designated goods or designated services, or goods or services similar thereto; (vi) the assignment, delivery, or possession for the purpose of assignment or delivery, of articles indicating the registered trademark or a trademark similar thereto, for the purpose of causing the registered trademark or a trademark similar thereto to be used in connection with the designated goods or designated services, or goods or services similar thereto; (vii) the manufacture or importation of products indicating the registered trademark or a trademark similar thereto, for the purpose of using or causing to be used the registered trademark or a trademark similar thereto in connection with the designated goods or designated services or goods or services similar thereto; and (viii) the manufacture, assignment, delivery or importation, as a business, of products to be used exclusively for the manufacturing of products indicating the registered trademark or a trademark similar thereto.
Article 67 of the Trademark Act	(Acts deemed to constitute infringement) The following acts shall be deemed to constitute infringement of a trademark right or an exclusive right to use: (i) the use of the registered defensive mark in connection with the designated goods or designated services; (ii) the possession for the purpose of assignment, delivery or export of the designated goods affixed with the registered defensive mark on the goods or their packages; (iii) the possession or importation of articles affixed with a registered defensive mark, that are used in the course of the provision of designated services by a person who receives the said services, for the purpose of the provision of the said services through use of the said articles; (iv) the assignment, delivery, or possession or importation for the purpose of assignment or delivery of articles affixed with a registered defensive mark, that are used in the course of the provision of designated services by a person who receives the said services, for the purpose of causing the provision of the said services through use of the said articles; (v) the possession of articles indicating a registered defensive mark, for the purpose of using the registered defensive mark in connection with the designated goods or designated services;

	(vi) the assignment, delivery, or possession for the purpose of assignment or delivery, of articles indicating a registered defensive mark, for the purpose of causing the registered defensive mark to be used in connection with the designated goods or designated services; and (vii) the manufacture or importation of articles indicating a registered defensive mark, for the purpose of using the registered defensive mark or causing the registered defensive mark to be used in connection with the designated goods or designated services.
Article 78-2 of the Trademark Act	Any person who has committed an act that shall be deemed to constitute infringement of a trademark right or an exclusive right to use under Article 37 or Article 67 shall be punished by imprisonment with work for a term not exceeding five years or a fine not exceeding 5,000,000 yen or combination thereof.
Article 79 of the Trademark Act	(Crime of fraud) Any person who has obtained a trademark registration, defensive mark registration, registration of renewal of the duration of trademark right or right based on defensive mark registration, decision on opposition to registration or trial decision by means of a fraudulent act shall be punished by imprisonment with work for a term not exceeding three years or a fine not exceeding 3,000,000 yen.
Article 80 of the Trademark Act	(Crime of false indication) Any person who fails to comply with Article 74 shall be punished by imprisonment with work for a term not exceeding three years or a fine not exceeding 3,000,000yen.
Article 74 of the Trademark Act	(Prohibition of false indication) It shall be prohibited for a person to do the following acts: (i) in using a trademark that is not a registered trademark, to affix an indication of trademark registration or an indication confusing therewith to the trademark; (ii) in using a registered trademark for goods or services that are not the designated goods or designated services, to affix an indication of trademark registration or an indication confusing therewith to the trademark; (iii) the possession, for the purpose of assignment or delivery, of articles affixed on goods or on their packages, a trademark other than a registered trademark, articles affixed on goods other than the designated goods, or on their packages, a registered trademark in connection with goods, or articles affixed on goods or on their packages, a registered trademark in connection with services, where the indication of trademark registration or an indication confusing therewith is affixed to the said trademark; (iv) the possession or importation of articles affixed with a trademark other than a registered trademark, that are used in the course of the provision of services by a person who receives the said services, articles affixed with a registered trademark in connection with services, that are used in the course of the provision of services other than the designated services by a person who receives the said services, or articles affixed with a registered trademark in connection with goods, that are used in the course of the provision of services by a person who receives the said services, where the indication of trademark

	registration or an indication confusing therewith is affixed to the said trademark (hereinafter referred to in the following item as "articles with a false indication of trademark registration pertaining to services"), for the purpose of the provision of the said services through use of the said articles; and (v) the assignment, delivery, or possession or importation for the purpose of assignment or delivery of articles with a false indication of trademark registration pertaining to services, for the purpose of causing the provision of the said services through use of the said articles;
Article 81 of the Trademark Act	(Crime of perjury, etc.) (1) A witness, an expert witness or an interpreter who has taken an oath under this Act and made a false statement or given a false expert opinion or a false interpretation before the Patent Office or a court commissioned thereby, shall be punished by imprisonment with work for a term of between three months and ten years. (2) Where a person who has committed the offense in the preceding paragraph has made a voluntary confession before a transcript of the judgment on the case has been served, or a decision on an opposition to registration or trial decision has become final and binding, the punishment may be reduced or waived
Article 81-2 of the Trademark Act	(Crime of breach of confidentiality order) (1) Any person who fails to comply with an order pursuant to Article 105-4(1) (including cases where it is applied mutatis mutandis pursuant to Article 13-2(5)) of the Patent Act as applied mutatis mutandis pursuant to Article 39 of this Act shall be punished by imprisonment with work for a term not exceeding five years or a fine not exceeding 5,000,000yen or combination thereof. (2) The prosecution of the crime under the preceding paragraph may not be instituted unless a complaint is filed. (3) The crime under paragraph (1) shall apply to a person who commits the crime under the said paragraph while outside Japan.
Article 82 of the Trademark Act	(Dual liability) (1) Where a representative of a juridical person or an agent, employee or other staff member of a juridical person or an individual has committed, in the course of performing social activities for the juridical person or individual, any act in violation of the provisions prescribed in the following items, in addition to the offender, the juridical person shall be punished by fine as provided in the corresponding items and the individual shall be punished by fine as provided in each article prescribed in the following items: (i) Article 78, Article 78-2 or 81-2(1), a fine not exceeding 300 million yen; and (ii) Article 79 or 80, a fine not exceeding 100 million yen. (2) In the case of the preceding paragraph, a complaint under Article 81-2(2) against the offender shall also have effect on the juridical person or individual and a complaint against the juridical person or individual shall also have effect on the offender. (3) Where a fine is imposed on a judicial person or individual pursuant to paragraph (1) with regard to a violation of Article 78, 78-2 or 81-

	2(1), the period of prescription shall be governed by the same rules as for crimes in the provisions thereof.

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

In Japanese criminal proceeding, criminal prosecution should be initiated by a public prosecutor (Article 247 of Code of Criminal Procedure, the "CCP" hereunder). On the other hand, certain types of crimes are only prosecutable upon complaints from a victim or certain other persons (such as a statutory representative of a victim) in order to respect the will of a victim. A violation of trade secret is one of such crimes. With respect to subjects (or categories of trade secret such as technical information), there is no limitation for entitling to start a criminal proceeding.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

We are not aware of such limitation about evidence.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

3.1 Investigation

From a purely legal standpoint, under the Code of Criminal Procedure, a criminal investigation can only be handled by prosecutors, prosecutors' assistant officers, and judicial police officials. Therefore, a holder of trade secret may not apply for ex parte orders or ask for a precautionary seizure set forth in the question.

The proceeding itself can be ex parte. Namely, under Article 218 of the Code of Criminal Proceeding, as you can imagine, to conduct search, seizure or inspection, a warrant should be issued by a judge. However, in this proceeding, a defendant, an owner of a place or articles do not need to be involved; a judge can proceed only with a prosecutor, a prosecutor's assistant officer, or judicial police official (the "Prosecutors, etc."). After a warrant is issued, prosecutors, prosecutor's assistant officers or judicial police officials start investigation. In order to search premises and conduct other investigations, they need to show the warrant to an owner of a place, etc., subject to the search or investigation (Article 222 and 110). However, practically, warrants are shown to such persons shortly before the investigation.

With respect to computer systems, Prosecutors, etc., can search them, but it is sometimes difficult to obtain the necessary information from them. Also, they can be connected with outside servers or other systems which actually involve necessary information. In such cases, another warrant for inspection will be necessary if the

original warrant is for the search of the premises. However, if an owner voluntarily prints out the data and submits it to the Prosecutors, etc., the Prosecutors, etc. can seize it.

As to the question about whether to require the Defendant to provide information as to the whereabouts of documents and files containing such data, we would like to refer to the right to keep silent under the Constitution of Japan. The defendants can keep silence at any time in any place and they cannot be required to provide any information. On the other hand, without the approval of the Defendants, the Prosecutors, etc. can conduct search, seizure or inspection.

Going back to the measures which a holder of a trade secret can take, it is sometimes possible that a holder requests such ex parte proceeding and the Prosecutors, etc., agree and conduct such ex parte proceeding. The holder may support the Prosecutors, etc., in the process by, for example, providing information.

3.2 Measures to cease the risk of further consequences

The investigation proceeding under the Code of Criminal Procedure is to collect evidence to be used in the criminal proceeding, and it cannot be used for the purpose of ceasing the risk of further consequences arising from the misuse of trade secrets. This purpose should be achieved by an injunctive relief under the UCPA. Of course, if certain pieces of evidence are seized, the misuse may actually stop. However, it is not a direct purpose of the investigation and rather it is a derivative effect.

3.3 Measure to avoid the continuation of the offence and the perpetuation of the consequences

As set forth 2.2 above, the investigation proceeding is to collect evidence in the criminal proceeding, and it cannot be used as a measure to avoid the continuation of the offence and the perpetuation of the consequences. This purpose should be achieved by an injunctive relief under the UCPA. Of course, if certain pieces of evidence are seized, the offence may actually stop, but it is a derivative effect.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Under Article 22(1) of the UCPA, companies may be liable for trade secret violations committed by their agents, employees, contractors or representatives who work under the control of the companies. This liability is that of the companies itself.

2. If so, which type of liability arises for companies? Which penalties shall apply?

Companies can be subject to criminal sanction independently, and the available penalty is a fine up to JPY300,000,000.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

There is no special court for the specific purpose of such cases. The criminal division of normal courts may adjudicate such cases.

Latvia

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Yes, the criminal liability is provided regarding the disclosure of non-disclosable information, which is not a state secret, unauthorised acquisition and disclosure of information containing commercial secrets and unauthorised disclosure of inside information of the financial instrument market (Article 200 of the Criminal Law).

For a person who commits unauthorised acquisition of economic, scientific, technical, or other information, in which there are commercial secrets, for use or disclosure by himself or herself or another person, or commits unauthorised disclosure of such information to another person for the same purposes, as well as commits unauthorised disclosure of inside information of the financial instrument market, the applicable punishment is the deprivation of liberty for a term not exceeding five years or the custodial arrest, or the community service, or the fine not exceeding one hundred times the minimum monthly wage (Article 200 Part 2 of the Criminal Law).
For a person, who commits theft of the information indicated above, the applicable punishment is the deprivation of liberty for a term not exceeding eight years or the community service, or the fine not exceeding one hundred and fifty times the minimum monthly wage (Article 200 Part 3 of the Criminal Law).

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

Article 200 of the Criminal Law refers to the purpose "*for use or disclosure by himself or herself or another person*". Therefore, it can be concluded that it is necessary to establish the purpose to use or disclose the commercial secrets.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

If the particular activities of a person conform to the criteria for other criminal offences, the particular liability of such offence may be invoked.

For instance, the criminal liability is set forth also regarding unfair competition practices (Article 211 of the Criminal Law) - for a person who commits unfair competition practices, if commission of such offences is repeated within a one-year period, the applicable punishment is the deprivation of liberty for a term not exceeding two years or the community service, or the fine not exceeding eighty times the minimum monthly wage, with or without the deprivation of the right to engage in entrepreneurial activity for a term of not less than two years and not exceeding five years.

The criminal liability is also set forth regarding the commercial bribery (Article 199 of the Criminal Law) - for a person who commits the offering or giving of material values, property or benefits of other nature, if the offer is accepted, in person or through intermediaries to an employee of an undertaking (company) or organisation, or a person who, on the basis of the law or a lawful transaction, is authorised to conduct affairs of another person, or a responsible employee of an undertaking (company) or organisation, or a person similarly authorised by an undertaking (company) or organisation, or a person who, on the basis of the law or lawful transaction, is authorised to settle disputes so that he or she, using his or her authority, performs or fails to perform some act in the

interests of the giver of the benefit or the offerer, or any other person regardless of whether the material values, property or benefits of other nature are intended for this person or any other person, the applicable punishment is the deprivation of liberty for a term not exceeding three years, or the custodial arrest, or the community service, or the fine not exceeding fifty times the minimum monthly wage. For a person, who commits the same acts, if commission thereof is repeated or on a large scale, the applicable punishment is the deprivation of liberty for a term not exceeding five years, or the community service, or the fine not exceeding one hundred times the minimum monthly wage.

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

The general rules of Criminal Law would be applicable, where appropriate, also to the cases of unlawful acquisition and usage of commercial secrets. Such could be the mitigating circumstances (Article 47), the circumstances, which exclude criminal liability (Chapter III) and the release from criminal liability and punishment (Chapter VI).

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

The commitment of unauthorised disclosure of trade secret information to another person is one activity for which the criminal liability is foreseen (Article 200 Part 2 of the Criminal Law).

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

Article 200 of the Criminal Law - The disclosure of non-disclosable information, which is not a state secret, unauthorised acquisition and disclosure of information containing commercial secrets and unauthorised disclosure of inside information of the financial instrument market:

- For a person who commits unauthorised acquisition of economic, scientific technical, or other information', in which there are commercial secrets, for use or disclosure by himself or herself or another person, or commits unauthorised disclosure of such information to another person for the same purposes, as well as commits unauthorised disclosure of inside information of the financial instrument market, the applicable punishment is the deprivation of liberty for a term not exceeding five years or the custodial arrest, or the community service, or the fine not exceeding one hundred times the minimum monthly wage (Article 200 Part 2 of the Criminal Law).

- For a person, who commits theft of the information indicated above, the applicable punishment is the deprivation of liberty for a term not exceeding eight years or the community service, or the fine not exceeding one hundred and fifty times the minimum monthly wage (Article 200 Part 3 of the Criminal Law).

Article 211 of the Criminal Law – The unfair competition practices:

- For a person who commits unfair competition practices, if commission of such offences is repeated within a one-year period, the applicable punishment is the deprivation of liberty for a term not exceeding two years or the community service, or the fine not exceeding eighty times the minimum monthly wage, with or without the deprivation of the right to engage in entrepreneurial activity for a term of not less than two years and not exceeding five years.

Article 199 of the Criminal Law - The commercial bribery:

- For a person who commits the offering or giving of material values, property or benefits of other nature, if the offer is accepted, in person or through intermediaries to an employee of an undertaking (company) or organisation, or a person who, on the basis of the law or a lawful transaction, is authorised to conduct affairs of another person, or a responsible employee of an undertaking (company) or organisation, or a person similarly authorised by an undertaking (company) or organisation, or a person who, on the basis of the law or lawful transaction, is authorised to settle disputes so that he or she, using his or her authority, performs or fails to perform some act in the interests of the giver of the benefit or the offerer, or any other person regardless of whether the material values, property or benefits of other nature are intended for this person or any other person, the applicable punishment is the deprivation of liberty for a term not exceeding three years, or the custodial arrest, or the community service, or the fine not exceeding fifty times the minimum monthly wage.

- For a person, who commits the same acts, if commission thereof is repeated or on a large scale, the applicable punishment is the deprivation of liberty for a term not exceeding five years, or the community service, or the fine not exceeding one hundred times the minimum monthly wage.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

Yes, the criminal liability is foreseen for the unlawful exploitation and disclosure of commercial secrets and the Commercial Law also provides that a company has the rights to request the protection of its commercial secrets, as well as the compensation for damages caused by the unlawful disclosure or exploitation of commercial secrets.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

There are no limitations as such set forth by the Criminal Law as to the items of commercial secrets. Besides, the Criminal Law itself does not contain any definition what is recognized as the commercial secrets.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

As noted, the Criminal Law itself does not contain any definition, what is recognized as the commercial secrets. Furthermore, this law does not provide any specific requirements regarding the commercial secrets to be protected.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Yes, the criminal liability is provided regarding the violation of inventors' and designers' rights (Article 147 of the Criminal Law), the infringement of copyright and neighbouring rights (Article 148 of the Criminal Law) and the illegal use of trademarks, other distinguishing marks and designs (Article 206 of the Criminal Law).

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public

Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

The criminal proceedings is performed in the interests of society regardless of the will of the person to whom the harm was inflicted, if the Criminal Law does not specify otherwise, and the prosecution function in criminal proceedings on behalf of the state is implemented by a public prosecutor (Artciel 7 Part 1 of the Criminal Procedure Law). Besides, there are certain offences where criminal proceedings are initiated, if a request has been received from the person to whom harm has been inflicted.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

No specific evidence has to be shown, but it is the task of prosecutor to prove all necessary facts and circumstances of the case to establish that a particular person has committed such offence and has to be accordingly punished.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

The owner of commercial secrets may not apply for the precautionary measures within a criminal procedure and investigation, since such is available within the civil procedure. Nevertheless, either police or prosecutor may exercise their powers and means to collect evidence etc. according to the applicable laws.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Generally, in a case of legal person, a natural person who has committed a criminal offence acting as an individual or as a member of the collegial institution of the relevant legal person on the basis of a right to represent the legal person, to act on behalf of or to take decisions in the name of such legal person, or realising control within the scope of the legal person or while in the service of the legal person, is criminally liable therefor (Article 12 Part 1 of the Criminal Law). Besides, for legal persons, who are not public law legal persons, the coercive measures applicable to legal persons may be applied (Article 12 Part 2 of the Criminal Law).

2. If so, which type of liability arises for companies? Which penalties shall apply?

For the criminal offences provided for in the Criminal Law, the coercive measures may be applied to a legal person, if the criminal offence has been committed in the interests of the legal person by a natural person in conformity with the provisions of Criminal Law (Article 70^1 Part 1 of the Criminal Law). Such coercive measures, applicable to legal persons, are not applicable to State, local government and other public law legal persons (Article 70^1 Part 2 of the Criminal Law).

For a legal person one of the following coercive measures may be applied (1) liquidation; (2) limitation of rights; (3) confiscation of property; or (4) monetary levy (Article 70^2 Part 1 of the Criminal Law). Besides, the following additional coercive measures may be

specified for a legal person: (1) confiscation of property; and (2) compensation for harm caused (Article 70^2 Part 2 of the Criminal Law).

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

There are no special rules regarding the court adjudicating cases of liability of companies. The respective court is determined according to the general rules.

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

First of all, the information in question has to have the status of commercial secrets. Subsequently, for a violation to occur a respective person either has to be aware of such status of particular economic, scientific, technical or other information or a respective person should have been aware of such status.

For example, in relation to employees, the employer is obliged to identify in writing the information that is to be considered as commercial secrets (Article 83 Part 1 of the Employment Law). Therefore, in order to establish the status of commercial secrets regarding employment relations, it is necessary to establish whether an employer has accordingly protected its commercial secrets and identified in writing such information for its employees. Afterwards, all conditions of the particular provisions of Criminal Law have to be determined.

Likewise, also in relation to other persons, it has to be established that the status of commercial secrets has been ensured for the particular information. As follows, it is necessary to determine whether a particular person has been aware or should have been aware of such status and particular restrictions. Afterwards, all conditions of the particular provisions of Criminal Law have to be determined.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

As regards the criminal liability for commercial bribery and the disclosure of commercial secrets, it is not necessary that an offender qualifies as a competitor or a potential competitor. It is *vice versa* as regards the violations of prohibition of unfair competition practices.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

Yes, an aggrieved person may, in the course of criminal proceedings, submit an application regarding compensation for caused harm at any stage of criminal proceedings up to the commencement of a court investigation in a court of first instance (Article 351 of the Criminal Law). However, it is at the discretion of the suffering party whether to submit an application on compensation of the material and/or moral harm in the criminal proceedings or initiate a separate civil procedure. It shall be mentioned that usually in practice the suffering party chooses to submit an application on compensation of the harm within the criminal procedure as in the criminal procedure the burden of proof is to a large extent shared with the prosecutor, whereas in the civil procedure each party is obliged to prove its claims/ objections.

If a suffering party has brought a claim for compensation within a criminal procedure and he/she believes that the entire damage caused to him or her has not been covered with a compensation awarded in a final and binding judgement within the criminal procedure, he or she has the right to request the compensation thereof in accordance with the procedures specified in the Civil Procedure Law (Article 350 Part 3 of the Criminal Law).

In determining the amount of consideration to be awarded in civil proceedings, the compensation rendered in criminal proceedings has to be taken into account (Article 350 Part 3 of the Criminal Law). Claims for damages cannot be filed and considered simultaneously in two pending proceedings.

Lithuania

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Yes, the Criminal Code distinguishes the crimes of commercial espionage (Article 210), and disclosure of commercial secret, which causes significant material damage (Article 211). Attempts to engage in commercial espionage are also punishable. Accidental violations, on the contrary, are not punishable; the act must be deliberate.

The criminal liability for disclosure of commercial secret is applied only if the damage caused exceeds 5 648 EUR.

The sanctions vary from deprivation of the right to be employed in a certain position or to engage in a certain type of activities up to two years of imprisonment. Monetary fine may also be imposed from 37 EUR to 18 800 EUR.

For more information see commentary to the Criminal Code - G. Švedas, A. Abramavičius, E. Bieliūnas. „Lietuvos Respublikos baudžiamojo kodekso komentaras" II tomas I dalis. 2009.

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

Commercial espionage requires that the accused has an intention of unlawfully acquiring the trade secret or communicating the commercial secret to another person. Violation of a trade secret requires that the defendant has tried to obtain financial benefit for him/herself or another or to injure another by obtaining or transferring the trade secret.

Disclosing a trade secret for one's own benefit can also result in being found guilty of misuse of trade secrets or a secrecy offence, but these crimes can also be committed by only using or disclosing the information contrary to a secrecy obligation.

However, no specific purposes of violations are required to be established, such as harming competitors, obtaining advantages from use (with exception to general monetary benefit).

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

If the activity of the defendant meets the criteria for other criminal offences, such as fraud or bribery, these can also be applied. A civil lawsuit can alternatively be pursued if the criteria are met (see the questionnaire on Commercial & IP law).

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

The general "safe harbor" clauses of Lithuanian criminal law (error concerning the elements of the crime, error concerning prohibition) apply also with abuse of trade

secrets, although not very relevant in practice. The court may also opt for not sentencing the defendant (or the prosecutor can opt not to prosecute him) if the crime as a whole can be held as slight or if there are other especially weighty reasons.

The de minimis threshold established in the Criminal Code for disclosure of commercial secret is that damage caused to the victim is at least 5 648 EUR. No threshold is established for commercial espionage.

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

Attempts to engage in commercial espionage can give rise to criminal liability even though the crimes would remain on the level of attempts. Liability for commercial espionage can arise if the defendant has taken action (preparation) with intention to acquire the trade secret or with intention to transfer trade secret to another person. In other ways, the risk of disclosure of trade secrets does not give rise to criminal liability as such.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

The following violations of trade secrets are recognized in the Criminal Code:

Commercial espionage

A person who unlawfully acquires the information considered to be a commercial secret or communicates this information to another person

shall be punished by deprivation of the right to be employed in a certain position or to engage in a certain type of activities or by restriction of liberty or by arrest or by imprisonment for a term of up to two years.

Disclosure of a commercial secret

A person who discloses the information considered to be a commercial secret which was entrusted to him or which he accessed through his service or work, where this act incurs major property damage to the victim,

shall be punished by deprivation of the right to be employed in a certain position or to engage in a certain type of activities or by a fine or by restriction of liberty or by arrest or by imprisonment for a term of up to two years.

These violations equally apply to any infringer.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

Protection of trade secrets does not fall within the intellectual property law in Lithuania.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

There are no limitations. Any items which may be proven as containing commercial secrets are covered.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

The only requirement is that the definition for a trade secret provided in the Civil Code is met.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Criminal protection is provided for all intellectual property rights (copyright, patents, trademarks, designs etc.)

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

Prosecution is required to start investigation of commercial espionage and disclosure of trade secrets when prosecution becomes aware of the facts leading to a possible crime.

The holder of a trade secret may file a report however it is not required for investigation to be started or continued.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

No specific evidence has to be shown, but it is the task of the prosecutor to show beyond reasonable doubt that said abuse has occurred.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

The holder of trade secrets may not apply or any precautionary measures, but the police investigating the matter have a range of possibilities for securing and searching for evidence (such as searches of premises for investigational purposes and seizure of computer systems if they can be held as evidence in the matter) under the Code on Criminal Procedure (14 March 2002, No. IX-785, as amended).

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Companies cannot be held liable for commercial espionage and disclosure of a trade secret.

2. If so, which type of liability arises for companies? Which penalties shall apply?

Not applicable.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

Not applicable.

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

Criminal laws do not require any additional specific expression of obligation to keep secret the information for a violation to occur. The question if the accused had an obligation to keep information secret and if disclosure of information constitutes breach of trade secret protection obligations is decided by referring to civil and, in relation to employees – employment laws.
There is a difference between employees of the company and other persons, however, the difference derives from employment laws, not criminal laws (see Commercial and IP Law Questionnaire).

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

The offender may be any person and it is not required that the offender qualifies as a competitor or potential competitor.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

A civil claim for damages may be brought in criminal proceedings by the aggrieved person. If the same claim is already investigated in civil proceedings the claim in criminal proceedings would not be accepted for investigation.

Luxembourg

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Yes.

Article 309 of the Criminal Code provides that:

« Celui qui, étant ou ayant été employé, ouvrier ou apprenti d'une entreprise commerciale, ou industrielle, soit dans un but de concurrence, soit dans l'intention de nuire à son patron, soit pour se procurer un avantage illicite, utilise ou divulgue, pendant la durée de son engagement ou endéans les deux ans qui en suivent l'expiration, les secrets d'affaires ou de fabrication dont il a eu connaissance par suite de sa situation, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 251 euros à 12.500 euros.

Il en est de même de celui qui ayant eu connaissance des secrets d'affaires ou de fabrication appartenant à une personne, soit par l'intermédiaire d'un employé, ouvrier ou apprenti agissant en violation des prescriptions de l'alinéa qui précède, soit par acte contraire à la loi ou aux bonnes moeurs, utilise ces secrets ou les divulgue, soit dans un but de concurrence, soit dans l'intention de nuire à celui à qui ils appartiennent, soit pour se procurer un avantage illicite.

Est passible de la même peine celui qui, dans un but de concurrence, soit dans l'intention de nuire à celui à qui ils appartiennent, soit pour se procurer un avantage illicite, utilise sans en avoir le droit ou communique à autrui des modèles, dessins ou patrons qui lui ont été confiés pour l'exécution de commandes commerciales ou industrielles.

Les tribunaux peuvent ordonner, en cas de condamnation, l'affichage ou la publication par la voie des journaux de la décision, aux frais de la personne qu'ils désignent. »

(Free translation: "Whoever, being or having been employee, worker or apprentice to a commercial or industrial company, with the intent to compete with or harm his employer, or to obtain an improper advantage, uses or discloses during the term of his contract or within two years after its expiration, trade or fabrication secrets of which he has knowledge by reason of its position, shall be punished with imprisonment from three months to three years and a fine of 251 euros to 12,500 euros.

The same applies to the one who, having the knowledge of trade or fabrication secrets belonging to a person, being through an employee, apprentice or worker acting in violation of the requirements of the preceding paragraph, or by an act contrary to law or morality, uses or discloses the secret, either for the purpose of competition or with intent to harm the person to whom they belong, or to obtain an improper advantage.

Is liable to the same penalty, the one who, for the purpose of competition or with intent to harm the person to whom they belong, or to obtain an improper advantage, uses it without having the right or communicates to others models, designs or patterns that have been given to him to carry out commercial or industrial orders.

The courts may order, in case of a conviction, display or publication through newspapers of the decision, at the expense of the person they designate.")

The infringer of trade secrets (former employee or person who has knowledge of the trade secrets) is punished, according to article 309 of the Criminal Code (Code pénal) with imprisonment from three months to three years and a fine of 251 euros to 12,500 euros.

According to case law, facts known only to a limited circle of people who have an interest in keeping them secret, who are related to a commercial or industrial enterprise and whose disclosure is likely to cause damages to the person they relate to, can be considered as trade secrets.

(Cour d'appel de Luxembourg, 25 février 2003, n° 54/03; Tribunal d'arrondissement de Luxembourg, 30 mai 2002, n° 1370/2002; Tribunal d'arrondissement de Luxembourg, 25 mars 2003, n° 773/2003)

The definition of trade secrets is the same in civil and criminal law.

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

According to article 309 of the Criminal code described above, the infringer must commit the infringement with the intent to compete with or harm the person to whom belongs the trade secret, or to obtain an improper advantage.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

The violation of trade secrets could in certain circumstances also be qualified as theft.

Furthermore, one can mention that non-compliance with an injunction issued pursuant to an expedite action on the merits in an unfair competition case is considered a criminal offence. (article 25 of the law of 30 July 2002)

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

No.

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

The sole risk of dissemination or disclosure of trade secrets cannot give rise to criminal liability.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

Article 309 of the Criminal code distinguishes 3 categories of persons who can violate a trade secret:

- employee, worker or apprentice of the company;

- person who, having the knowledge of trade or fabrication secrets belonging to a person, being through an employee, apprentice or worker, or by an act contrary to law or morality;
- person who uses without having the right or communicates to others models, designs or patterns that have been given to him to carry out commercial or industrial orders.

These persons are not treated differently by law.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

Intellectual property law does not protect trade secrets in Luxembourg because trade secrets are not considered as intellectual property rights.

Any dissemination of trade secrets, be it manufacturing technology or commercial know how like customer information, will result in a criminal offence.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

No. The definition of trade secrets derived from case law is very broad and includes all types of items like technology, methods, documents etc.

According to case law, facts known only to a limited circle of people who have an interest in keeping them secret, who are related to a commercial or industrial enterprise and whose disclosure is likely to cause damages to the person they relate to, can be considered as trade secrets.

(Cour d'appel de Luxembourg, 25 février 2003, n° 54/03; Tribunal d'arrondissement de Luxembourg, 30 mai 2002, n° 1370/2002; Tribunal d'arrondissement de Luxembourg, 25 mars 2003, n° 773/2003)

(In English : Court of appel of Luxembourg, 25 February 2003, n° 54/03; District Court of Luxembourg, 30 May 2002, n° 1370/2002; District Court of Luxembourg, 25 March 2003, n° 773/2003)

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

There are no specific requirements that have to be met other than those mentioned in the definition mentioned in question 9 above.

Patentability should normally not impact on the extent of the protection granted by law. However, one has to mention one case where the judge decided that manufacturing secrets relate to industrial protection and were therefore excluded from unfair competition law.

(Tribunal d'arrondissement de Luxembourg siégeant en matière de concurrence déloyale, 29 janvier 1981)

(In English : Luxembourg District Court sitting in unfair competition matters, 29 January 1981)

The judge seemed to imply that since the manufacturing secret was patentable, there could be no protection by unfair competition law.

This decision is in our opinion wrong and isolated and should not have any impact on criminal law.

In any case, this question is quite important and should be addressed in any future trade secrets legislation, be it national or European.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Our jurisdiction provides for criminal protection of copyright.
There is no criminal protection for patents and trademarks as such.

However, article 184 of the Criminal code provides that will be punished (…) 'whoever counterfeits or forges seals, stamps, punches or marks of any Luxembourg authority, legal person under public or private law, under any name whatsoever, or individual person'.
Article 191 of the Criminal Code provides that 'whoever has affixed or made someone affix, by addition, deletion or any alteration, to manufactured goods, the name of a manufacturer other than that of the author, or the commercial name of a manufacturer other than that of the actual manufacturer, will be punished (…)'. The same applies to any merchant, dealer or trader who knowingly sells, imports, or circulates, goods to which supposed or altered names have been affixed.

These provisions are sometimes used by trademark holders to file criminal proceedings in accordance with article 13 of EC Regulation 1383/2003 on border measures to prevent customs from releasing the seized goods.

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

The holder of a trade secret has to file a criminal complaint with the Public prosecutor who can however decide not to prosecute the case.

The holder can also file a criminal complaint with the investigating judge ("juge d'instruction") together with a claim for damages.
In this situation, the judge will be obliged to investigate the case.
However, the complaint will have to be quite precise and evidenced.

There is no limitation as to the holder of the trade secret who can file such a criminal complaint.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

The evidence that has to be brought before the court is the same than the one necessary in civil cases, i.e. proof of the existence of the trade secret as well as of the infringement.

The proof of the infringement is however less stringent in criminal cases since the Public prosecutor and/or the investigating judge can order supplementary measures, such as house searches and the hearing of witnesses. The offender will also be heard.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

The Public prosecutor or the investigating judge, who investigate their cases in prosecution and defense independently, can order ex parte house searches as well as the seizure of items relating to the crime. However, the holder of the trade secret cannot formally apply for such a measure.

In general, the influence of the trade secret holder is quite limited in criminal proceedings.

The legislation does not provide the possibility of ex parte orders to cease the risk of further consequences arising from the misuse of trade secrets.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

The criminal liability of corporations has been introduced in Luxembourg by a law of 3 March 2010.

The offence must have been committed in the name and interest of the company by one of its statutory bodies or de jure or de facto directors.

If the company, i.e. one of its statutory bodies or directors has instructed these persons to commit the said violations or helped them, the company may be liable as an accomplice or even as a co-offender.

2. If so, which type of liability arises for companies? Which penalties shall apply?

The penalties that apply to companies are:
- fines
- confiscation of goods used to commit the offence or resulting from the offence
- exclusion of public procurement markets
- dissolution of the company

Concerning the fines, the maximum amount provided for private persons is doubled. In the case of trade secrets violations (article 309 of the Criminal code), this would be a maximum of 25.000 €

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

Only the criminal chambers of the Luxembourg and Diekirch district courts can hear criminal liability cases, hence also criminal cases based on trade secrets violations committed by companies.

The country is divided into two judicial districts, the district of Luxembourg for the capital and south of the country and the district of Diekirch for the north of the country (less important).

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

No, the specific obligation to keep secret does not have to be expressed for a trade secret violation to occur and there is no distinction between employees and other persons.

The mere existence of a trade secret is sufficient for a violation to occur.

As mentioned in point A.9 above, trade secrets are facts known only to a limited circle of people who have an interest in keeping them secret, who are related to a commercial or industrial enterprise and whose disclosure is likely to cause damages to the person they relate to.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

No.

According to article 309 of the Criminal code, the offender can be an employee or third party who intends to hurt his employer. It must hence not be a potential competitor.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

The trade secrets owner can claim damages before the criminal court together with the criminal complaint or separately before the civil court.

However, damages can of course not be claimed twice.

In Luxembourg, article 3 of the Code of criminal procedure (Code d'instruction criminelle), provides that if damages are claimed separately before a civil court, alongside criminal proceedings, the civil lawsuit will be suspended until the criminal court has rendered a judgment.

If there is already an ongoing civil lawsuit for compensation, the civil judges will hence suspend the case until the criminal judgment is rendered. To claim damages before the criminal judges, the claimant may have to drop his civil lawsuit at the request of the defendant.

Malta

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Criminal Code (Cap. 9 of the Laws of Malta):

Malta does not expressly provide for the protection of trade secrets and there are no specific provisions in the Criminal Code regulating the matter

We are, nevertheless, of the opinion that the wording contained in Articles 293 and 309 of the said Criminal Code, relating to "misappropriation" and "fraudulent gains" are drafted in such a manner as to provide a potentially wide enough interpretation, and to be construed as covering also the violation of trade secrets.

In such case, the applicable penalties include:

i. Imprisonment for a term of up to two (2) years if found to be in violation of Article 293; and
ii. Imprisonment for a term from one (1) to six (6) months or to a fine (*multa*) if found to be in violation of Article 309.

Professional Secrecy Act (Cap. 377 of the Laws of Malta):

Maltese law also provides for criminal liability in relation to the violation of any professional secrets under the Professional Secrecy Act.

The law defines a professional secret to be a secret that is confided as a result of the persons "*calling, profession or office"*.

However, the applicability of the said Act in relation to the sphere of business remains a moot point, since ultimately the provisions thereof appear to be geared towards regulating professionals in a strict interpretation of the word.

Any person in violation of the provisions of the Professional Secrecy Act may be liable to:

i. Imprisonment for a term not exceeding two (2) years; and
ii. A fine (*multa*) not exceeding forty-six thousand and five hundred and eighty-seven Euro and forty-seven cents (€ 46,587.47); and
iii. Both fine and imprisonment as aforesaid.

Exceptions to the disclosure of a "Professional Secret" include:

i. Instances where the disclosure was compelled by statute or a court order; or
ii. Instances where the disclosure was made in respect of a police investigation.

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

The wording of Articles 293 and 309 of the Criminal Code are extremely wide and, consequently, the said articles do not provide for the need of any particular pre-requisite in respect of the commission of the offence, for any such action to actually amount to such an offence.

The main elements applicable to misappropriation found in Article 293 include:

i. The person, *"misapplies or converts to his own benefit or to the benefit of another"* and
ii. *"Anything entrusted or delivered to him … for a specific purpose".*

The main elements applicable to fraudulent gains found in Article 309 include:

i. "*the prejudice of any other person"* and
ii. "*fraudulent gain*"

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

Both Civil and Criminal liability may arise consequent to the violation of trade secrets and one course of action would not preclude the other. Indeed, this is the case consequent to the fact that all criminal actions in Malta are instituted by the Executive Police and/or the Attorney General's Office, while any civil action is instituted at the behest of a private party.

Criminal liability would, potentially arise if the violation in question falls under any of the aforementioned provisions relating to misappropriation, fraudulent gains, and professional secrecy.

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a *"fair use*", *"just cause", "de minimis threshold*")?

As previously stated, there are no specific clauses or provisions in respect of trade secrets under Maltese Criminal Law.

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

In order to be held criminally liable under misappropriation the offender must be proven to have made use of the confidential information outside than the scope that it was intended and, accordingly, the risk alone would not suffice to impute criminal liability. The same would apply in respect of a fraudulent gain, where it must be proven, beyond reasonable doubt that a fraudulent gain was, in fact, made.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

As previously stated, there are no specific clauses or provisions in respect of trade secrets under Maltese Criminal Law.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

Since there is no specific criminal legislation a comparison cannot be made.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

There are no specific limitations under Maltese law to this effect.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

There are no specific requirements and the patentability of the items would not impact the extent of protection.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Yes, Maltese Criminal law does provide for various crimes in respect of the protection of other IP rights, including, patents, copyright and trademarks.

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

In terms of Article 294, the crime of misappropriation is aggravated if the thing is entrusted to the offender by reason of his, "*profession, trade, or business"*.

While in criminal matters, generally, the Executive Police are entitled to act following the complaint of the injured party; the aggravations stipulated above would entitle the Executive Police to institute proceedings *ex officio*, even without the complaint of the injured party.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

There is no pre-established specific evidence in this regard.

Under the crime of misappropriation, the plaintiff must demonstrate that consequent to the misappropriation, the person converted to his own benefit or to the benefit of another, and that the information in question was entrusted or delivered to him for a specific purpose.

Under the crime fraudulent gains the plaintiff must demonstrate that a fraudulent gain was made, i.e. the prosecution must provide sufficient evidence to demonstrate, beyond a reasonable doubt, that the defendant had the intention to deceive.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer

systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

The Criminal Code provides grants the Executive Police powers of entry, search and seizure provided that they have a warrant to this effect. Having lawfully entered any such premises the Executive Police also have the right to seize and retain documents and information.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Maltese law does not provide for criminal corporate responsibility.

Therefore it's the power of representation or who has authority to take decisions on behalf of a company that is held responsible.

2. If so, which type of liability arises for companies? Which penalties shall apply?

As stated above, there is no corporate responsibility in terms of Maltese law.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

Not applicable.

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

No there is not. The Professional Secrecy Act grants special protection to the employers in respect of his/ her employees and stipulates that, *"A person shall also be deemed to have become the depositary of a secret by reason of his calling, profession or office when he obtains such secret by reason of being an employee"*.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

Maltese Law does not make any reference whatsoever to information given to competitors.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

In terms of general principles of Maltese law, any civil action and any criminal action are to be instituted separately before the respective competent courts and, accordingly, there is no impediment for an aggrieved person, to bring a claim for damages in the course of criminal proceedings. It is important to note that the civil action and criminal act may be instituted at the same time or at a different time, provided that these are instituted in the respective competent courts, with one action having no bearing or consequence on the other.

The Netherlands

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Yes, the breach/disclosure of trade secrets is a felony under criminal law, as set out in Articles 272 and 273 of Dutch Penal Code ("DPC"). Article 272 DPC relates to the disclosure by persons appointed in a certain office or having a certain capacity e.g. an attorney disclosing confidential client information or a government inspector who has access to a factory floor for an environmental inspection. Article 273 DPC relates to the intentional disclosure by an employee of confidential details, to which he has sworn secrecy, that are not generally known and that may harm the company he works or worked for. In addition, Article 273 relates to the disclosure of confidential information that is obtained from the computer system of a commercial organisation through criminal means. Using such information for financial gain also qualifies as a crime under Dutch law.

The protection of trade secrets under criminal law is targeted mostly at the person who disclosed the secret information. It does not relate to the use of the secret information by third parties. However, under Dutch criminal law, whoever orders or procures the commission of a criminal offense can be convicted as if he committed the crime himself.

The penalty for a breach of secrecy under Articles 272 and 273 DPC is – respectively - a maximum of one year in prison and six months in prison. Each individual offense under these Articles can also be fined up to €19.500,-.

Relevant literature

A.H.G. de Groot, "General provisions regarding the penalization of the violation of secrets", *Fiscal Law Weekly* (1953), p. 461.

Ch. Gielen, *Protection of trade secrets (Preadvice for the Trade Law Society*), Zwolle 1999.

Cleiren & Verpalen (ed.), *Text & Commentary Criminal Law*, 8th ed., Kluwer (2010).

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

The public prosecutor must prove that the accused had the *intent* to disclose the confidential information (i.e. violate the trade secret). The purpose that the accused aimed to achieve (e.g. harming a former employer) may influence the penalty that the court will impose, but it does not influence the question as to whether a crime was committed.

However, under Art. 273(1)(ii) the *intentional* use *for financial gain* of certain confidential information that was obtained from a computer system of a commercial organization through criminal means also qualifies as a crime. In this case, the public prosecutor will need to prove the specific intended purpose of the accused.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

The violation of trade secrets may entail other criminal offences, including theft of secret documents or hacking of computer systems. It may also result in a civil lawsuit.

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

Article 273 DPC explicitly carves out a "safe harbor" for the accused who could have assumed – in good faith – that the disclosure was in the public interest (e.g. a whistleblower).

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

No, the disclosure and the intent to disclose must be proven in order for the accused to be found guilty. Risk of disclosure is not enough.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

The law makes a number of distinctions.

In art. 272 DPC, the law targets those who are obligated by law or profession to keep certain information confidential, such as attorneys or civil notaries.

In art. 273 DPC, the law targets those who intentionally disclose confidential information with regard to a business in which he is or was employed and to which he is contractually obligated to maintain secrecy. This provision relates to (a) (former) employees, which have been (b) contractually bound to secrecy.

Art. 273 DPC also penalizes the disclosure or use for financial gain of confidential information relating to a business which was obtained from the computer system of that business through criminal means. This provision therefore relates to any party, including – but not limited to – employees.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

Trade secrets are not protected under Dutch intellectual property laws.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

No, the DPC refers to disclosure of certain "specifics", "data" and/or "secrets" and does not contain any limitations as to the items covered by legal protection of trade secrets.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

Art. 272 DPC does not mention any specific requirements.

Art. 273 DPC(1)(i) does not mention any specific requirements.

Art. 273(1)(ii) requires that the information
(a) was not generally known; and
(b) the disclosure or use of the information is detrimental to the business (of the person) owning the confidential information.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Yes, Dutch criminal law penalizes willful copyright infringement of in Art. 31 *et seq.* Dutch Copyright Act (*Auteurswet*) and patents in Art. 79 Dutch Patent Act (*Rijksoctrooiwet*).

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

The public prosecutor may in principle prosecute a violation of Art. 272 DPC at his own initiative. However, if a specific person was harmed by the disclosure, this violation may only be prosecuted after the victim of the disclosure files a complaint.

The government may only prosecute a violation of Art. 273 DPC if *the management of the business* whose confidential information was disclosed, files a complaint.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

No.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

No, individuals – including the holders of trade secrets – do not have the right to seize evidence in a criminal trial.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Yes, under Dutch law corporations can commit crimes, just like individuals. However, the prosecution will have to show that the corporation itself committed the crime instead of – or in addition to – the individuals actually committing or organizing the criminal activities.

2. If so, which type of liability arises for companies? Which penalties shall apply?

For corporations increased fines apply (as opposed to individuals). Fines for disclosure of confidential information by a corporation can amount to €78.000,-.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

The case may be prosecuted before any of the following courts: the court of the place where the crime was committed, the court of the place where the accused resides, the court where the accused is being tried for another crime.

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

Article 272 of the Dutch Penal Code penalizes the disclosure of information that was obtained by an individual who was bound by secrecy by way of his (former) profession, e.g. an attorney disclosing confidential client information. This obligation of secrecy need not be expressed, since it is inherent to the profession of the individual. This individual need not be an employer of the business that owns the trade secret.

Article 273(1) of the Dutch Penal Code penalizes the disclosure by (former) employees of secret information, if he was bound by an obligation of secrecy. Therefore, there is only a violation of Article 273 if it was committed by a (former) employee who was bound by secrecy.

Article 273(2) relates to the disclosure, or use for motives of pecuniary gain, of data that has been obtained by means of criminal offense from a computerized device or system of a business where the data, at the time of disclosure or use, were not generally known and where any disadvantage may ensue from such disclosure or use. In such a case there is no need for the individual who is being prosecuted under this provision to be either a (former) employee or to be bound by secrecy.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

Article 272 and 273 do not require the prosecuted individual to be a (potential) competitor.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

A victim of a crime (such as breach of confidentiality, Art. 272 and 273 Dutch Penal Code) may also claim damages in criminal proceedings (Art. 51f Dutch Code of Criminal Procedure). However, a victim may not pursue an award of damages for the same crime in two venues simultaneously; therefore a claim for damages in criminal proceedings will not be admissible once civil proceedings have been initiated.

Poland

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Yes. Art. 23 of the Act on Counteracting Unfair Competition of 16 April 1993 (hereinafter "Unfair Competition Law") provides for criminal liability for trade secret violation (cited below).

Art. 23 (1) Whoever, in breach of his/her duty towards an entrepreneur, discloses to another person or derives benefit from any such information which is a company trade secret in his/her own economic activity and causes substantial damage to an entrepreneur shall be liable to a fine, restriction of liberty (community sentence) or imprisonment of up to 2 years.

(2) The same penalty shall be imposed on those who, having illegally acquired information being a company trade secret, disclose it to other persons or use it in their own economic activity.

The fine may be imposed in the maximum amount of PLN 1,080,000 (approx. EUR 260,000) and the restriction of liberty - from one month to twelve months.

List of relevant literature:

Reference material	Summary
E. Nowińska, M. du Vall, „A Commentary on the Act on Combating Unfair Competition" ed. 5, Warsaw 2010	This commentary on the Unfair Competition Law covers unfair competition acts, including criminal liability issues.
P. Kozłowska-Kalisz, „Criminal Liability for a Trade Secret Violation", Kraków 2006	The article is a comprehensive study on criminal liability resulting from trade secret violation. The author refers also to the related civil liability and provides a detailed analysis of the object of crime, including the definition of "serious damage".
P. Kozłowska-Kalisz, „Breach of a Trade Secret in the Light of Empirical Studies (in:) Theory and Practice of Criminal Law", Lublin 2005	The article is a survey of criminal liability cases resulting from trade secret violation. The author has based her research on 180 cases. The main conclusion is that trade secret cases are not considered as a high priority by public prosecutors. A large number of cases were discontinued during pre-trial proceedings.
M. Mozgawa , „Criminal Law Aspects of Combating Unfair Competition", Prosecutors and Law, 1996	One of the first articles on criminal liability resulting from an unfair competition act.

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has

the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

No.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

Yes. The violation of trade secrets may entail other criminal offences. For instance, Art. 266 § 1 of the Criminal Code of 6 June 1997 (hereinafter "Criminal Code") is a basis for liability for offences against the protection of information (cited below). This provision aims at protecting the integrity of information, its availability and confidentiality.

Art. 266 § 1. A person who in violation of the law or an obligation he/she has undertaken, discloses or uses information which he/she has become aware of in connection with the function, work performance, public, social, economic or scientific activity is subject to a fine, restriction of liberty (community sentence) or imprisonment for up to two years.

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

The trade secret violation provided for in Art. 23 (1) of the Unfair Competition Law requires that the entrepreneur have suffered a substantial damage in order to trigger criminal liability. There is no such a requirement in Art. 23 (2) of the Unfair Competition Law. The prerequisite of "substantial damage" is not exactly a "de minimis threshold", as it is not defined and would be assessed on a case-by-case basis. There are no exemptions based on "fair use" or "just cause". However, the prosecutor may discontinue the case on general grounds, if the violation is considered to bring "minimal social harm".

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

No.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

Art. 23 of the Unfair Competition Law distinguishes the following types of violations of trade secrets:

(a) disclosing, in breach of the infringer's duty towards an entrepreneur, an information which is a company's trade secret;

(b) deriving, in breach of the infringer's duty towards an entrepreneur, benefit from information which is a company trade secret in the infringer's own economic activity;

(c) disclosing information, which is a company trade secret, to other persons or using it in the infringer's economic activity if such information has been illegally acquired.

The above types of violations are treated equally. They do not depend on any personal qualities of the infringer nor the type of items covered by trade secrets.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

The criminal law provisions relating to the violation of trade secretes are provided for in the Unfair Competition Law (Art. 23) (Art. 11). However, the scopes of criminal and civil liability are not overlapping and in some instances criminal liability is limited and civil liability extended. For instance, Art. 23 (1) of the Unfair Competition Law does not penalize transfer of information which is a company trade secret but only its disclosure and use. On the other hand, civil law protects against a risk to entrepreneurs' interests while the criminal law penalizes violation of trade secrets, under Art. 23 (1), only if an entrepreneur has suffered a substantial damage.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

No, there are no such limitations. Any information irrespective of its form meeting the criteria of a trade secret is subject to protection. Please see the definition of trade secrets described in point A.5 of the Commercial and IP Law Questionnaire.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

Yes. Trade secrets, in order to avail themselves of the relevant legal protection have to meet the following criteria: (i) have commercial value; (ii) be confidential; and (iii) protection measures must have been taken to keep their secrecy. Please see also Section A.5 of the Commercial and IP Law Questionnaire.

The patentability of items covered by trade secrets does not impact on the extent of the protection granted by the Unfair Competition Law under the trade secret regime.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Yes. The Act on Industrial Property Law of 30 June 2000 (hereinafter "Industrial Property Law") provides for criminal liability for infringement of IP rights (registered and non-registered).

For instance, the Industrial Property Law provides that a person who is claiming authorship or is misleading others as to the authorship of an invention shall be liable to a fine, restriction of liberty or imprisonment for a period not exceeding one year. A sanction, of up to two years of imprisonment, is foreseen for a person who, not being entitled to be granted a patent or a protective registration right applies without authorization for a patent, protective registration right to an invention, a utility model, an industrial design or a topography of an integrated circuit created by another person. The same penalty is stipulated for anyone marking goods with a counterfeit trademark or a registered trademark, without authorization with an aim of placing them on the market.

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

The proceeding is initiated by a motion for launching criminal investigation filed with the police or the Public Prosecutor by the holder of the trade secret. Such proceedings cannot be prosecuted at the sole initiative of the Public Prosecutor.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

In order to prove violation of a trade secret in the criminal court the following evidence should be brought:

(a) for the purposes of Art. 23 (1) it should be evidenced that the holder of a trade secret has suffered serious damage and that the perpetrator acted in breach of his/her duty towards the holder of the trade secret.

(b) for the purposes of Art. 23 (2), it should be evidenced that the infringer has illegally acquired information being a trade secret.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

Yes. Under the Criminal Proceeding Code (1997) (hereinafter "Criminal Proceeding Law") the holder of trade secrets may request either the Public Prosecutor or the criminal court to search premises and computer systems for misappropriated data, seize misappropriated data or infringing items, and to require the suspects to provide information as to the whereabouts of documents and files containing such data. However, the holder of a trade secret may not apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets or ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Yes. Art. 3 of the Act on Liability of Collective Entities for Prohibited Acts (2002) (hereinafter ”Criminal Liability of the Collective Entities Law”) provides for collective entities’ (e.g. companies) liability for criminal acts committed by an individual who:

(1) acting on behalf of the entity or in the interest of the entity with the right to represent it, decides on the entity’s behalf or exercises the internal control or by exceeding this right or by failing to comply with the obligation;

(2) is authorized to act as a result of exceeding rights or breaching a duty by a person referred to in point one;

(3) is acting on behalf or in the interest of the collective entity, with the consent or knowledge of the person referred to in point one;

(4) is an entrepreneur that directly interacts with the entity in order to achieve a legally permitted objective;

- if such a behavior has brought or could have brought a benefit to the entity, even non-pecuniary.

2. If so, which type of liability arises for companies? Which penalties shall apply?

The collective entity shall be subject to criminal liability if the offence (e.g. violation of a trade secret), has been confirmed by a final judgment convicting the person mentioned in Section 1 above.

The sanction is a fine in the amount ranging from PLN 1,000 PLN up to PLN 5,000.000 (approx. from EUR 240 to EUR 1,200,000) but not higher then 3% of the revenues gained in the fiscal year when the offence was committed.

The liability based on the Criminal Liability of the Collective Entities Law does not exclude civil liability for damages nor the individual liability of the perpetrator.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

Such a case would be heard by a District Criminal Court.

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

In case of the offence defined in Art. 23 (1) of the Unfair Competition Law the offender must have acted in the breach of his/her duty towards an entrepreneur. Thus, the obligation to keep secret the information must had been expressed (directly or indirectly) prior to the breach. The law does not require that the obligation to keep secret the information is expressed in any specific manner. Further, under this provision there is no distinction between employees and non-employees to the extent that, for instance, employee's obligation to keep secret the information may be derived from general principles of the Labour Law (expressed indirectly). In case of the offence defined in Art. 23 (2) of the Unfair Competition Law there is no obligation to keep secret the information to be expressed for a trade secret violation to occur.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

No. The offender does not need to qualify as a competitor or potential competitor of the owner of the disclosed trade secret. Art. 23 of the Unfair Competition Law states that anyone ("whoever"/"those who") may qualify as an offender.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

Yes. The aggrieved person may, in the course of a criminal proceeding, bring a claim for damages. However, damages may be awarded only if as a result of the criminal proceeding the accused person was criminally convicted. If the claim for damages was considered by the criminal court on the merits, irrespectively whether or not the damages were awarded, the same claim cannot be raised in the course of the civil

lawsuit. However, if the criminal court dismissed the claim for damages, refused to consider the claim for damages or considered the claim for the damages only partially, that claim may be raised in the civil lawsuit and compensation awarded by the civil court. The general rule is that the same claim for damages/compensation cannot be considered by the both criminal and civil court.

Portugal

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

In the Portuguese legal system there is a broad criminal liability for the violation of secrets, including all sorts of secrets, whether trade secrets or not. The framework crime is described under the provisions of article 195.º of the Portuguese Penal Code (henceforth, "PPC").

"Article 195.º
(Violation of a secret)
Whoever reveals someone else's secret, which came to his knowledge because of his status, occupation, job, profession or art, shall be punished with imprisonment up to one year or with a fine up to 240 days".

This framework crime is accompanied by several specific incriminations, arising from particular characteristics of the criminal activity, such as the nature of the secret or the identity of the agent.

However, within the PPC there is no specific incrimination of the violation of trade secrets. The incrimination of the violation of secrets is seen as a means to protect a personal benefit: the privacy of a person.

In addition to the referred incrimination, the PPC differentiates the undue usage of a secret as an autonomous crime. The framework crime is described under the provisions of article 196.º of the PPC.

"Article 196.º
(Undue use of a secret)
Whoever uses a secret relating to someone else's commercial, industrial or artistic activity, which came to his knowledge because of his status, occupation, job, profession or art, and by that gives cause to damages to another person or the State, shall be punished with imprisonment up to one year or with a fine up to 240 days".

Differently from the mere violation of secrets, the incrimination of the undue ue of a secret, aims to protect the secret as an economic asset, or, in other words, the economic advantages that the owner of the secret obtains from its use.

Relevant literature on the subject:
- Jorge de Figueiredo Dias, "Comentário Conimbricense do Código Penal", Tomes I and III, Coimbra Editora, 1999;
- Manuel Lopes Maia Gonçalves, "Código Penal Português Anotado e Comentado", 18th edition, Almedina, 2007;
- Paulo Pinto de Albuquerque, "Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem", Universidade Católica Editora, 2008.

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

According to the provisions of article 195.º of the PPC, the mere disclosure of a secret without the consent of its owner is considered a crime, independently of the purpose or the motives of the agent of the crime.

Nonetheless, if the agent seeks to gain a financial advantage with his criminal activity or if intends to cause harm to another person, said intention has relevance, on the one hand, (a) to characterize the criminal activity of the agent as undue use of a secret (pursuant to Article 196º), on the other hand, (b) to increase up to one third the maximum and minimum limits of the penalties applicable to the agent, pursuant to Article 197.º of the PPC.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

Given the generic and broad nature of the types of incrimination regarding violation of secrets and the undue use of secrets, under the provisions of Articles 195.º and 196 .º of the PPC, these incriminations usually encompass other more specific incriminations.

However, as with other crimes, the violation or the undue use of a secret may entail practicing other criminal offences – e.g., slander (Article 180.º of the PPC), insult (Article 181.º of the PPC) or computer and communications fraud (Article 221.º of the PPC).

Like in any other crime that gives cause to harm, the agent of the violation of secrets or of the undue usage of secrets may be held liable for the damages caused, the offender being entitled to an indemnity, which may be claimed within the criminal procedure itself, under the provisions of article 71.º of the PPC.

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

Since both the violation of secrets and their undue use of secrets are incriminated in case the owner of the secret does not authorize the agent to reveal or to use the secret, the consent of the owner is sufficient to avoid incrimination.

Apart from the obtaining consent, the violation or undue use of secrets may be justified or excused, if a legal provision authorizes it (such as the procedural legal provisions determining the breach of secrets, in order to discover the truth), or if any of the absolving justifications of the PPC are applicable (such as legitimate defense, situation of distress and conflict of duties).

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

Both the violation and the undue use of secrets are incriminations which always depend of an objective harm made to the secret.

This means that the mere creation of a risk of harm by the agent is not enough to give rise to criminal liability.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

The PPC distinguishes various specific violations of secrets from the framework crime described on Article 195.º, depending on the nature of the secret or on the identity of the agent, such as the following provisions:

"Article 316.º
(Violation of a State secret)
1- Whoever, jeopardizing the Portuguese State's interests regarding national independence, the State's unity and integrity or its internal and external security, transmits or makes accessible to unauthorized personnel, or makes public fact or document, plan or object, which should, in the name of those interests, remain secret, shall be punished with imprisonment from two to eight years.
2- Whoever destroys, subtracts or falsifies a document, plan or object referred in the previous number, jeopardizing the interests indicated in the same number, shall be punished with imprisonment from two to eight years.
3- If by practicing the behavior described in the previous numbers, the agent violates a duty specifically imposed to him by the status of its function or service, or the mission which was conferred to him by a competent authority, shall be punished with imprisonment from three to ten years.
4- If the agent negligently practices the facts referred on numbers one and two, having access to the objects or secrets of State because of his function or service, or of mission which was conferred to him by a competent authority, shall be punished with imprisonment up to three years."

This specific incrimination differs from the generic framework crime of the violation of a secret, through the nature of the secret revealed, which has to be a State secret, and also through the additional requirement of the endangerment of essential State interests.

The extreme gravity of this criminal activity, which by nature endangers the existence of the State itself, justifies its punishment with more severe penalties.

"*Article 371.º*
(Violation of an investigation secret)
1- Whoever illegitimately makes public the totality or part of the content of an act performed within a penal procedure, which is covered by investigation secrecy, or to which course the general public is not allowed to assist, independently of having contacted with the procedure or not, shall be punished with imprisonment up to two years or with a fine up to 240 days, except if a different penalty is applicable to the case according to the procedural law.
2- If the fact described in the previous number concerns to:
a) A procedure concerning an administrative offence, until the administrative authority's decision; or
b) A disciplinary procedure, while the secret is legally maintained;
the agent shall be punished with imprisonment up to six months or with a fine up to 60 days."

This specific incrimination differs from the framework crime, through the nature of the secret, which is, in this case, the investigation secret, as a means to guarantee the efficiency of the investigative authority's labor in attaining the truth.

The legislator clearly graduates the gravity of this criminal activity in different terms, according to the nature of the procedure in question: when the secret is related to a criminal procedure, the penalties are higher than the ones established in the framework

crime; when the secret is related to non-criminal procedures (administrative or disciplinary), the penalties are lower.

"Article 383.º
(Violation of a secret by public official)
1- The public official who, without being duly authorized to do so, reveals a secret of which he gained knowledge or that has been transmitted to him due to is functions, or which knowledge has been facilitated by his role, with the intention of obtaining, for himself or for other person, benefit, or with the consciousness of giving cause to damages to the public interest or to third parties, shall be punished with imprisonment up to three years or with a fine.
2- If the public official practices the fact foreseen in the previous number and by doing so creates a hazard to the life or the physical integrity of other person or to high value assets of other person shall be punished with imprisonment from one to five years.
3- The criminal procedure depends of the complaint of the entity that superintends the respective service or of the complaint of the aggrieved party."

This specific incrimination differs from the framework crime both by the identity of the agent and by the nature of the secret revealed. On the one hand, the agent of this criminal activity must be considered a public official for criminal purposes, under the provisions of article 386.º of the Portuguese Penal Code. On the other hand, the agent must have acquired konwledge of the (trade) secret due to his position in the public entity.

"Article 384.º
(Violation of a correspondence or telecommunication secret)
1- The public official from postal, telegraph, telephone or telecommunications services who, without being duly authorized:
a) Suppresses or subtracts letter, package, telegram or other communication entrusted to those services and which is accessible to him in result of his functions;
b) Opens letter, package or other communication which is accessible to him in result of his functions or, without opening it, gains knowledge of its content;
c) Reveals to third parties communications between certain persons, made by postal mail, telegraph, telephone or other means of telecommunications of those services, of which he gained knowledge in result of his functions;
d) Records or reveals to a third party the full or partial content of the referred communication, or makes it possible to hear them or to gain knowledge of them; or
e) Allows or promotes the facts in the previous subparagraphs;
shall be punished with imprisonment from six months to three years or with a fine no lower than 60 days."

This specific incrimination differs from the framework incrimination by the identity of the agent and by the method by which the harm is made. On the one hand, the agent of this incrimnation must be a public official from the postal, telegraph, telephone or telecommunications services. On the other hand, the harm caused to the secret must be made through the normal channels of the delivery of correspondence or communications.

The legislator considered it to be relevant to confer a specific protection to the confidence of the population on the public postal and communications services.

There is a relevant specific type of undue use of secrets, described on Article 378.º of the Portuguese Securities Code, which consists on insider trading practices within the securities market.

8. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts

prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

Under the provisions of the PPC there is no specific legal notion of trade secret.

9. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

Articles 195.º and 196.º of the PPC do not specify any limitation of the scope of the incriminations and, therefore, all trade secrets irrespective of their form or nature are covered.

10. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

As previously referred in response to the previous questions, the framework crimes in Articles 195.º and 196.º of the PPC give a broad coverage to trade secrets, regardless from their form or nature and, therefore, irrespective of its patentability.

However, the legal protection of trade secrets, under the provisions of article 318.º of the IPC, depends of three requirements: the confidential nature of the knowledge, its commercial value in result of the secrecy and having occurred considerable efforts by the holder of the secret to maintain its secrecy.

Nevertheless, since the IPC only considers the violation of trade secrets as an administrative offence, this offence can be consumed by the criminal offences of the Portuguese Penal Code, under the provisions of article 20.º of the Portuguese Administrative Offences Law.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

There is no specific incrimination regarding the violation of any IP registered rights under the provisions of the PPC.

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

Both the violation and undue use of secrets are considered semi-public crimes under the provisions of article 198.º of the Portuguese Penal Code, meaning that the Public Prosecutor may not initiate criminal proceedings by his sole initiative.

The commencement of criminal proceedings depends of a complaint set by the aggrieved party. The aggrieved party is the individual whose rights or interests are protected by the incrimination, which – as regards trade secrets – means the aggrieved party tends to be the owner of the secret.

However, if the aggrieved owner of the secret perishes before exercising his right to complain, his descendants may exercise it.

The right to complain must be exercised within the time limit of six months, counting from the date in which the aggrieved party gains knowledge of the criminal activity.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

Under the provisions of article 127.º of the Portuguese Penal Procedure Code, the court may base its conviction and decision freely upon analysis of the evidence carried to the procedure.

This means that the court does not depend of a specific type or form of evidence to decide on the criminal liability of the agent of a violation or undue use of secrets.

The only evidence which may not be considered by the court is evidence that should be considered forbidden pursuant to Article 126.º of the Penal Procedure Code – such as evidence obtained through torture, coercion, or any offense to the physical or moral integrity of people, and also evidence obtained through the illegal intromission on the private life, domicile, correspondence or telecommunications of people.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

Under the provisions of article 174.º, number 2 of the Portuguese Penal Procedure Code, whenever there are traces that the objects related to a certain criminal activity are present in a place with restricted or no access to the general public, a search may be ordered.

In case the place in question is the domicile of an individual, a search warrant issued by a judge is usually necessary to conduct the search. In the other cases the search may be ordered by the Public Prosecutor.

The holder of the secret may therefore request the Public Prosecutor or the competent judge to order a search.

However, the holder of a trade secret may not require the defendant to provide information as to the whereabouts of documents or files containing such data.

In fact, the defendant is entitled to remain silent throughout the penal procedure, being constitutionally forbidden any kind of mandatory self-incrimination.

Regarding the means to cease the risk of further consequences arising from the misuse of trade secrets, the holder is entitled to request the interim measures consecrated in the Civil Procedure Code, as long as he proves the existence of danger to the content of his right and the urgency in attaining an interim decision that removes such danger.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

According to the provisions of the Portuguese Penal Code, companies are only criminally liable for a narrow number of crimes, listed on article 11.º.

Among those crimes, the Portuguese Penal Code does not include the violation or undue use of a secret, which means that the legislator considered that companies cannot be considered criminally liable for such crimes.

This does not exclude the criminal liability of any agents, employees, contractors, consultants or representatives of those companies for those criminal activities, even if the referred individuals were only acting in the compliance of company orders.

However, in these cases the agents of the criminal activity may benefit from an absolving excuse, given the circumstance he is complying with company orders, in order to maintain his job.

2. If so, which type of liability arises for companies? Which penalties shall apply?

Not applicable.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

Not applicable.

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

Although some areas of the Portuguese Law determine specific secret-keeping obligations, such as the Labor Code in what concerns employees' duties, the incrimination of the violation of a secret or the undue use of a secret are not dependent of the existence of such specific obligations. For those incriminations to be verified, it is sufficient that there is a secret owned by some entity and it is revealed or used by the criminal agent, and also the knowledge of such secret having been obtained because of the agent's status, occupation, job, profession or art.

Therefore, even though employees may be more prone to act as the agents of such criminal activity, as they shall often deal with trade secrets of their employers, any specific confidentiality obligation arising from the labor agreement or from the Portuguese Labor Code, if non-complied, only produces civil effects (entitlement to an indemnity), and not specific criminal effects apart from the general incriminations of Articles 195º and 196º of the Portuguese Penal Code.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

For criminal liability purposes, no specific quality of the agent is required by the incriminations of Articles 195º and 196º of the Portuguese Penal Code, meaning the agent does not have to be a competitor or potential competitor.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

Under the provisions of Article 71º of the Portuguese Penal Procedure Code, the aggrieved party must bring a claim for damages within the penal procedure, except in some cases, listed on Article 72º of the Portuguese Penal Procedure Code, in which a civil claim may be brought to court separately from the criminal procedure. These cases include situations such as the penal procedures which are dependent of a complaint by the offended party.

When pursuing a penal procedure depends on the filing of a complaint by the offended party, the submission of a civil claim by the aggrieved party before the submission of the penal complaint has as the effect of renouncing the right to complain within a penal procedure. This means that in these cases an ongoing civil lawsuit for compensation prevents a posterior criminal procedure with the same factual scope.

If a civil lawsuit for compensation is already ongoing when a criminal procedure regarding the same factual basis is started, the presentation of another claim for damages within the criminal procedure shall not be legally possible, due to the *lis pendens* exception.

Romania

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Romanian criminal provisions are not set forth in a sole criminal law, being scattered between the Criminal Code, as the general criminal law, and specific laws regulating certain fields or activities, which include sections referring to criminal offences.

The criminal liability for trade secrets violation is specifically regulated under Romanian Unfair Competition Law. In addition, the Romanian Criminal Code sanctions specific criminal deeds in relation to state secret, professional secret and business secret.

As a general principle under Romanian law, the same criminal deed could not be sanctioned twice. Therefore, violation of a specific trade secret will be sanctioned under the relevant specific law or, if not applicable, under the Unfair Competition Law, as the general law regulating protection of trade secrets. If the trade secret is part of a state or professional secret, the relevant provisions of the Criminal Code will be applicable.

The penalties for criminal offences are imprisonment or criminal fines, which could be accompanied by other non-custodial (precautionary) punishments.

Unfair Competition Law

Please see below a comparative analysis of the criminal offences related to trade secrets violation, as reflected in the Romanian unfair competition law in force and the unfair competition draft law:

Unfair Competition Law in force (Law 11/1991)		Draft Law	
Text of deed	Sanction	Text of deed	Sanction
Criminal offences		Criminal offences	
the use for commercial purposes of results of experiments whose obtaining required considerable effort or other secret information in relation thereto, provided to the competent authorities in view of acquiring marketing authorizations for pharmaceuticals or agricultural chemical products, containing new chemical compounds (art. 5, para 1, letter c)	imprisonment from 6 months to 2 years or fine ranging from 2.500 lei (c.a Eur 570) to 5.000 lei (c.a Eur 1.135)	the use for commercial purposes of results of experiments whose obtaining required considerable human or financial effort or other secret information in relation thereto, provided to the competent authorities in view of acquiring marketing authorizations for pharmaceuticals or agricultural chemical products, containing new chemical compounds (art. 11, para 1, letter a)	imprisonment from 6 months to 5 years or fine ranging from 20.000 lei (c.a Eur 4.545) to 200.000 lei (c.a Eur 45.450) plus, if the case may be: complementary sanctions:
the disclosure of the information provided under letter c), except when the disclosure of such information is required in order to protect the public or except when measures have been taken in order to ensure that the		the disclosure of the information provided under letter a), except when the disclosure of such information is required in order to protect the public or except when measures have been taken in	a) the prohibition of being a shareholder, director or holding another executive position within a company; b) the prohibition of directly or indirectly operating a company for up to 2 years upon the

information are protected against unfair commercial use, if such information stem from the competent authorities (art. 5, para 1, letter d)	order to ensure that the information are protected against unfair commercial use, if such information stem from the competent authorities (art. 11, para 1, letter b)	date a conviction is issued.
the disclosure, the acquisition or the use of a trade secret by third parties, without the consent of the legitimate owner of such trade secret, as a result of an action of commercial or industrial espionage (art. 5, para 1, letter e)	the disclosure, the acquisition or the use of a business secret by third parties, without the consent of the legitimate owner of such business secret, as a result of an action of business espionage (art. 11, para 1, letter c)	
the disclosure or the use of the trade secrets by persons pertaining to public authorities, as well as by persons empowered by the legitimate owners of such secrets in order to represent them before the public authorities (art. 4, para 1, letter f)		

Criminal Code

a) Provisions of the Criminal Code currently in force

Professional secret (Article 196 Criminal Code)

"Disclosure, without right, of data by those to whom they were entrusted, and who learned as a result of their job or position, if the offense is likely to harm a person, shall be punished with imprisonment from 3 months to 2 years or a criminal fine."

Business secret (Article 298 Criminal Code)

"Disclosure of data or information which is not intended to be publicly known, by the person who knows such data as a result of his/her professional duties, if the offense is likely to cause damages, shall be punished with imprisonment from 2 to 7 years.

If such disclosure is made by other persons, irrespective of the way such other persons managed to know the respective data or information, the punishment will be imprisonment from 6 months to 5 years."

As a general comment, it should be mentioned that the business secret violation under the Criminal Code is in fact an aggravate form of the professional secret violation, provided that the infringer is an employee or other person who knows the secret as result of his/her professional duties (para 1 of Article 298). In case the infringer has no special quality (para 2 of Article 298), the business secret violation is quite similar with the same crime sanctioned under the Unfair Competition Law.

State secret

Disclosure, illicit appropriation and/or unpermitted use of state secrets are also punished under Romanian Criminal Code, with imprisonment and restriction of certain civil rights.

b) Provisions of the Criminal Code coming into force in 2012

Disclosure of secret professional information or non-public information (Article 304)

"The unlawful disclosure of secret professional information or of information that is not intended for public use, by the person who knows them as result of his/her professional duties, if such deed affects the interests or the activity of a person, shall be punished by imprisonment from 3 months to 3 years or by fine.

Unlawful disclosure of secret business information or of information that is not intended for public use, by the person who takes cognizance of the same, shall be punished by imprisonment from one month to one year or by fine.

If, as a result of the deed provided for under paragraph (1) and paragraph (2), a crime was committed against the undercover investigator, the protected witness imprisonment from 2 to 7 years, and if a crime against life was committed with intent, the punishment is imprisonment from 5 to 12 years."

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

In case of criminal liability of trade secret violation under the Unfair Competition Law, there is a sole criminal offence qualified by purpose, respectively the use of results of secret experiments referring to pharmaceuticals or agricultural chemical products containing new chemical compounds (article 5, para 1, letter a). In this case, the use of secret experiment information is sanctioned only if such use is made by the infringer for "commercial purposes", namely for profit or other financial advantages.

In case of criminal liability of professional/business secret violation under the Criminal Code, the secret violation is sanctioned even if no purpose of the infringer is revealed.

However, please note that the criminal liability under the Romanian law is usually a direct or indirect outcome of a "general purpose" of the infringer, who must act by intention, deliberately. This intentional behavior of the infringer, which is different from the special purpose referred by your question, must also exist in the trade/professional secret violation.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

Violation of trade secrets may result in a criminal lawsuit, when the violation is incriminated by one of the criminal offences mentioned at point 1 from above. In this case, it is a matter of public policy and the violation, if proved, is sanctioned with criminal fine or imprisonment and, in addition, with potential non-custodial punishments (i.e: prohibition of being a shareholder or director within a company).

The same violation may also result in a civil lawsuit, in order for the prejudiced owner of the disclosed secret to sue for damages and obtain redress from the infringer.

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

The "safe harbor" clauses in the Romanian criminal law are specific conditions under which the offender may not be prosecuted, although the "violation" (disclosure, use, etc) had occurred. For instance, in case of trade secrets abuse:

a) general "safe harbor" clauses

- disclosure, acquisition or use of a trade secret is not sanctioned if the consent of the legitimate owner of the secret was previously obtained. In case of violation of professional secret (article 196 Criminal Code), the later parties' reconciliation removes criminal liability;
- disclosure of professional secret is permitted at the request of courts, prosecutors or other criminal investigation authorities, the persons receiving such confidential information being also obliged to keep it secret.

b) specific "safe harbor" clauses

- disclosure of the results of secret experiments referring to pharmaceuticals or agricultural chemical products containing new chemical compounds, if such information stem from the competent authorities, is not sanctioned when the disclosure of information is required in order to protect the public;
- disclosure of banking secret by the bank's employees is permitted in certain cases (i.e: at the request of the accountholders or their legal and/or statutory representatives, or with their explicit permission; in case the bank has a legitimate interest).

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

The risk of dissemination/disclosure of trade secrets by itself (the "attempt"), if not followed by concrete actions of dissemination/disclosure, is not sanctioned under Romanian criminal law.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

There are two main types of violations of trade secrets under Romanian criminal law, depending on the personal quality of the infringer:

a) the trade secrets violations made by an employee or other person who knows the secret as result of his/her professional duties (trade secret as part of professional secret);

b) the trade secrets violations made by persons having no specific quality for the purposes of the criminal law, regardless of the way such other persons managed to know the respective secrets.

The trade secret violation made by professionals is more severely sanctioned because the trade secret abuse is doubled by an employment/disciplinary abuse.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

As described at Point 2 and Point 4, Section A - Commercial and IP Law Questionnaire, trade secrets are not specifically protected under the Romanian Intellectual Property Law.

However, information regarding the invention described in the patent application may be protected as trade secret until the publishing of the patent application. Non-disclosure of such information by the staff of the State Office for Inventions and Trademarks represents a conduct prohibited under intellectual property law which also results in criminal offence, considering that this type of information is confidential for such staff and its simple disclosure is punished with imprisonment, without being necessary supplementary requirements to be met.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

Legal protection of trade secrets covers items regardless of the instrument in which they are incorporated, provided that the respective documents, know-how, ideas etc, cumulatively met the legal general requirements of a trade secret, namely:

- they are not generally known by, or not easily accessible to, the persons in the environment that usually deals with such information;
- they gains commercial value by being secret;
- their legitimate owner preserved the secrecy.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

According to provisions of Unfair Competition Law, specific requirements for certain trade secrets in order to obtain protection under criminal law may be considered the following:

- missing of the owner consent for disclosure (art. 5, para 1, letter e);
- disclosure, acquisition or use of a trade secret is a result of an action of commercial or industrial espionage (art. 5, para 1, letter e);
- the trade secrets stem from persons pertaining to public authorities (art. 5, para 1, letter d); or
- disclosure or use of the trade secrets is made by persons empowered by the legitimate owners of such secrets for representing them before the public authorities (art. 4, para 1, letter f).

Considering all the above mentioned, the patentability of a trade secret is not a requirement for obtaining criminal protection under the Romanian criminal law.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Romanian legislation stipulates measures for criminal protection of IP registered rights, such as patents or trademarks. For instance, Romanian Trademark Law[1] entitles the owner of a registered trademark to claim the criminal liability by a counterfeit action. Also, as we already mentioned in the Commercial and IP Law Questionnaire, invention are protected by criminal law before its patent registration, considering that disclosure of the information contained in a patent application, prior to its publication, represents a criminal offence.

B. CRIMINAL LITIGATION

[1] Law 84/1998 on trademarks and geographical indications, as republished in 2010

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

Criminal investigation for trade secret violation is usually initiated by means of a prior complaint filed by the person having suffered damages as result of unlawful disclosure or by any interested party having a legitimate interest, including Competition Council. For instance, *ex officio* investigations can not take place for the criminal offences provided by the Unfair Competition Law and by article 196 of the Criminal Code (disclosure of professional secret), the prior complaint being mandatory.

By exception, *ex officio* trade secrets investigation is permitted in very limited cases and is generally put in place by the police, as the main investigation force, the Public Prosecutor having a supervisory role, allowing or denying certain investigation actions executed by the police. If he/she considers there are enough grounds in order to start the proceedings, the Public Prosecutor allows *ex officio* police initiative and decides to send the cause in court.

Also, the holder of the secret may file a report of the offence with the police or Public Prosecutor in order to start investigation proceedings, but however the ruling to send the cause for the court judgment belongs to the Public Prosecutor. If he/she decides not to send the cause in court, such ruling can be appealed.

The criminal files for which the Public Prosecutor ruled to be sent shall be judged in courts of law.

Claims for civil damages can be directly started by the legitimate holder of the trade secret or, as the case may be, by the person/persons having suffered damages as result of the trade secrets violation.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

There are no specific evidences to prove the abuse of trade secrets under Romanian criminal law.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

The holder of the trade secret has no direct action to ask the court for permission to search premises and computer systems for misappropriated data. Such proceedings can be ordered only by the Public Prosecutor during the investigation of a criminal complaint, if there are enough grounds in order to do that, and must be approved by judge. In theory, *ex parte* orders coercing the defendant to provide information as to the whereabouts of documents and files containing the trade secrets of the plaintiff could be obtained if certain evidence is provided to the court.

However, in case of trade secrets violation in competition field the legitimate holder may ask the Competition Council to present in court, as evidences, the results of its investigation on the premises and computer systems of the infringer, provided that such

investigation was already performed by such authority (for details in relation to investigative powers of the Competition Council, please see the answer to point 3 - Section B of the Competition Law Questionnaire). In addition, according to specific provisions of Unfair Competition Law, the legitimate holder of the trade secret may directly ask the court to rule upon certain measures of prohibition of the industrial and/or commercial exploitation of the products resulting from the illicit appropriation of the trade secret or of destruction of such products.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Romanian criminal law stipulates the principle of personal liability, so no other person may be held liable under the criminal law instead of or jointly with the offender.

Nevertheless, the company is liable for those trade secrets violations which are committed in relation to its scope of work, on its own behalf or for its benefit. In such cases, the criminal liability of the company does not exonerate the criminal liability of the natural person who contributed, in any manner, to the perpetration of the respective violation.

In conclusion, the companies are liable under criminal law only for their own trade secret violations, not for the ones committed by their agents, employees, contractors, consultants or representatives, on their own behalf and for their personal benefit.

In the view of civil liability under the Unfair Competition Law, the company shall be held liable jointly with the employee for the damages caused in the course of exercising his/her professional duties, unless it can prove that it was not in the position to prevent the perpetration of such violation.

2. If so, which type of liability arises for companies? Which penalties shall apply?

Penalties applicable to companies according to Romanian criminal law are the following:

- the sole main penalty which may be inflicted on companies is the criminal fine, with common limits from 2,500 lei (c.a Eur 570) to 2,000,000 lei (c.a Eur 455.000), as it is stipulated in the Criminal Code; the special limits for unfair competition criminal offences on trade secrets are 2,500 lei to 5,000 lei (c.a Eur 1.135).
- complementary penalties which may be ordered by the court additionally to the main sentence are:
  - company ’s winding-up;
  - interruption of the company’s activity for a period of 3 months to one year or the suspension of one of the activities performed by the legal person, in respect of which the offence was perpetrated, for a period of 3 months to 3 years;
  - closing down of certain offices of the company for a period of 3 months to 3 years;
  - prohibition to take part in any tender procedure for a period of 1 to 3 years;
  - posting or publishing of the court decision.

- precautionary measures - the precautionary measures are regulated by Criminal Code without making any distinction between the natural persons and the legal entities. The specialized literature mentions that the special seizure is the sole precautionary punishment which could be ordered in respect of the companies. The special seizure may be enforced only in respect of the goods that are closely related to the perpetrated offence.

Although the companies can not be convicted under criminal law for offences committed by their employees, they can be held liable for damages injured by third parties as result of such offences, based on the non-contractual liability rules. For example, as already mentioned above, in case of a criminal offence committed by an employee in the performance of his professional duties, the employer will be held liable jointly with the employee for damages caused, unless the former can prove that it was not able to prevent the offence.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

According to the Unfair Competition Law, the competent court which may adjudicate cases of criminal liability of companies for trade secrets violations is the tribunal in whose jurisdiction the offenses were committed or in where the premises of the defendant is located.

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

Being an employee of the company owning the trade secret is not a condition for a person to be held liable for the criminal offences stipulated by the Romanian Unfair Competition Law[2]. Also, according to Romanian Unfair Competition Law there is no distinction regarding the criminal fine applied to the offender who is an employee of the company owning the trade secret or to any other third party who may be held liable for the criminal offence of disclosing trade secrets.

According to Romanian Criminal Code there is a distinction between the act of disclosing business secrets by an employee ant the act of disclosing business secrets by another person. Consequently, the criminal offense of disclosure of business secrets by the employees, if such disclosure is likely to cause damage, is punished with imprisonment from 2 to 7 years. The criminal offense of disclosure of business secrets committed by other persons, regardless of the way such other persons managed to know the respective business secrets, is punished with imprisonment from 6 months to 5 years. As a conclusion, according to Romanian Criminal Code disclosing of a business secret by an employee is an aggravating circumstance.

As for the offense of disclosing professional secret, considered by the Romanian Criminal Code an unlawful disclosure of data if such disclosure is likely to harm a person, by the persons to whom such data were entrusted or who learned as a result of their job or position, is punished with imprisonment from 3 months to 2 years or with criminal fine. Therefore, disclosing of professional secret may be committed only by a person to whom the professional secret was entrusted during the performing of its profession/job. In fact, such disclosing may be perpetrated by an employee only or at least by a person who is in a work relation with the company owning the professional secret, even if it is not necessarily an employment relation.

[2] Unfair Competition Law no 11/1991

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

A certain person may be held liable as a criminal offender for an unlawfully disclosure of a trade secret without being necessary to be a competitor or a potential competitor of the owner of the disclosed trade secret. As a result, being a competitor or a potential competitor of the owner of the disclosed trade secret is not o condition for the offender to be punished under the Romanian Unfair Competition Law. Also, it is not necessary for the offender to be a competitor or a potential competitor of the owner of the disclosed business secret/professional secret in order to be sanctioned for the disclosure of business secret or professional secret according to Romanian Criminal Law.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

According to the Romanian Procedural Criminal Code, any aggrieved person may be a civil party against the defendant in a criminal action. Such aggrieved person may become a civil party during the criminal investigation proceedings, and also in front of the criminal court until the reading of the act of referral. The civil action in front of the criminal court is exempt from stamp duty.

The injured person who is not a civil party in a criminal action may separately submit a claim for damages in the civil courts in relation to material and moral prejudices caused through the criminal offence. Such separate civil actions for damages, irrespective of they are ongoing or are submitted in the course of criminal proceedings, are suspended until awarding a final resolution in the criminal action.

The aggrieved person who is a civil party in the criminal action is also entitled to start a separate action for damages in civil court if the criminal action was suspended. In case of resumption of criminal proceedings, the action before civil court is suspended. However, the aggrieved party who started a damage action in civil court may leave the civil court in favour of the criminal court, if the criminal proceedings were resumed after suspension. Leaving civil court can not take place if the court already awarded a decision which is not final and may be appealed.

The final decision of the criminal court is *res judicata* in civil court judging civil action regarding the existence of the offense, the person who committed it and the type of criminal fault.

The final decision of the civil court which was settled civil action has not *res judicata* in criminal action regarding the existence of the offense, the person who committed it and the type of criminal fault.

Slovak Republic

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Yes, there is a criminal liability for trade secrets violation in the Slovak jurisdiction.

The Slovak Penal Code (Act. No. 300/2005 Coll.) contains provisions directly dealing with endangering of trade secrets and disclosing of trade secrets (Art. 264).
Article 264 of the Penal Code is titled "Jeopardizing of trade secrets, bank secrets, post secrets, telecommunication secrets and tax secrets". According to this article who spies the trade secrets, bank secrets, post secrets, telecommunication secrets or tax secrets with the intention to disclose it to an unauthorized person or who such secrets to an unauthorized person intentionally discloses, shall be punished by imprisonment for a term from six months to three years.

The perpetrator shall be punished by imprisonment for a term of three to eight years if he commits the crime defined in paragraph 1

a) and causes a greater damage,
b) due to specific motive for the act, or
c) by serious manner of the act.

The perpetrator shall be punished by imprisonment for a term of seven to twelve years if he commits the crime defined in paragraph 1

a) and causes a damage of large scale,
b) as a member of dangerous group, or
c) during the emergency situation.

Proper functioning of the market economy and economic competition are legal values protected under this provision.

As trade secrets are also protected by provisions prohibiting unfair competition, the criminal liability for unfair competition conducts applies:

According to the Article 250 of the Slovak Penal Code whoever misuses his participation in the economic competition in a way that

a) through unfair competition in the economic relation harms the goodwill of another competitor, or
b) through acting that is contrary to the act regulating protection of economic competition causes a significant damage to another competitor or endangers running of his enterprise,

shall be punished by imprisonment for a term of up to three years.

The perpetrator shall be punished by imprisonment for a term of two to six years if he commits the crime defined in paragraph 1

a) and causes the damage of large scale
b) and causes the bankruptcy of another competitor
c) due to specific motive for the act, or
d) by serious manner of the act

Proper functioning of economy and fulfilling of economic tasks of the state are legal values protected under this provision.

As far as we know, there is no Slovak literature specifically dealing with criminal liability for trade secrets violation. Various commentaries to the Penal Code provide only short explanations regarding this criminal offence.

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

Yes, relevant provisions of the Penal Code establish several requirements as to the purposes that the infringer has to pursue to be charged with violation of trade secrets.

First of all, in order to make infringer liable for committing any of these offences it is necessary to prove that the infringer acted intentionally. Negligence is not sufficient for criminal liability in case of these offences.

Further, Article 250 sets that a significant damage (i.e. more than EUR 26 600) has to be caused to another competitor or running of another competitor's enterprise has to be endangered. A higher penalty is applicable if the infringer by breaching of trade secrets caused the damage of large scale (i.e. more than EUR 133 000) or caused the bankruptcy of another competitor or if the infringer had a specific motive for the act or if the breach of a trade secrets was performed by serious manner.

According to the Art. 264 no specific purpose has to be pursued as to be liable for endangering or breach of trade secrets. A higher penalty is applicable if the infringer by breaching of trade secrets caused a greater damage (i.e. more than EUR 2 660) or if the infringer had a specific motive for the act or if the breach of a trade secrets was performed by serious manner. Yet higher penalty is applicable if the infringer by breaching of trade secrets caused a damage of large scale (i.e. more than EUR 133 000) or performed this acting as a member of dangerous group or performed this acting during the emergency situation.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

Violation of trade secrets can result both in civil lawsuit and criminal proceedings for following two offences - Jeopardizing of trade secrets, bank secrets, post secrets, telecommunication secrets and tax secrets and Misuse of participation in the economic competition.

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

In order to make infringer liable for abuse of trade secrets it is necessary to prove that the infringer acted intentionally. Negligence is not sufficient for criminal liability in this case. The relevant provisions stipulate further conditions that have to be fulfilled in order to make the infringer liable for that criminal offence (the amount of damage, etc.)

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

According to the Article 264 a sole endangering of a trade secret (dissemination or disclosure) constitutes a criminal liability. The first part of this article states that „who

spies the trade secrets, bank secrets, post secrets, telecommunication secrets or tax secrets with the intention to disclose it to an unauthorized person…".

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

There are no different types of trade secrets violations in the Slovak jurisdiction depending on personal qualities of the infringer or the type of items covered by trade secrets.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

The notion of trade secrets is defined in the Commercial Code. It is the only definition of trade secrets contained in the Slovak law. All other laws (for example Penal Code or Law on Economic Competition) just refer to the definition contained in the Commercial Code. There are no different definitions of trade secrets for different fields of law. IP laws do not contain provisions regarding trade secrets.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

The legal definition of trade secrets is contained in the Commercial Code. According to the relevant provision of the Commercial Code trade secrets consist of all business, manufacturing and technological facts related to the enterprise with actual, or at least potential, tangible or intangible value. Trade Secrets are not normally available in the appropriate industry and should not be disclosed without the entrepreneur's consent, providing the entrepreneur adequately ensures such non-disclosure.
Each item (document, know-how, idea) that meets the above requirements is considered to be a trade secret and is legally protected.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

Yes, trade secrets have to meet special requirements in order to avail themselves of the relevant legal protection. The conditions for protection of trade secret are:

- information of commercial, manufacturing or technical nature related with the plaintiff's enterprise that
- have actual or at least potential material or immaterial value,
- are not commonly available in the relevant business circles,
- should be maintained in secrecy on basis of the trader's decision, and
- the trader ensures their secrecy adequately.

The patentability of the items covered by trade secrets does not impact on the extent of protection granted by law. If the item is already patented, it is protected by the provisions of the Penal Code dealing with patent infringement.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Yes the Slovak jurisdiction provides for criminal protection o f other IP registered rights. Article 281 of the Penal Code protects trademarks, designations of origin, geographical indications and business names. Article 282 of the Penal Code protects other IP rights – patents, utility models, designs, topographies of semiconductor products and accepted

plant variety or animal breed. The Article 283 protects authorship and author's rights (copyright).

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

Generally, the Public Prosecutor has the duty to initiate the criminal proceedings regarding any criminal offence he becomes aware, notwithstanding how he becomes aware of the offence. As a matter of fact, the Public Prosecutor usually does not initiate criminal proceedings without the impulse from the right holder or aggrieved party. The criminal proceedings regarding trade secrets violations are in a vast majority of cases initiated on the basis of the report of the offence filed by the holder of a trade secret. Anybody can file a report of the offence and thus initiate criminal proceedings. As regards the damages, only the aggrieved party is entitled to claim damages.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

Any evidence proving an abuse of trade secrets is applicable.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

Yes, in criminal proceedings the holder of trade secret can apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and filed containing such data. The holder can also ask for precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

In the Slovak jurisdiction the companies can not be liable for criminal offences.

2. If so, which type of liability arises for companies? Which penalties shall apply?

In the Slovak Republic companies can be sued only in civil proceedings for a breach of trade secrets. Breach of trade secrets is a special provision under falling under the provisions of unfair competition.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

A civil district court may adjudicate cases of liability of companies for trade secrets violations.

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

No specific obligation to keep secret the information has to be expressed for a trade secret violation to occur. Trade secrets are protected directly by the law. In case anyone violates trade secrets he becomes liable for this violation.

There are no distinctions between employees of the company owning the secret and any other persons other than employees.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

No, the offender does not have to be a competitor or potential competitor of the owner of the disclosed trade secret.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

Yes, an aggrieved person may bring a claim for damages in the course of a criminal proceeding. In cases where assessment and evidencing of damage requires deeper investigation, the court usually refers the aggrieved person to civil proceedings to bring a claim for damage. In case the civil lawsuit for compensation is already ongoing, the judge handling criminal proceedings will most probably suspend such claim in criminal proceedings will refer the aggrieved person to civil proceedings to claim damage/compensation.

Slovenia

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Yes. Article 236 of the Penal Code of the Republic of Slovenia (Official Gazette of the Republic of Slovenia, no. 66/2008, as amended, hereinafter referred to as "Penal Code") establishes criminal liability for "*Disclosure of and unauthorized access to trade secrets*"). The Penal Code incriminates: disclosure of trade secrets; the act of providing access to trade secrets to any unauthorized person; collecting trade secrets with the purpose of delivering them to any unauthorized person; and illicit obtainment of trade secrets with the purpose of delivering them to any unauthorized person. The penalty for committing any of the aforementioned criminal acts is imprisonment for up to three (3) years.

The Penal Code also provides for a qualified version of this act, i.e. if the information concerned is "of particular importance"; if the infringer hands over such information for the purpose of them being taken abroad; or if the criminal act is committed with the purpose of making profit, the infringer may be sentenced to imprisonment for up to five (5) years.

If the criminal act is committed out of negligence, the penalty for the infringer is imprisonment for up to one (1) year.

Article 236 protects business coherence and intellectual property. It secures the rights of every business/company to protect their knowledge and other information which gives them a competitive advantage on the market.

Literature on the subject:

Books:

- Deisinger Mitja: "Kazenski zakonik s komentarjem" ("*Penal Code with commentary"*), Posebni del, Gospodarski vestnik, Založba, Ljubljana 2002;

Articles:

- Deisinger Mitja: "Kazenskopravno varstvo gospodarstva v tranziciji in tržnem sistemu" ("*Criminal law protection of the economy in transition and market system"*) , Podjetje in delo, Issue 5-6/1996;

- Deisinger Mitja: "Gospodarska kazniva dejanja" ("*Economy-related criminal acts"*), Podjetje in delo, Issue 5-6/1993;

- Jakulin Vid: "Trgovanje na podlagi zaupnih notranjih informacij" ("*Insider Trading"*), Dnevi javnega prava. Uprava in sodstvo v evropskih povezavah in reforma javne uprave v Sloveniji, Inštitut za javno upravo, pp. 281-290, Ljubljana 1998.

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

No. The violation of the relevant provisions is established if the conditions mentioned therein are fulfilled (please see the point 1, paragraph 1 above) and the existence of the violation does not depend on any specific purpose pursued by the infringer (in other words, the infringer is not required to act with *dolus coloratus*, a specific intent). However, if the infringer pursues a certain purpose by his actions (profit-making, or providing the information with the intention for them to be taken abroad), this can result in a qualified version of this criminal offence, for which a higher prison penalty is prescribed (up to 5 years instead of 3). The law itself provides for an exhaustive list of purposes which the infringer must pursue, and no other purposes besides the ones listed in the law can be taken into account.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

The violation of trade secrets may result in a civil lawsuit, as well as criminal proceedings. The only criminal offence in the Penal Code which involves trade secrets is the abovementioned Article 236. However, it is possible that the infringer commits several offences with one and the same act. In that event, other criminal proceedings can also be brought against the infringer – for example, the same act may represent disclosure of trade secrets to an unauthorized person and the abuse of insider information (Article 238 of the Penal Code).

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

No, the Penal Code does not provide for any such safe harbor clauses or specific conditions under which the infringer may not be prosecuted. However, the prosecutors have a certain measure of discretion in determining which violations to prosecute (principle of opportunity) and are legally not required to prosecute all violations.

We note that in order to find the infringer guilty, the court must establish that the information in question was in fact a trade secret. If the accused proves that he did not know and could not have reasonably known that the information concerned was a trade secret (or that he was not authorized to collect or disclose this information), the infringer cannot be found liable for the crime.

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

According to the Penal Code, not only disclosure of trade secrets, but also the act of collecting information considered to be trade secrets "with the intention" of disclosing them to an unauthorized person, gives rise to criminal liability. In this respect, the answer to this question is in the affirmative, since already the action which causes the mere risk of disclosure is incriminated. Please note that the infringer can only be found liable if proven that he was acting with intent or negligence – if (as explained in the answer to the preceding question) the infringer succeeds in proving that he was not aware and could not have been aware of the fact that the information is a trade secret and/or that he is not authorized to collect or disclose the information, he cannot be found liable.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

The Slovenian jurisdiction only recognizes the general type of violation of trade secrets, as described in the answer to question no. 1, and does not discern between different types of trade secrets or the personal qualities of the infringer. The Companies Act (Off. gaz. of the RS, no. 65/2009, as amended, hereinafter referred to as "Companies Act") provides in Article 39 that:

- a trade secret is any information which the company defines as a trade secret by a written decision (in addition to specific information which are defined as trade secrets by the law).
- regardless of the (non)existence of any written decision of the company, any information for which it is reasonable to anticipate that substantial damage would be caused to the company if the information would be disclosed to an unauthorized person, is considered a trade secret.

The Slovenian legislation therefore provides for two different types of trade secrets: information which is defined as trade secret by the company (subjective criteria) and information which is so important that it is considered trade secret as such (objective criteria). However, the law does not make any differences between different information considered to be trade secrets and incriminates their (unauthorized) collection and disclosure in general.

Please note that in the ensuing text, wherever we refer to "trade secrets" in general, we are referring to both types of trade secrets described above.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

Intellectual property law in Slovenian jurisdiction does not specifically cover or mention trade secrets. Trade secrets are very broadly defined. As mentioned before, any information which is not public can be defined as a trade secret by a written decision issued by the company. Intellectual property law only provides protection for certain types of information: copyright, trademark, patent, innovation, geographical indication, design. Violation of intellectual property rights is also criminalized in Slovenia.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

No. As long as certain information fulfils any of the two (subjective or objective) conditions set forth in the Companies Act (Article 39), the information is granted protection. It is important to note that the Companies Act also provides (Article 39/3) that any information which is public (or must be made public according to the law), or any information about the wrongdoing or malpractice of the company, cannot be defined and considered as a trade secret.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

In principle trade secrets are not required to meet any specific requirements in order to avail themselves of the relevant legal protection, provided that they are defined as trade secrets according to the rules set forth in the Companies Act or meet the objective

criteria. In the decision-making practice of certain governmental bodies trade secrets have to confer a commercial advantage on the company in order to be protected under specific laws.

Yes, if a certain item can be patented or registered as a trademark, design, innovation, etc., it is also protected by the Industrial Property Act (Off. gaz. of the RS, no. 51/2006) and the Protection of Competition Act (Off. gaz. of the RS, no. 18/1993). However, the Penal Code provides for criminal liability with regard to unjustified use of another's patents, trademarks, etc. (Article 233) in a different provision than criminal liability for the disclosure of trade secrets. In this way, the Penal Code makes a difference between information which are considered as trade secrets on one hand, and information/items which are patented, or registered as a trademark or design, on the other. The act of disclosing trade secrets can only result in criminal liability (civil lawsuit is also possible), whereas the act of unjustified use of patent/trademark/etc. can result in criminal liability according to the Penal Code, as well as a monetary fine according to the Industrial Property Act and Protection of Competition Act, in addition to the possibility of a civil lawsuit.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Yes. Article 233 of the Penal Code provides: *whoever unjustifiably uses a brand, trademark, geographical indication, patent or other specific indication of goods or services, of which he is not the rightful owner; or uses an essential part of this mark as pa part of his own trade name, trademark or other sign by which the products are labeled; shall be imprisoned for up to 3 year*s.

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

The Penal Code and the Criminal Procedure Act (Off. gaz. of the RS, no. 32,/2007, as amended, hereinafter referred to as "Criminal Procedure Act") provide that the crime in Article 236 of the Penal Code is prosecuted by the public prosecutor. The proceedings begin *ex officio*. Any holder of a secret or other person may freely report a violation to the police or the public prosecutor's office. The proceedings are commenced and managed by the public prosecutor and the holder of a trade secret (harmed party) cannot itself commence criminal proceedings against the infringer.

However, if the public prosecutor decides not to commence criminal proceedings and bring charges against the infringer, the harmed party who reported the act may assume the role of prosecution as a subsidiary prosecutor and commence criminal proceedings against the infringer. During the course of criminal proceedings the public prosecutor may at any time replace the subsidiary prosecutor and itself take over the prosecution of the criminal act.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

No, there are no requirements for any specific evidence to be brought before a court. The holder must of course prove that the information was a trade secret (if it is not defined as such by the law). To this aim, he must provide a written decision taken by the company in which certain information is defined as trade secret and prove that anyone who handled this information was notified of this decision.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

A search of the private premises of the defendant is available in criminal proceedings according to the Penal Code and the Criminal Procedure Act. The decision is issued by the prosecutor and the search is executed by the police. The defendant cannot be forced to provide the whereabouts of documents and files containing trade secrets.

The Criminal Procedure Act provides for several measures which are intended to prevent the defendant to continue or resume with the acts which are suspected to infringe the law. Such measures are detention of the defendant, house arrest, precautionary seizure of objects (computer systems, documents,...), etc. However, all these measures are imposed by order of the public prosecutor. The holder may make a suggestion when filing the report or criminal charges to the prosecutor to impose these measures, but the decision is up to the public prosecutor.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Yes, the Liability of Legal Persons for Criminal Offences Act (Off. gaz. of the RS, no. 98/2004, as amended) provides for liability of legal persons for the violation of Article 236 of the Penal Code.

2. If so, which type of liability arises for companies? Which penalties shall apply?

Criminal liability, as well as civil liability arises for companies in case of disclosure and unauthorized access to trade secrets.

The possible penalties for companies are:

1.) monetary fine;
2.) seizure of assets (expropriation);
3.) liquidation of the company;
4.) prohibition of participation in tenders for public procurements;
5.) prohibition of trading in financial instruments.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

In the first instance, the Local court decides in cases of liability of companies. If the case includes the qualified version of the violation (Penal Code, Article 236/3, see above), the competent court is the District court. The law does not provide for any differences in competence of courts regarding whether the infringer is a natural person or a legal person.
In the second instance, the competent court is the High Court.

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

The answer to this question depends on what type of information we are talking about. The Companies Act (Off. gaz. of the RS, no. 65/2009, as amended, hereinafter referred to as "Companies Act") provides in Article 39 that a trade secret is:

> a.) any information which the company defines as a trade secret by a written decision (in addition to specific information which are defined as trade secrets by the law) and;
>
> b.) regardless of the (non)existence of any written decision of the company, any information for which it is reasonable to anticipate that substantial damage would be caused to the company if the information would be disclosed to an unauthorized person, is considered a trade secret.

With respect to information under a.), the offender must be aware that such a decision was made by the owner of information (he must have been notified in order for a violation to occur). The plaintiff must prove that the offender was made aware that the information was considered a trade secret and that a written decision was made by the owner to that effect – without this, there can be no liability. Thus, the obligation to keep the information secret arises when the person is informed of the decision made by the owner.

With respect to information under b.), the obligation to keep the information secret arises *ipso facto* when the person receives the information (is made aware of certain information). No special decision in this respect is required from the owner of such trade secrets. Of course, a dispute arises before the court regarding the disclosure of such information, the court will first have to decide whether the information in question was of such a nature to be classified under point b.) of Article 39 of the Companies Act.

With respect to the above said, the law does not differ between employees of the company owning the secrets and any other person who is made aware of such secrets. For a trade secret violation to occur, the offender must be either notified beforehand that certain information is considered as a trade secret; or the information in question must be of such a nature as described under point b.) of Article 39 of the Companies Act.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

No, there is no such requirement in order for a trade secret violation to occur.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

The aggrieved person may bring a claim for damages in the course of criminal proceedings, but not within the frame of criminal proceedings. Criminal proceedings are meant solely for the purpose of determining the offender's criminal liability. Claims for damages can be brought against the offender only in the context of civil proceedings (a civil lawsuit), but the two procedures can be pursued simultaneously.

Spain

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Regarding the general nature of the criminal liability for trade secrets violation, we have to state that articles 278 to 280 of the Spanish Criminal Code (SCC) punishes some conducts that harms the competitiveness of a company because of the discovery of some of the trade secrets from its activity.

Those offences are not considered offences against Industrial Property. The reason for it is that the SCC differentiates between trade secrets and IP based on the nature of the rights the owner claims. In the case of the IP rights, those arise from registering an invention in order to make it public and avoid that anybody else can reproduce it (with certain limitations).

On the other side, the protection given to the trade secret arises from the secret nature of the item and the will of the owner of keeping it secret because of the economic/competitive benefit he obtains hiding such information from its competitors.

In case of the trade secrets related offences, the legal value protected is the fair competition between the companies in the same economic branch. It is fundamental for the development of the economy of any country that every company is able to use its resources (i) to improve the technical part of their business by developing their products in order to make them more competitive and (ii) to improve the economic part of its own business by means of applying some techniques in order to turn it more economically and financially competitive.

The referred offences are as follows:

(I) Article 278.1 SCC states that *"whoever obtains data, written or electronic documents, computer media or other objects related thereto in order to discover a company secret, or who uses any of the means or instruments described in Section 1 of Article 197*[1]*, shall be punished with a sentence of imprisonment of two to four years and a fine of twelve to twenty four months"*.

It is important to highlight that, according to the Judgment 864/2008 issued on 16 December 2008 by the Criminal Section of the Spanish Supreme Court, the offence is compound by four elements:

- The action of the offence is to discover a trade secret obtaining any items like data, written or electronic documents, computer media, etc.
- The goal of the action carried out is to find out a trade secret, concept which has been developed by the Spanish Supreme Court (see Section A.8.).
- The data obtained should be considered a trade secret. It is stated that it is something wider than the technical secret, including also those data related to the organization of the company and its commercial/economic information (see also Section A.8.).

[1] To seize papers, letters, electronic mail messages or any other documents or personal belongings, or intercepts his telecommunications or uses technical devices for listening, transmitting, recording or to play sound or images, or any other communication signal.

- It can be committed by any person. The only requirement is that the author should not be aware of the trade secret and tries to find it out.
  Consequently, if any person commits the action but it was not his/her intention to find out a trade secret, he/she will not be committing an offence under article 278.1 SCC.
- Finally, we should stress that this offence is an "early completion offence", meaning that it is not necessary to discover the secret to prosecute the author. It is only necessary to obtain the item in order to find the trade secret out to consider that the offence has been committed.

(II) Under article 278.2 SCC we can find the aggravated form the above mentioned offence. According to it *"A sentence of imprisonment of three to five years and a fine of twelve to twenty-four months shall be imposed if the secrets discovered are disclosed, revealed or communicated to third parties"*.

Therefore, if the author of the offence punished under article 278.1 SCC reveals the trade secret discovered by obtaining the referred data, documents, media, etc. will commit a more serious offence and will be punished with a more serious penalty.

Also, it is important to highlight that under article 278.3 SCC it is stated that *"the terms set forth in this Article shall be construed to be without prejudice to the penalties that might be relevant for appropriating or destroying the computer media"*.

Consequently, if a person appropriates some devices in order to find out a trade secret, he/she will be prosecuted because of the commission of an offence regulated under article 278.1 or 278.2 SCC but also because of the commission of an offence of theft or misappropriation, for example.

(III) Under article 279 SCC it is punished the disclosure of a trade secret by anybody who has the obligation to keep it secret. *"Diffusion, disclosure or communication of a company secret perpetrated by whoever has the legal or contractual obligation of confidentiality, shall be punished with a sentence of imprisonment of two or four years and a fine of twelve to twenty four months"*.

According to the Judgment 864/2008 issued on 16 December 2008 by the Criminal Section of the Spanish Supreme Court, the elements that compound this offence are:

- The action of the offence is to spread or disclose the trade secret.
- The object of the offence is a trade secret (see Section A.8).
  We have to specify that if the author discloses a secret regarding an unlawful activity by the owner of the secret, it will not be considered as a trade secret and, therefore, he/she will not be committing any offence.
- The author must by a person who has a legal or contractual obligation of keeping unrevealed the trade secret. Consequently, it is a special offence, meaning that cannot be committed by any person (if a person who does not fulfil this requirement commits the offence, he will be considered an extraneous and will be considered as a participant in it, but not the author).
- Finally, it is required that the person who infringes his/her obligation and discloses the company secret does it with an entrepreneurial or commercial objective. That is, the trade secret must be disclosed in order to obtain an economic benefit from an entrepreneurial or commercial standpoint.

> If he discloses the trade secret only in his/her own benefit without the entrepreneurial objective, he will be sanctioned under the second section of article 279 SCC[2].

Regarding the legal or contractual obligation of keeping unrevealed the trade secret, it has been considered the most determinant element in order to consider the offence committed. Our case law has clearly stated that[3]:

> The simple generic obligation of keeping confidentiality about their job binding all the employees is not strong enough to consider committed the offence we refer to, despite it can trigger other liabilities, because legal protection of the market, competitiveness and consumers should not be developed by criminal law, *ultima ratio*. Instead, it should be directed by non criminal law […]
> Accordingly, the Provincial Court of Madrid of 28 April 1999 states that *"The author of the offence is, exclusively, the one who know the trade secret and has a legal or contractual obligation to keep it unrevealed. It is a special offence that requires the necessary existence of an institutional competence. That is, if the obligation of being confidential is express, the subject becomes obliged to guarantee the protection of the secret, but if that obligation is a generic one (the one related to good faith and diligence referred to in art. 5a) of the Statute of Workers), it will only trigger a breach of his generic legal duties, giving rise to a civil liability"*.

Therefore, according to the said judgement and the rest of the case law, the legal/contractual obligation of keeping the secret unrevealed must be an express obligation in which it is clearly stated the duties of the obliged to keep the secret unrevealed and being confidential.

If there is not such an express obligation, the offence will not be considered committed. Consequently, in order to prove the commission of the offence, it will not be enough to argue that the employee was bound by a generic obligation recognized under the Statute of Workers, the author must be bound by an express obligation.

(IV) Finally, under article 280 SCC it is sanctioned the disclosure of the trade secret regulated under articles 278.2 and 279 SCC when the author (i) did not participate in discovering the secret but (ii) he is aware of the unlawful origin of the discovery of the trade secret.

"Whoever, with knowledge of their unlawful origin, and without having taken part in their discovery, perpetrates any of the actions described in the preceding two Articles shall be punished with a sentence of imprisonment from one to three years and a fine of twelve to twenty four months".

It is important to highlight that according to article 109 SCC, *"perpetration of an act defined as a felony or misdemeanour by Law shall entail, pursuant to the provisions contained in the laws, to repair the damages and losses caused thereby"*. This is called civil liability arisen from an offence.

The said liability includes the restitution, repairing the damage and a compensation of material and moral damage.

The responsible for the civil liability arisen from an offence committed, according to article 116 SCC, will be the author/s of the offence. If more than one individual are

[2] If the secret is used for one's own benefit, the penalties imposed shall be half the lower penalty.
[3] Judgment 15/2007 issued on 21 January 2007 by the 3rd Section of the Audiencia Provincial de León

found criminally liable, the Judges will set the proportion of the civil liability for which each one must be held accountable.

Regarding principals and accessories, each within their own respective category, shall be held jointly and severally liable for their proportions and vicariously, for those of the other parties responsible.

Legal entities found criminally liable for the offence committed will also be considered civil liable jointly and severally with the individuals who are found guilty of the same acts.

Finally, article 120 SCC regulates who will be considered vicariously civil liable in case the direct civil liable does not pay:

> 1. The parents or guardians, for the damages and losses caused by the felonies or misdemeanours committed by those over eighteen years of age subject to their parental rights or guardianship and who cohabit with them, provided their is culpability or negligence on their part;
> 2. Natural or legal persons owning publishing houses, newspapers, magazines, radio stations or television channels, or any other means of written, spoken or visual diffusion, for felonies or misdemeanours committed using the media they own, notwithstanding what is set forth in Article 212 of this Code;
> 3. Natural or legal persons, in cases of felonies or misdemeanours committed in the establishments they own, when those that manage or administer them, or their assistants or employees have breached the police by-laws or provisions by the authority related to the punishable offence committed, so that would not have happened had that infringement not taken place;
> 4. Natural or legal persons dedicated to any kind of industry or commerce, for felonies or misdemeanours their employees or assistants, representatives or managers may have committed in the carrying out of their obligations or services;
> 5. Natural or legal persons owning vehicles liable to create risks to third parties, for the felonies or misdemeanours committed in use of these by their assistants, representatives or authorised persons.

Therefore, if an offence against trade secrets is committed, the author will face criminal liability and civil liability arisen from the offence committed in order to indemnify the victim of the offence for the damages suffered.

Finally, find below the list of the relevant literature on the matter:

- M. de M. Carrasco Andrino, *"Criminal protection over trade secrets"*, Cedecs Derecho Penal, Barcelona 1998.
- F. Muñoz Conde, "*Criminal Law-Special Part"*, Tirant Lo Blanc Libros, Valencia 2004.
- L. Rodríguez Ramos, *"Criminal Code. Comments and case law"*, La Ley, grupo Wolters kluwers, Madrid 2007.
- G. Quintero Olivares, *"Criminal Code's reform of 2010. Analysis and comments"*. Aranzadi-Thomson Reuters, Navarra 2010.
- A. Santaló Ríos, "The offences against intellectual property and industrial property after the Criminal Code's reform of L.O. 15/2003", Revista Xurídica Galega nº 43, available at https://www.rexurga.es/pdf/COL103.pdf

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

(I) According to what we have stated in Section A.1., we have to stress that the offence sanctioned under article 278 SCC can be committed by every person who was not aware of the trade secret, meaning that only those who do not know the trade secret and try to obtain it can commit this offence.

Therefore, there is a second requirement for this offence to be committed. The person who obtains the data, written or electronic documents, computer media, etc. should have the initial intention of discovering the trade secret. Consequently, if a person does not intend to discover the trade secret but he/she finds it out, he/she can not be prosecuted for the commission of this offence.

(II) The offence regulated under article 279 SCC can only be committed by those who (i) were aware of the trade secret and (ii) have the legal or contractual obligation of confidentiality. Therefore, this offence is a "special one", meaning that if an individual does not fulfil those two requirements, he/she can not commit the offence regulated under article 279 SCC.

As we have already stated (section A.1.) the author of this offence must act with an entrepreneurial or commercial objective. That is, the trade secret must be disclosed in order to obtain an economic benefit from an entrepreneurial or commercial standpoint.

If he/she discloses the trade secret only in his/her own benefit without the entrepreneurial objective, he will be sanctioned under the second paragraph of article 279 SCC

(III) Finally, the offence regulated under article 280 SCC can only be committed by those who fulfil two requirements. Firstly, the author should have not collaborated in order to discover the trade secret and, secondly, he/she should be aware of the unlawful origin of the trade secret discovered.

We have to highlight that the three offences abovementioned can only be committed maliciously, i.e. intentionally. Accordingly, it is impossible to commit it negligently.

The term *dolo* (willful misconduct) has various definitions under Spanish law. Under the SCC it is understood simply as the awareness of and intention to carry out a crime. From this definition, it follows that willful misconduct is made up of two components: one which is intellectual or cognitive and another which is volitive.

> A. From an intellectual standpoint, for the misconduct to be willful, the perpetrator must know what he is doing and be aware of the components characterizing his actions as criminal conduct. Nonetheless, that intellectual sphere of willful misconduct only refers to the objective components of the conduct: perpetrator, conduct, result, causal relationship between the conduct and the result.
> Such knowledge must be current; it cannot be merely potential. In other words, the perpetrator must know what he is doing and, accordingly, it is not sufficient to claim that he should or could have known.
>
> B. In addition to his knowledge, as explained above, it is necessary for the perpetrator to intend to carry out each and every one of the objective components of the criminal conduct referred to above. This volitive aspect of willful misconduct

entails the unconditional intention of the perpetrator to carry out the criminal conduct he thinks he can get away with.

Such an intention also entails the foregoing knowledge/awareness; since no one can intend to do something he does not know or is unaware of.

Accordingly, willful misconduct means conscious aggression against a protected legal asset (as described by Spanish case law, the perpetrator knows what he is doing and wishes to do what he knows), whereas negligence, which has no place in the offences we are analyzing, is merely a lack of care in which, at times, the perpetrator has not even considered the potential damage to the legal asset.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

Regarding other criminal offences that can arise from the violation of trade secrets, we have to state that there are not any more offences arisen from the violation to trade secrets than the three specified in Section A.1. above to which we refer.

Nevertheless, as we have previously stated in Section A.1., under article 278.3 SCC it is stated that *"the terms set forth in this Article shall be construed to be without prejudice to the penalties that might be relevant for appropriating or destroying the computer media"*.

Consequently, if a person appropriates some devices in order to find out a trade secret, he/she will be prosecuted because of the commission of an offence regulated under article 278.1 SCC but also because of the commission of an offence of theft or misappropriation if he/she fulfils the legal requirements to do so.

Regarding civil liability arisen from the offences related to violation of trade secrets, we also refer to Section A.1. above where it has been explained how it is regulated the civil liability in criminal proceedings under the SCC.

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

Regarding the "safe harbor" clauses with respect to the abuse of trade secrets, we have to specify that there is not any such clause contained under the SCC in relation to Trade Secrets.

There are no specific conditions under which the offender may not be prosecuted. The only way of not prosecuting the offender will be if one of the different elements of the offence has not been fulfilled.

That will occur when, for example, the secret trade cannot be considered as such because the information is public.

Therefore, if any individual carries out the actions contained in article 278 SCC but he manages to prove that his intention was not to obtain any trade secret to disclose it, he will be prosecuted by the commission of a different offence (theft, misappropriation, etc.) but he will not be prosecuted by the commission of an offence against trade secrets because he has not fulfilled all the offence elements.

It will be the same situation if one individual who has access to a trade secret and a legal/contractual obligation of keeping it confidential (like it is stated under article 279

SCC) but he recklessly breaches that obligation, he will not be prosecuted because he has not committed any offence. He will face some other liability, but not criminal.

Nevertheless, regarding the offence regulated under article 279 SCC, we have already specified that if the author discloses a secret regarding an unlawful activity by the owner of the secret, it will not be considered as a trade secret and, therefore, he/she will not be committing any offence.

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

According to what we have stated in Section A.1., the answer to the question if the risk of disclosure will give rise to criminal liability will depend on what offence is committed by the author.

(I) If the offence committed is the one regulated under article 278.1 SCC, prosecuting those who do not know a trade secret and try to disclose it by means of obtaining data, written or electronic documents, computer media or other objects, the offence will be committed every time that the author obtains the data, written or electronic documents, etc., even though if he does not disclose the secret.

If he discloses the secret and reveals it, he will be committing the aggravated offence regulated under article 278.2 SCC.

Therefore, if (i) the author was not aware of the trade secret and (ii) obtains all the data, documents, media, etc. in order to disclose it, it will be enough with the sole risk of dissemination or disclosure to give rise to criminal liability.

(II) Nevertheless, if the offence committed is the one regulated under article 279 SCC or the one regulated under article 280 SCC, the disclosure of the trade secret is necessary in order to trigger criminal liability.

In the case of the article 279 SCC, it will be necessary that the person who was aware of the trade secret (i) was bound by a legal or contractual obligation of keeping unrevealed the trade secret and (ii) he/she breaches that legal/contractual obligation revealing or disclosing it.

As we have mentioned in Section A.2., depending on the motivation to disclose it, the penalty will be more or less severe, but in any case, it is necessary to disclose the trade secret to trigger the criminal liability.

In the case of the article 280 SCC, to trigger the criminal liability, it will be necessary that (i) the author did not participate in the obtaining of the trade secret, (ii) he/ she was aware of its unlawful origin and (iii) he/she discloses or reveals it.

Therefore, in this case it is also necessary to disclose or reveal the trade secret in order to give rise to criminal liability.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

According to Section A.1. above, the Spanish Criminal Code recognizes there are three types of violation of trade secrets depending on the knowledge of the trade secret that the author may have.

(I) The one punished under article 278 SCC, in which the author does not know the content of the trade secret and tries to discover it.

(II) The one punished under article 279 SCC, in which the author has the trade secret because of his position and is bound a legal or contractual obligation of confidentiality but he breaches it and discloses the trade secret.

(III) The last one is the offence punished under article 280 SCC, in which the author does not know the content of the trade secret, he does not try to discover it but once he is aware of its existence, he disclosures it.

The main differences between the three offences are the penalties that the author of the offence committed may face:

(I) If the offence committed is the one sanctioned under article 278.1 SCC, the penalty imposed would be imprisonment ranging from 2 to 4 years and a fine ranging from 12 to 24 months.

(II) If the trade secret is disclosed according to article 278.2 SCC, the penalty imposed would be imprisonment ranging from 3 to 5 years and a fine ranging from 12 to 24 months.

(III) In case the offence committed is the one regulated under article 279 SCC, the penalty imposed would be the same than in the case of the article 278.1 SCC, that is, the penalty imposed would be imprisonment ranging from 2 to 4 years and a fine ranging from 12 to 24 months[4].

Finally, if the offence committed is the one sanctioned under article 280 SCC, the penalty imposed would be lower than in the case of the other two offences and it would be imprisonment ranging from 1 to 3 years and a fine ranging from 12 to 24 months.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

As explained in the Questionnaire regarding Commercial and IP Law, the Spanish Intellectual Property Law does not regulated nor defined the trade secrets.

According to the criminal case law, the trade secrets will need to meet some specific requirements. The most important cases analyzing this issue are as follows:

(I) Judgment 285/2008 issued on 12 May 2008 by the First Section of the Criminal Chamber of the Spanish Supreme Court:

> The key element of this offence –as well as the one of the offence contained under article 278 SCC- is the concept of trade secret. It is not defined under the Spanish Criminal Code, probably because it is a dynamic concept, a concept that cannot be limited by a *numerus clausus*. Therefore, we should look for a functional-useful conception, considering trade secrets as those typical of each business, that if were known against a company will, it will harm to its competitiveness.
>
> Its main characteristics are:
>
> - Confidentiality (the owner wants to keep secret)

[4] If the offence committed is the one regulated under on the second paragraph of article 279 SCC, the penalties will be reduced one grade.

- Exclusivity (it is a secret of only one company or business)
- Economic value (profitability)
- Lawfulness (the activity developed by the owner of the trade secret must be legal to be protected)

The grounds for its protection arises from the loyalty that must be kept by those who known the trade secret because of their legal or contractual relationship with the company, because the legal value protected under these offences will be the fair competition between the companies in the same economic branch.

Its content is normally compound by technical secrets (the products developed by the company); commercial secrets (the company's clients, marketing) and organizational secrets (labour issues, company's plans).

It can be collected in any kind of medium, paper or electronic, original or copies, even by an oral conversation. It can include figures, lists, accountability, organization charts, plans, internal memorandums, etc.

(II) According to the Judgment 180/2008 issued on12 March 2008 by the 2nd Section of the Audiencia Provincial de Barcelona *"The concept of trade secret is compound of three elements: a) its secret nature, b) the will of the owner of the secret to keep it confidential and c) the interest on keeping it secret"*.

Those three elements are defined in the said Judgment as:

- The secret nature establishes that the object of the offences can only be those data that the competitors do not know and that are very difficult to find out.
- The second element consists of the will of the owner of the secret to keep it confidential. It is enough if this intention can be recognized by the others, it is not necessary to make it expressly.
- Finally, is also necessary that the secret has an objective economic interest that justifies keeping it confidential.

(III) Nevertheless, we have to point out that, according to our case law –Judgment 970/2007 issued on 26 September 2007 by the 17th Section of the Audiencia Provincial of Madrid– regarding the concept of trade secret, *"finally, it cannot be considered as trade secret the professional abilities, capabilities and experiences owned by an employee or the know how and relationships he has with the clients, even if he has acquired those capabilities as a result of his position and work developed for a concrete employer"*.

Consequently, if the claimed secret is part of those professional abilities, capabilities and experiences owned by the employee, it will not have the consideration of trade secret.

Therefore, we can state that the concept of trade secret used by our criminal courts can be considered as every business secret that in case of revealing it will harm the competitiveness of the company if the said secret fulfils the four said requirements: confidentiality, exclusivity, economic value and lawfulness. It includes (i) technical secrets, (ii) commercial secrets and (iii) organizational secrets. It will not cover the know-how obtained by an employee during the job developed for the employer.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

As we have mentioned in Section A.8. above, SCC does not define any concept of trade secret but Spanish Criminal Courts use the concept defined by our Supreme Court.

At that point, we can state that there are no limitations as to the items covered by legal protection of trade secrets.

The limitations we can find in order to consider if an item can be considered as trade secret or not will come from the information they contain but not from the kind of item in which it is collected.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

According to Section A.8. above, SCC does not contain any definition of trade secret. Consequently, we have to use the concept of trade secret contained in our case law.

Therefore, there are four characteristics that any information must have to consider it as a trade secret:

- Confidentiality (the owner wants to keep secret)
- Exclusivity (it is a secret of only one company or business)
- Economic value (profitability)
- Lawfulness (the activity developed by the owner of the trade secret must be legal to be protected)

If the owner of the claimed trade secret can prove that the information object of the alleged offence fulfils the four requirements, then the information will be considered as a trade secret.

Regarding the patentability of the items covered by trade secrets, we have to stress that it does not impact on the extent of the protection. It will only have relevance if the item has finally been patented. In that case, it will not receive any protection as a trade secret and it would receive it as an IP Right.

If an item is patentable and it also fulfils the four requirements our Supreme Court has defined, it will receive the legal protection provided by our criminal code for trade secrets.

Regarding the protection of other IP registered rights, please look Section A.11 below.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Regarding the criminal protection provided by our jurisdiction of other IP registered rights, we have to state that under the Second Section of the Chapter XI, Title XIII Book II SCC are regulated all the offences regarding the Industrial Property registered rights.

According to Francisco Muñoz Conde[5], *"the concept of Industrial Property to which these offences refer is that part of the corporate economic activity that relates to both the creation or invention of technical and industrial objects and its exploitation, but also certain signs or trademarks used by some companies in order to distinguish their products from similar ones offered on the market. Ultimately, what the law protects in*

[5] F. Muñoz Conde, "*Criminal Law-Special Part"*, Tirant Lo Blanc Libros, pp.497, Valencia 2004.

this area is fair competition among entrepreneurs which has a private economic interest but also has a socio-economic content to the extent that also affects the rights of consumers".

Therefore, according to our case law –Judgment 84/2006 of 13th March of the 1st Section of the Audiencia Provincial of Guipúzcoa– *"The legal value protected is the exclusive right of exploitation of the IP rights for its owner. The privileges granted to the owner of an exclusive right, basically have a negative content, as it is the power to exclude other from performing certain acts relating to the invention covered by the patent (article 49 et seq LP)"*.

Consequently, the main difference between both the IP criminal protection and the trade secret criminal protection comes from the nature of the rights the owner claims. In the case of the IP rights, those arise from register an invention in order to make it public and avoid that anybody else can reproduce it (with certain limitations).

On the other side, the protection given to the trade secret arises from the secret nature of the item and the will of the owner of keeping it secret because of the economic/competitive benefit he obtains hiding such information from its competitors.

With regards to the offences affecting industrial property rights:

(I) Under article 273 SCC it is stated that:

> 1. Whoever, for industrial or commercial purposes, without the consent of the holder of a patent or utility model and being aware of registration thereof, manufactures, imports, possesses, uses, offers or markets objects protected by those rights shall be punished with a sentence of imprisonment of six months to two years and a fine from twelve to twenty four months.
> 2. The same penalties shall be imposed upon whoever, likewise and for the purposes stated, uses or offers the use of a patented procedure, or possesses, offers, markets or uses a product directly obtained by the patented procedure.
> 3. Whoever perpetrates any of the acts described in Section 1 of this Article when equal circumstances concur with regard to objects protected in favour of a third party by an industrial, artistic or topographic model or design of a semiconductor product shall be punished with the same penalties.

Under Criminal Law, we define a patent as the right of the patentee of an invention; it refers to a product or manufacturing process for either a specific improvement or development of existing patents and a utility model as an invention which is less innovative, maybe something that improves the structure or constitution of something which has been previously invented[6].

The most important elements of this offence are:

- The action is to manufacture, import, possess, use, offer or market an object protected under such rights, patent or utility model.
- In any case, the express consent of the owner of the rights will exclude any criminal liability of the alleged author.
- The object must have been previously registered (protected).
- The author of the offence must be aware of the registration of the said object and with an entrepreneurial or commercial objective.

[6] F. Muñoz Conde, "*Criminal Law-Special Part"*, Tirant Lo Blanc Libros, pp.497, Valencia 2004.

We must stress that under article 273.3 it is sanctioned the offence related to industrial, artistic or topographic model or design of a semiconductor product.

The penalties imposed would be imprisonment ranging from 6 months to 2 years and a fine ranging from 12 to 24 months.

(II) Under article 274 SCC it is stated that:

> 1. Whoever, for industrial or commercial purposes, without the consent by the holder of a registered industrial property right pursuant to the trademarks legislation and being aware of registration thereof, reproduces, imitates, amends or in any other way usurps a distinctive sign that is identical or may be mistaken for the former, to distinguish the same or similar products, services, activities or establishments for which the industrial property right is registered, shall be punished with the penalties of six months to two years imprisonment and a fine of twelve to twenty- four months. The same punishment shall be incurred by those who import such products.
> 2. The same penalties shall be imposed upon whomever, knowingly possesses products or services with distinctive signs that, pursuant to Section 1 of this Article, amount to infringement of the exclusive rights of the holder thereof, even in the case of imported products, in order to commercialise or market these.
> However, in cases of retail distribution, in view of the characteristics of the offender and the low amount of the financial profit, as long as none of the circumstances of Article 276 concurs, the Judge may hand down the punishment of a fine from three to six months or community service of thirty one to sixty days. In the same cases, when the profit does not exceed four hundred Euros, the act shall be punished as a misdemeanour under Article 623.5.
> 3. Whoever, for agricultural or commercial purposes, without the consent of the owner of a new plant variety title and being aware of its registration, produces or reproduces, conditions with a view to production or reproduction, offers on sale, sells or otherwise commercialises, exports, imports or possesses, for any of the purposes mentioned, plant material for reproduction or propagation of a protected plant variety pursuant to the laws on protection of new plant varieties shall be punished with the same penalty.
> 4. Whoever perpetrates any of the acts described in the preceding Section using, plant material for reproduction or propagation that does not belong to the variety stated, under the denomination of a protected plant variety, shall be punished with the same penalty.

Regarding the most important elements of the offence, we must highlight that:

- The action is to reproduce, imitate, amend or in any other way usurp a distinctive sign that is identical or may be mistaken for the former, to distinguish the same or similar products, services, activities or establishments for which the industrial property right is registered.
- As well as in the offences regulated under article 273 SCC, the most important element in this offence is that the trademark or distinctive sign must have been registered before the offence has been committed.
- In any case, the express consent of the owner of the rights will exclude any criminal liability of the alleged author.
- The author of the offence must also be aware of the registration of the said object and with an entrepreneurial or commercial objective.

(III) Also, under articles 274.3, 274.4 and 275 SCC there are regulated the offences against new plants variations and the denominations of origin.

(IV) Article 276 SCC regulates those cases in which the penalties imposed would be more severe. Those cases are:

- When the profit obtained is of special economic importance.
- When the events are especially serious, in view of the value of the objects unlawfully produced or the special importance of the damage cause.
- When the offender belongs to an organization whose purpose is to perpetrate activities that infringe IP rights.
- When persons under eighteen years of age are used to commit those offences.

(V) Finally, under article 277 SCC it is regulated the offence of disclosing the invention protected under a "secret patent" rights. Secret patents are those which content has been made secret because the invention is related to national defence.

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

According to article 287 SCC, *"prosecution of the offences foreseen in Section 3 of this Chapter, except those foreseen in Articles 284 and 285, must necessarily be reported by the victim or by his legal representatives. When the victim is a minor, incapacitated or handicapped person, they may also be reported by the Public Prosecutor"*.

Therefore, a criminal procedure because of the commission of one of the offences against a trade secret, punished under articles 278, 279 and 280 SCC, will only start if the victim or his/her legal representative reports it to the authorities.

Nevertheless, taking into account that these offences are "semipublic", once the victim has filed his report for the commission of the said offences, the Public Prosecutor can then become a party to the proceedings and, if the victim forgives the author for the offence committed, the Public Prosecutor is entitled to keep the accusation against the author if he/she deems that an offence has been committed.

In any case, there is a legal exception to the abovementioned, contained in article 287.2 SCC. According to it *"The report required in the preceding section* (article 287.1) *shall not be necessary when the commission of the offence affects general interests or multiple persons"*.

Consequently, in order to initiate criminal proceedings against the author of one of the said offences, it will be necessary the report of the victim of the offence before the public prosecutor is able to become a party to the proceedings.

If the commission of the offence affects general interests or multiple persons, then the victim's report will not be necessary and the proceedings could be started after the report of the Public Prosecutor.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

Regarding the evidences that should be brought before a court in order to prove that an abuse of trade secrets has occurred, we have to stress that the first thing that should be proved is that the information/item can be considered as a trade secret under Criminal Law.

According to Section A.8. above, the main characteristics of a trade secret are its confidential nature, its exclusivity, its economic value or profitability and its lawfulness.

Therefore, the owner of the trade secret who considers that the secret has been abused and an offence has been committed must prove in his report that the object of the alleged offence was really a trade secret.

The most important evidences in order to prove it are (i) confidential agreements signed in order to keep the secret confidential and (ii) every kind of document that can prove its secret nature and its economic/competitive interest.

Once the owner of the trade secret has proved that the information was really a trade secret, depending on the claimed offence, he/she will have to prove:

1. If the alleged offence is the one regulated under article 278 SCC, the owner will have to prove (i) that the defendant was not aware of the trade secret and (ii) that he/she was trying to find it out.

   The owner of the trade secret will have to prove as well that the author has appropriated some data, devices and items of his property. Taking into account that the trade secret can be physically kept or by means of a computer device, it will be important to obtain the information of all the electronic devices available in order to prove it.

2. If the alleged offence is the one regulated under article 279 SCC, the owner will have to prove (i) that the one who committed the alleged offence was aware of the existence of the trade secret, (ii) that he was bound by a contractual obligation of keeping it confidential, (iii) that he has breach the obligation to keep confidential the trade secret disclosing it and (iv) that he has made it with an entrepreneurial objective and not for his own benefit (if he committed the offence for his own benefit, the offence will be the one regulated under article 279.2 SCC).

   The main documents to prove the commission of this offence will be the confidential agreement stating the secret nature of the item and the obligation of not disclosing it. In fact, according to what we have stated in Section A.1., case law tends to deny the commission of this offence if there is not a document proving the contractual obligation of not disclosing the trade secret.

3. Finally, if the alleged offence is the one regulated under article 280 SCC, the owner of the trade secret will have to prove that the author was aware of the unlawful obtaining of the trade secret he/she has disclose and (ii) that he has really disclosed it.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

First of all, we have to state that under article 334 of the Spanish Criminal Procedure Act it is regulated the concept of body of evidence. According to it, *"The Examining Magistrate will try to pick up in the very first moment the weapons, instruments or any*

kind of effects related to the offence that can be found in the scene where the offence was committed, around it, held by the defendant or other known place, issuing a Court order specifying the place, the time and occasion in which the item was found, describing it in order to state a global idea of the item and the circumstances in which it was found".

Therefore, if the body of evidence is a computer, documents, misappropriated data, etc. and the defendant is found committing the offence, the Examining Magistrate will be able to pick up the body of evidence in order to preserve the evidences of the commission of the offence to value them during the Trial Hearing.

Nevertheless, if the body of evidence cannot be found at first place or the Examining Magistrate did not pick it up to preserve it, the accusing party can request the Judge to found and preserve those items by different means.

According to article 776.3 of the Spanish Criminal Procedure Act, *"those who become a party to the proceedings are able to learn what has been done during the case file and request to carry out of those enquiries necessary to protect their rights, ordering the Judge to carry out them or not according to the Law"*.

Consequently, if you are a party to the proceedings, you are able to request as many enquiries as you consider necessary in order to protect your legal rights and it will be the Examining Magistrate who will decide if it is appropriate to carry out the requested enquiries.

However, it should be noted that according to article 118 of the Spanish Criminal Procedure Act and article 24 of the Spanish Constitution, the defendants of a criminal proceedings are protected by their defense rights and, accordingly, they are able to reject rendering a statement against themselves and admit their culpability.

Consequently, the defendant will be able to reject the requests made by the Examining Magistrate if those request would imply their culpability.

In any case, within the enquiries the parties are able to request, there are the precautionary measures, which, once agreed, can not by denied by the defendant (he can file an appeal against the order but if his appeals do not succeed, he will have to carry them out).

Precautionary measures can be ordered by the Judge per request of the accusing party in order to (i) allow the process to take place despite the actions of the defendant and (ii) ensure that the judgment will be enforced and fulfilled by the author of the offence.

There are two necessary elements that should be checked by the Judge in order to order the carry out of the precautionary measures requested by the parties. Those are (i) *fumus boni iuris*, meaning that it should appear from the investigation phase enough evidences that the offence was effectively committed by the defendant (it should be taken into account that precautionary measures are a limitation of the defendant's rights and, accordingly, it is necessary that some evidences of the commission of the offence appear during the investigation) and (ii) *periculum in mora* which means the risk of disappearance of the items related to the offence as well as the defendant or his/her assets, making impossible to pay the civil liability arisen from the offence.

In conclusion, we have three options under Spanish Criminal Procedure Act to obtain the precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof:

a) The order issued by the Examining Magistrate's Court agreeing to seizure the body of evidence in the crime scenario in order to preserve it until the Trial hearing takes place.
b) The request to the Examining Magistrate of carrying out some enquiries in order to ensure that the defendant will stop committing the offence and that the items obtained will not be destroyed.
c) The order of the Examining Magistrate agreeing to carry out any of the Precautionary Measures requested by the accusing parties.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

After the approval of the Organic Law 5/2010, dated 22 June 2010, amending Organic Law 10/1995, dated 23 November 1995, on the Criminal Code, legal entities – companies- can be found criminally liable in Spain.

This change has been introduced by new article 31 bis SCC, according to which:

> 1. In the cases included in this Code, legal entities will be criminally liable for offences committed in their name or on their behalf, and to their benefit, by their legal representatives and directors in fact or *de jure*.
> In these same cases, legal entities will also be criminally liable for offences committed in the exercise of corporate activities and on behalf and to the benefit of such persons, by those who, being subject to the authority of the individuals mentioned in the preceding paragraph, may have performed such acts in the absence of due control over them, after giving consideration to the specific circumstances in each case.
> 2. The criminal liability of legal entities will apply whenever there is evidence that an offence has been committed by someone who holds a position or performs the duties referred to in the preceding point, even in cases where the specific individual responsible for an act has not been individualised or it has not been possible to direct the proceeding against that person. When, as a consequence of an offence, the penalty of a fine is imposed upon both persons, the judges or courts will modulate the respective amounts in such a way as to ensure that the sum imposed will not be disproportionate in relation to the seriousness of the offences.
> 3. With respect to the persons who have materially performed the acts or those who have made such actions possible on account of their failure to exercise due control, the concurrence of circumstances affecting the culpability of the accused or aggravating their liability, or the fact that such persons are deceased or have eluded justice, will not exclude or modify the criminal liability of the legal entities involved, notwithstanding the provisions of section 4 below.
> 4. Solely the following actions, performed subsequently to the commission of an offence and through the legal representatives of the legal entities concerned, may be considered as circumstances attenuating their criminal liability:
>
> a) To have confessed the infringement to the authorities, prior to having learned that the judicial proceedings were directed against them.
> b) To have cooperated in the investigation of the act by providing evidence at any stage in the process that is new and decisive for clarifying the criminal liabilities emanating from the facts.
> c) To have proceeded to repair or to reduce the damage caused by the offence at any stage of the proceedings and prior to the trial.
> d) To have taken, prior to the commencement of the trial, effective measures in order to prevent and detect any offences that could possibly be committed in the future using the resources or under the coverage of the legal entity.

5. The provisions relating to the criminal liability of legal entities will not be applicable to the Central Government, territorial and institutional public administrations, regulatory bodies, public entrepreneurial agencies and entities, political parties and trade unions, international organisations governed by public law, or any others which exercise public powers of sovereignty or of administration or when Government-owned companies implementing public policies or providing services of general economic interest are involved.
In these cases, the jurisdictional bodies will be able to make a statement of criminal liability if they find that the case involves a legal form created by its promoters, founders, executives or representatives for the purpose of avoiding an eventual criminal liability.

Consequently, for cases of intellectual and industrial property offences, offences relating to the market and to consumers, as well as the offence of corruption between private parties (commercial bribery) under article 286 bis (all of which are included under Title XIII, Chapter XI, Book II SCC) legal entities may be declared criminally liable:

a) for offences committed, on its behalf or to its benefit, by its legal representatives, directors in fact and/or directors de jure and

b) for offences committed in the exercise of its activities, on its behalf and to its benefit, by those who, being subject to the authority of the aforementioned individuals, would have performed the criminal acts in the absence of due control over them.

This dual channel has thus been established in order to determine the liability of the legal entities which, as indicated above, arises from the actions of another in a vicarious and objective manner in the first instance described and through *culpa in vigilando* or negligence in the second instance.

Moreover, the foregoing does not mean in any way whatsoever that the criminal liability of the individual disappears, but rather that the liability of the legal entity is added to it, whereby the latter liability may be declared (i) even if the specific individual who is responsible has not been individualised (ii) or when the proceedings could not be brought against the individual (for example, due to the lapse of liability by death or by application of the statute of limitations). This signifies that the legal entity will not be affected by any circumstances that may modify the criminal liability of the individual – those known as attenuating and aggravating circumstances– because, as it will be explained later, the company will be affected by its own modifying circumstances.

Similarly, the *ex delicto* civil liability of legal entities is maintained in a direct, joint and several manner with the individuals (article 116. 3 SCC) and on a vicarious basis (article 120 SCC).

The penalties to be imposed upon legal entities are determined as follows in article 33. 7 SCC:

The penalties applicable to legal entities in serious cases are as follows:
a) A fine assessed in instalments or proportional fine.
b) Winding up of the legal entity. Winding up will bring about the definitive loss of its legal personality, as well as the loss of its capacity to act in any way in legal trade or to engage in any kind of activity, even when such activity is lawful.
c) Suspension of its activities for a period not to exceed five years.
d) Closing-down of its premises and establishments for a period not to exceed five years.

e) Prohibition of engaging in the same activities in the future as those, in which the offence was committed, aided or concealed. This prohibition may be temporary or definitive. If temporary, the period of prohibition may not exceed fifteen years.
f) Ineligibility for obtaining subsidies and public assistance, public sector contracts and tax or Social Security rebates and incentives for a period not to exceed fifteen years.
g) Judicial intervention in order to safeguard the rights of employees or creditors for as long as considered necessary, although such period may not exceed five years.
The intervention may affect the entire organisation or be restricted to one or more of its facilities, sections or business units. The Judge or Court, in the Judgment or, subsequently, by means of a writ, will determine the content of the intervention in detail and will determine who is to take charge of the intervention and at what intervals monitoring reports are to be made for submission to the judicial body. The intervention may be modified or suspended at any time, following a report by the controller and the Public Prosecutor. The controller will have the right to access all of the facilities and premises of the company or legal entity and to receive whatever information he may consider necessary for the exercise of his duties. Aspects relating to the exercise of the controller's duties, such as his remuneration or the qualification required, will be determined in the relevant regulation.

The temporary closing-down of premises or establishments, the suspension of the company's operations and the judicial intervention may also be decided by the Examining Magistrate as a precautionary measure during the preliminary investigation of the case.

Article 66 bis SCC requires that, in the application of these severe penalties –excluding the penalty of a fine– the Judge or Court must take into account a) the need for the penalty in order to prevent the continuation of the criminal activity or the effects thereof, b) the economic or social consequences, particularly for the employees and c) the position within the organisation of the individual who failed to exercise due control.

Finally, it should be noted that all of the foregoing is not applicable to Central Government, territorial and institutional public administrations, regulatory bodies, public entrepreneurial agencies and entities, political parties and trade unions, international organisations governed by public law, or any others which exercise public powers of sovereignty or of administration or Government-owned companies which implement public policies or provide services of general economic interest (article 31 bis. 5).

Article 31 bis SCC also regulates the circumstances which could limit this severe criminal liability affecting legal entities.

Firstly, we have to state that there is a sector of the doctrine that understands that article 31 bis SCC *in fine* makes it possible to state that a company which exercises due control over those of its members subject to the authority of legal representatives, directors in fact and/or directors *de jure* could eliminate any possibility of being considered criminally liable for their acts.

The question as to what due control is, how it is exercised or how *"the specific circumstances of the case"* are taken into account is something which is not defined in the SCC (unfortunately, taking into account that the SCC was modified on December 2010, case law has not yet addressed these issues). Nevertheless, there is a consensus as to what our legislators have intended to introduce into our criminal law system is, what in Anglo Saxon legal practice is known as *corporate compliance*.

If the legal entity is unable to eliminate its criminal liability, article 31 bis.4 SCC regulates the following as the sole attenuating circumstances affecting its criminal liability:

> a) To have confessed the infringement to the authorities, prior to having learned that the judicial proceedings were directed against them.
> b) To have cooperated in the investigation of the act by providing evidence at any stage in the process that is new and decisive for clarifying the criminal liabilities emanating from the facts.
> c) To have proceeded to repair or to reduce the damage caused by the offence at any stage of the proceedings and prior to the trial.
> d) To have taken, prior to the commencement of the trial, effective measures in order to prevent and detect any offences that could possibly be committed in the future using the resources or under the coverage of the legal entity.

In conclusion, we can state that regarding those offences related to trade secrets, legal entities may be found criminally liable:

> a) for offences committed, on its behalf or to its benefit, by its legal representatives, directors in fact and/or directors *de jure* and
>
> b) for offences committed in the exercise of its activities, on its behalf and to its benefit, by those who, being subject to the authority of the aforementioned individuals, would have performed the criminal acts in the absence of due control over them.

2. If so, which type of liability arises for companies? Which penalties shall apply?

If, according to article 31 bis SCC, a legal entity is found criminally liable of one of the offences regulated under articles 278, 279 and 280 SCC, the penalties to be imposed to the legal entities are regulated under article 288 SCC.

This article states that:

> When, pursuant to the terms established in Article 31 bis, a legal person is responsible for the offences defined in this chapter, it shall have the following penalties imposed thereon:
> 1. […]
>
> In the case of the offences foreseen in articles 277, 278, 279, 280, 281, 282, 282 bis, 284 and 286 bis:
> a) Fine from one to three years, if the offence committed by a natural person has a punishment foreseen of more than two years custodial sentence.
> b) Fine of six months to two years, in the rest of the cases.
> 2. According to the rules established in Article 66 bis, the Judges and Courts of Law may also impose the penalties established in Sub Sections b) to g) of Section 7 of Article 33.

According to Section 1 above, the penalties established in Sub Sections b) to g) of Section 7 of Article 33 are:

> b) Winding up of the legal entity.
> c) Suspension of its activities for a period not to exceed five years.
> d) Closing-down of its premises and establishments for a period not to exceed five years.

e) Prohibition of engaging in the same activities in the future as those, in which the offence was committed, aided or concealed. This prohibition may be temporary or definitive. If temporary, the period of prohibition may not exceed fifteen years.
f) Ineligibility for obtaining subsidies and public assistance, public sector contracts and tax or Social Security rebates and incentives for a period not to exceed fifteen years.
g) Judicial intervention in order to safeguard the rights of employees or creditors for as long as considered necessary, although such period may not exceed five years.

In any case, those penalties should follow the rules established in article 66 bis SCC, according to which, the Judge or Court must take into account a) the need for the penalty in order to prevent the continuation of the criminal activity or the effects thereof, b) the economic or social consequences, particularly for the employees, and c) the position within the organisation of the individual who failed to exercise due control in order to impose one of them and the duration of the penalty imposed.

Therefore, if according to article 31 bis SCC a legal entity is found criminally liable for the commission of an offence punished under articles 278, 279 or 280 SCC, the penalties imposed to the company (in addition to the penalties imposed to the individual) would be a fine, ranging from one to three years, and one or more of the penalties regulated under article 33.7 SCC depending on the offence committed, its consequences, whose failure in exercising due control originated the offence, etc.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

First of all, we have to specify that Spanish Criminal Procedures can be classified, amongst other criteria, according to their special or ordinary nature and ordinary and special proceedings are therefore different.

Ordinary procedures relating to criminal offences (*delitos*) can be of two types: (i) procedures for serious crimes which exclusively cover crimes punishable by terms of imprisonment exceeding nine years and (ii) abbreviated procedures for offences punishable by terms of imprisonment not exceeding nine years or by other penalties of a different nature, whether individually, combined or alternatively applied, whatever the amount or duration thereof.

In the case of the offences regulated under articles 278, 279 and 280 SCC, the applicable procedure is the abbreviated one, which is governed by Articles 757 *et seq* of the current version of the Spanish Criminal Procedure Act.

Therefore, the offences related to trade secrets, punished under articles 278, 279 and 280 SCC will be investigated and judged according to the abbreviated proceedings.

The investigation phase will be directed by the Examining Magistrate's Court of the place where the offence has been committed but there are two exceptions to this rule:

a) If the offence is committed abroad but, according to article 23 of the Spanish Judiciary Act, Spanish Criminal Courts are competent to judge those offences, then the offence will be investigated by one of the Central Examining Magistrate's Court.

b) If the place where the offence was committed cannot be identified, according to article 15 of the Spanish Criminal Procedure Act, it will be investigated by the Examining Magistrate's Court of (i) the place where the main evidences have been found, (ii) the place where the author has been arrested, (iii) the place of residence of the author or (iv) the Court of the place in which the offence was first noticed.

The Judging Court in this case, according to article 14. 3 of the Spanish Criminal Procedure Act will be the Criminal Court of the place where the offence was committed.

In any case, if we are under one of the abovementioned exceptions, the Court in charge of judging the offences related to trade secrets will be:

a) The Central Criminal Court, according to article 65 of the Spanish Judiciary Act.
b) The Criminal Court of the same place where the Examining Magistrate's Court carried out its investigation.

In conclusion, the offences related to trade secrets, punished under articles 278, 279 and 280 SCC will be investigated and judged according to the abbreviated proceedings. The investigation will be carried out by the Examining Magistrate's Court of the place where the offence was committed and it will be judged by the Criminal Court associated to that place (unless we are facing one of the said exceptions).

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

It is necessary to differentiate between two questions. Regarding the offences related to trade secret, according to the answers provided in the previous questionnaire, there are three different offences sanctioned under the Spanish Criminal Code (SCC) depending on the knowledge of the trade secret that the perpetrator may have.

a) The one punished under article 278 SCC, in which the author does not know the content of the trade secret and tries to discover it.

If the employee/perpetrator is not aware of the trade secret and he tries to discover it, he will be committing the offence sanctioned under article 278 SCC (there is not a confidentiality obligation in this case since the perpetrator did not own the trade secret and his actions are aimed to obtain it). If he discovers the trade secret and reveals it; he will be punished with a more severe penalty, although there is not such an obligation in this case either.

b) The one punished under article 279 SCC, in which the author is aware of the trade secret because of his position and is bound by a legal or contractual obligation of confidentiality but he breaches it and discloses the trade secret.

c) The last one is the offence punished under article 280 SCC, in which the author does not know the content of the trade secret, he does not try to discover it but once he is aware of its existence, he discloses it.

Therefore, if the information discovered is considered as trade secret (according to Spanish Case Law), the offence committed will be determined by the knowledge or unknowledge the employee/perpetrator has about the said information as a consequence of its work.

It is important to highlight that it is only regarding article 279 SCC where a specific confidential clause is required in order to commit the said offence.

Article 279 SCC states that the perpetrator of the offence has to be bound by a *legal or contractual obligation of confidentiality*. Nevertheless, our case law has defined the

concept, stating that [Judgment 15/2007 issued on 21 January 2007 by the 3rd Section of the Audiencia Provincial de León]:

The simple generic obligation of keeping confidentiality about their job binding to all employees is not strong enough to consider committed the offence we refer to, despite it can trigger other liabilities, because legal protection of the market, competitiveness and consumers should not be developed by criminal law, *ultima ratio*. Instead, it should be directed by non criminal law […]
Accordingly, AAP Madrid of 28 April 1999 states that *"The perpetrator of the offence is, exclusively, the one who know the trade secret and has a legal or contractual obligation to keep it unrevealed. It is a special offence that requires the necessary existence of an institutional competence. That is, if the obligation of being confidential is express, the subject becomes obliged to guarantee the protection of the secret, but if that obligation is a generic one (the one related to good faith and diligence referred to in art. 5a) of the Statute of Workers), it will only trigger a breach of his generic legal duties, giving rise to a civil liability"*.

Therefore, according to the said judgement and the rest of the case law, the legal/contractual obligation of keeping the secret unrevealed must be an express obligation in which there are clearly stated the duties of the obliged party to keep the trade secret unrevealed and being confidential.

According to the abovementioned, in order to commit an offence sanctioned under article 279 SCC, the perpetrator must be a person who knows the trade secret (an employee, usually) and is bound by an express contractual obligation to keep it confidential. Consequently, a specific obligation of keeping secret the information is required.

If the person is aware of the trade secret but he is not bound by such an express obligation but the generic one stated under article 5a) of the Statute of Workers, he will not be able to commit the offence sanctioned under article 279 SCC, so the breach of such an obligation disclosing the said secret will only may give rise to a civil liability.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

Regarding the qualification of the perpetrator as a competitor or a potential competitor of the owner of the disclosed trade secret, we have to specify our answer depending on which offence has been committed.

If the claimed offence is the one sanctioned under article 278 SCC, the offence will be committed when the perpetrator obtains any items like data, written or electronic documents, computer media, etc. in order to discover a trade secret.

As we stated in section A.1. of the previous questionnaire, it is only necessary to obtain the item in order to discover the trade secret, meaning that if the item is obtained by the perpetrator but he is unable to find out the trade secret or he is caught before discovering it, he will have also committed the offence. Consequently, the perpetrator may be a person with no relationship at all with the owner of the trade secret but who has been paid to discover it, for example[7].

Likewise, according to article 278.2 SCC, if the trade secret is discovered and disclosed, the penalty imposed would be more serious than if the perpetrator only obtained the item to discover the trade secret. In any case, it is not required that the perpetrator of this concrete offence must be a competitor of the owner of the trade secret.

[7] This will be the case also regarding the offence sanctioned under article 280 SCC.

Therefore, regarding the qualification of the perpetrator of this concrete offence, it is not necessary that he is a competitor or potential competitor of the owner.

If the claimed offence is the one sanctioned under article 279 SCC, it is clearly stated that the perpetrator of the offence (i) must be aware of the trade secret, (ii) must be bound by a contractual or legal obligation of keeping it unrevealed and (iii) must reveal or disclose the trade secret, breaching such obligation.

Therefore, if one of the persons who is aware of the trade secret is bound by such an obligation and breaches it, disclosing the trade secret with an entrepreneurial or commercial aim, he will be committing the offence.

According to the abovementioned, it is not necessary that the offender qualifies as a competitor or potential competitor of the owner of the secret.

Nevertheless, according to the second paragraph of the said article, if the perpetrator of the offence commits it only for his own benefit, the penalty to be imposed will be a lower one.

This means that if the perpetrator commits the offence in order to obtain a personal benefit instead of disclosing the trade secret for others to use it after paying him a sum of money, like earning money competing against the owner of the offence, his penalty will be lower than if he discloses it to a third party for them to use it.

According to this, we have two different scenarios:

- If the perpetrator discloses the trade secret to a third party for its illegal use, it will not be necessary that the offender previously qualifies as a competitor of the owner of the trade secret. It will only be necessary that he fulfils the three requirements previously stated.

- If the perpetrator uses the trade secret for his own benefit, with an economic/entrepreneurial purpose, he will be committing an offence but sanctioned with a lower penalty. In this case, it is possible that the perpetrator may have committed the offence to compete against the owner of the trade secret, but it has not been established as a requirement under SCC.

Consequently, it is not required under said articles that the perpetrator must qualify as a competitor of the owner of the trade secret to consider that the offence has been committed.

3. May the aggrieved person, in the course of a criminal proceedings, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

As we stated under section A.1. of the previous questionnaire, it is important to highlight that according to article 109 SCC, *"perpetration of an act defined as a felony or misdemeanour by Law shall entail, pursuant to the provisions contained in the laws, to repair the damages and losses caused thereby"*. This is called civil liability arisen from an offence.

The said liability includes the restitution of the damages caused, the reparation of such damage and a compensation of material and moral damages.

The civil liable from criminal offence, according to article 116 SCC, will be the perpetrator/s of the offence.

Article 120 SCC regulates who will be considered vicariously civil liable in case the direct civil liable does not pay.

Therefore, if an offence against trade secrets is committed, the perpetrator will face criminal and civil liability both arisen from the offence committed in order to indemnify the victim of the offence for the damages suffered.

Civil liability will usually be judged by a Criminal Court during a criminal proceeding. Therefore, if as a result of the criminal proceedings, it is stated by the Judge that the claimed offence has been committed, he will also determine the civil liability arisen from the said offence and who is liable to pay it.

Regarding the question whether it is possible to bring a claim for damages in the course of a criminal proceeding, we have to state that it is possible, according to the SCC and Civil Code, that the aggrieved person saves the option of filing a civil claim concerning civil liability separately to the criminal proceedings.

Nevertheless, this claim will not be investigated by the civil court until the Criminal Proceedings has finished.

The civil proceedings will be conditioned by the result of the criminal proceedings. Therefore, if the criminal case has finished with a condemnatory ruling, the civil judge will have to stick to the ruling regarding the facts, the perpetrator of the offence and the objective damages caused.

If the criminal case is dismissed, a new civil proceeding will be initiated in order to determine if there are damages to be compensated and the amount of damages caused.

It is important to state that the evidences used during a criminal proceedings and considered valid by a Criminal Court, will have probative effects during a civil proceedings.

According to the abovementioned, it is usual in our jurisdiction that civil liability arisen from the alleged commission of an offence is judged by a Criminal Court during a criminal proceedings, determining in its ruling the amount of damages caused and the civil liable who has to pay them.

Nevertheless, the aggrieved person has the possibility of saving the option of filing a civil claim regarding the civil liability separately to the criminal proceedings, but it will have to wait until the criminal proceedings is finished and it will be conditioned by the result of the criminal ruling.

Sweden

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Sweden has since 1990 provided a specific law regarding the protection of trade secrets, The Swedish Act (1990:409) on the Protection of Trade Secrets [*Sw*. Lag (1990:409) om skydd för företagshemligheter] (hereinafter the "Trade Secrets Act").

The Trade Secrets Act contains criminal regulations on trade espionage and unauthorized dealing with trade secrets as well as civil regulations on liability for damages for criminal and non-criminal acts involving unlawful use and disclosure of trade secrets. The civil regulations are further described in the Commercial and IP Law Questionnaire - B. In addition to the Trade Secrets Act there are also criminal provisions in the Swedish Penal Code that can be applicable to trade secrets violations.

Section 3 in the Trade Secrets Act regulates criminal liability for *trade espionage*. Anyone who wilfully and without authorization accesses a trade secret can be sentenced for trade espionage to fines or imprisonment up to 2 years, or when the offence is serious up to 6 years. Circumstances that may lead to a serious offence is if the act was of particularly dangerous kind, concerned a considerable monetary value or resulted in a particular serious damage. The penalty will not be sentenced if a more serious penalty follows under the Swedish Penal Code. Attempts and planning of espionage is penalized in accordance with Chapter 23 in the Penal Code.

Section 4 in the Trade Secrets Act regulates criminal liability for *unauthorized dealing with a trade secret*. Anyone who obtains a trade secret knowing that the person who made available the trade secret, or anyone before him, accessed it through an act of trade espionage can be sentenced for unauthorized dealing with a trade secret to fine or imprisonment up to 2 years, or if the offence is serious, up to 4 years. The penalty will not be sentenced if a more serious penalty follows under the Swedish Penal Code.

Section 5 in the Trade Secrets Act regulates civil liability, for anyone who commits an offence in accordance with section 3 or 4, to pay damages caused through the offence, or the use or disclosure of the trade secret without authorization.

A list of relevant literature, related to trade secrets in general, is available under Question A 8 in the Commercial and IP Law Questionnaire - B.

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

The relevant criminal provisions in the Trade Secrets Act do not establish any requirements as to the purpose that the infringer may pursue. The requirement is that the offender accessed the trade secret wilfully and without authorization. Regarding the prerequisite on wilfulness, liability also includes offences where the offender suspected that the information was confidential and still carried on with his/her actions unconcerned of the result thereof. There is no requirement regarding the purpose, e.g. obtaining advantages or the like. It is neither required that the offender actually used or disclosed the trade secrets.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

The violation of trade secrets may entail other criminal offences as well as civil lawsuits. In addition to the Trade Secrets Act the following criminal provisions in the Swedish Penal Code that can be applicable to trade secrets violations:

Chapter 4 Section 9 c in the Penal Code regulates liability for *unauthorized access to computer systems* [*Sw*. dataintrång]. A person who unlawfully accesses, amends, deletes, blocks or in a register inserts data intended for automated processing can be liable.

Chapter 8 Section 8 in the Penal Code regulates liability for *unlawful dispossession* [*Sw*. egenmäktigt förfarande]. A person who unlawfully takes and utilizes something can be liable. The regulation is subsidiary in relation to other regulations in chapter 8 of the Penal Code, such as theft and robbery. This means that the regulation can be applicable if any of the prerequisites in the other regulations are not fulfilled.

Chapter 10 Section 4 in the Penal Code regulates liability for *fraudulent conversion* [*Sw*. olovligt förfogande]. A typical case is when someone has something in his or her possession that someone else owns and the offender deprives the rightful owner of his property.

Chapter 10 Section 5 in the Penal Code regulates criminal liability for *breach of faith against principal* [*Sw*. trolöshet mot huvudman]. The liability applies to individuals with high positions in the organization who abuses a position of trust concerning financial, legal or technical control. The criminal act may in such cases consist of disclosure of trade secrets. To be enforceable the act must have resulted in an immediate or indirect financial loss for the principal. It is not required that the offender benefits financially from the actions.

Chapter 10 Section 7 in the Penal Code regulates criminal liability for *unlawful use* [*Sw*. olovligt brukande]. The regulation is applicable to individuals that unlawfully use something that belongs to somebody else.

Chapter 19 Sections 5 and 6 in the Penal Code regulates liability for *espionage* [*Sw*. spioneri]and *serious espionage* [*Sw*. grovt spioneri] for a person who, in order to benefit a foreign power, unauthorized obtains, transfers, gives, or discloses information which relates to facts that may cause detriment for the national defence or national security.

Chapter 19 Section 7 of the Penal Code regulates liability for *unlawful dealing with secret information* [*Sw.* obehörig befattning med hemlig uppgift]. A person who transfers, gives or discloses confidential information, that may cause detriment for the national defense or national security, without having the purpose of benefitting a foreign power, can be liable.

Chapter 19 Section 9 in the Penal Code regulates *negligent dealing with confidential information* [*Sw*. vårdslöshet med hemlig uppgift]. A person who out of gross negligence transfers, gives or discloses such confidential information as referred to in Chapter 19 Section 7 in the Penal Code can be liable.

Chapter 20 Section 2 in the Penal Code regulates criminal liability for *taking a bribe* [*Sw.* mutbrott]. The regulation is applicable to individuals that receives, accepts a promise of, or demands a bribe or other improper reward for the performance of his or her duties. Supposedly an employee that lawfully has gained access to a trade secret in its employment could be subject to this regulation if he or she discloses the trade secret against some improper reward. Chapter 17 Section 7 in the Penal Code regulates

criminal liability for the individual who gives the reward. In such cases Section 3 in the Trade Secrets Act regulating trade espionage should possibly be applicable in stead, since the trade secret has been assessed unlawfully.

Chapter 20 Section 3 in the Penal Code regulates criminal liability for *breach of professional confidentiality* [*Sw.* brott mot tystnadsplikt]. The liability applies to individuals that are subject to a statutory duty of professional confidentiality. Liability does not require that the confidential information is actually reviewed by a third party. It is sufficient that confidential information is used by the professional or provided by the professional to a third party.

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "*fair use*", "*just cause", "de minimis threshold*")?

For criminal liability under the Trade Secrets Act the information must first fall within the definition of "trade secrets" in the Trade Secrets Act meaning that (i) the information must concern business conditions or operating conditions of a business, (ii) the information must be kept confidential, and (iii) a disclosure of the information must be likely to be damaging for the competiveness of the business in question.

Also the Trade Secrets Act does only apply to unauthorized attacks on trade secrets meaning that disclosures aiming to reveal criminal activity and other wrongdoings of a company, i.e. so called "whistle blowing" are not prohibited. It is also permitted to use or disclose a trade secret that you or somebody before you gained knowledge of in good faith.

For criminal liability the information must have been accessed wilfully and without authorization. Information that a person lawfully gained in a business relationship or in line with his or her employment is not ground for criminal liability in accordance with the Trade Secrets Act. A criminal action is conditioned upon that the prosecutor can prove that the suspect has gained access of the information in an unlawful manner. This means that criminal liability can not be charged upon somebody that was informed of secret information in a business meeting or gained knowledge of secret information in line with his or her work tasks. In such cases it might be possible to initiate civil proceedings in stead. In some cases it might also be possible to apply other criminal regulations in the Penal Code. In a judgment from the Court of Appeal a former employee disclosed information to a foreign intelligence officer regarding products in the communications business which belonged to the former employer group. The District Court and the Court of Appeal stated that disclosing information on communication was considered as a threat against national security, and the former employee was sentenced to 8 years imprisonment for serious espionage in accordance with Chapter 19 Section 6 in the Penal Code. The former employee had received the information from two employed engineers. The Court of Appeal found that one of the engineers was guilty of trade espionage as he unlawfully and wilfully had accessed the information. However, the Court of Appeal dismissed the criminal charges against the second engineer as this engineer had lawful access to the disclosed information in his work.

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

The sole risk of dissemination or disclosure of a trade secret does not give rise to criminal liability.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

The criminal violations of trade secrets apply generally and are not depending on the personal qualities of the infringer or the type of items covered by trade secrets.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

Trade secrets are considered closely related to intellectual property rights, however not regarded or protected as such. There are differences as to the conditions for protection as well as the scope of protection. Intellectual property rights in contrary to trade secrets enjoy protection as exclusive rights. Unauthorized use of intellectual property rights are subject to criminal liability under Swedish intellectual property laws. Unauthorized use of trade secrets is not as such subject to criminal liability under the Trade Secrets Act, although it is subject to civil actions. The criminal liability regarding trade secrets requires that the trade secret has been assessed without authorization.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

Trade secrets can be information documented in some form as well as the mere knowledge of single individuals about a specific circumstance even if it has not been documented. If the information is so connected to a specific individual that it cannot by instructions or direction be transferred to someone else, the information is considered a skill of personal nature. In such cases the information is not regarded as a trade secret under the Trade Secrets Act. Different types of information can be recognized as trade secrets in Sweden, such as for instance technical information, commercial information and business operative information. More specific examples are manufacturing technology, know how, price lists, customer lists, financial reports etc. Also relatively trivial details can qualify as trade secrets. Different types of trade secrets are not treated differently under the Trade Secrets Act.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

There are no specific requirements for trade secrets to avail themselves of the relevant legal protection, such as for instance requirements for originality, inventive step or the like. The requirement is that the information must concern business conditions or operating conditions of a business, be kept confidential, and that a disclosure of the information must be likely to be damaging for the competiveness of the business in question.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Sweden provides criminal protection for unauthorized use of registered and unregistered IP rights, which is regulated in applicable IP legislations, for instance the Patents Act, Trademarks Act, Design Protection Act and the Act on Copyright in literary and artistic Works.

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

The offender may be prosecuted at the sole initiative of the public prosecutor. However, in order to call the public prosecutor´s attention to the offence, it is advisable to file a report with the public prosecutor.

The injured party may only institute criminal prosecution at court (so-called private prosecution) if the injured party has reported the offence for prosecution and the public prosecutor has decided not to institute any prosecution.

The injured party may always institute civil litigation (regardless of any prosecution) in order to claim damages and file an application for a summons with the court in this respect.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

In criminal cases the prosecutor has to prove "beyond reasonable doubt" that the person prosecuted has committed the crime. The public prosecutor has to determine and bring before court the evidence deemed necessary in order to fulfil the burden of proof. Usually the prosecutor relies on documentary evidence and witness examinations in order to substantiate this, but other means of evidence is allowed as well. There are no specific evidence as such that has to be brought before the court, it rather depends on the situation of the specific case.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

The Trade Secrets Act does not allow the holder to apply for any such ex parte orders to secure evidence. In criminal proceedings the public prosecutor has various means to take action (such as searching premises and computer systems and to seize computers and to interview the offender and other witnesses) in the course of the criminal proceedings in order to investigate the crime. However, the holder has no influence in this respect. The measures by the public prosecutor are not aimed at protecting the interests of the holder but to investigate the crime and eventually get the offender prosecuted.

A person who has violated a trade secret in accordance with the Trade Secret Act can be prohibited by the court under a penalty of fine to use or disclose the trade secret. Such claim can also be brought in the criminal proceedings. The claim shall be brought by the person who has been subject of the unlawful violation. The prohibition requires that the prerequisites of either of the criminal provisions are met.

The court may also order that documents or objects which contain trade secrets shall be surrendered to the plaintiff by the defendant provided that they are in his or her possession. The court may order that such surrender shall take place against

redemption. The documents or objects do not have to be identical to those that have originally been obtained be the defendant. If the document or object can not be surrendered without inconvenience the court may order that the document or object shall be destroyed or altered or that another action shall be taken as to prevent misuse.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Criminal liability may only be enforced on natural persons and companies can not as such be liable for criminal offences. A corporate fine may be imposed under certain circumstances for crimes committed in the business, in accordance with Chapter 36 Section 7 in the Penal Code. The regulation on corporate fine is rarely applied, and when so, it is usually related to environmental or tax cases.

2. If so, which type of liability arises for companies? Which penalties shall apply?

A corporate fine may be imposed for crimes committed in the business, if the trader has not done what is reasonably necessary to prevent the crime, or the offense was committed by a person in a leadership position or a person who otherwise had a special responsibility for the supervision or control of the business.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

The Swedish General courts, i.e. the District Courts, the Courts of Appeal and the Supreme Court.

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

There are no formalities how to keep the information secret. There is no requirement to express a specific obligation to keep information confidential, for a trade secrets violation to occur. Even without any specific measures the owner's intention to keep the information confidential can be clear. The aim and the character of the business can be such that it is clear that the information is confidential even without an expressed obligation. The owner of the information, is however likely to bear the risk of any unclearness as to whether or not specific information is confidential. A case-by-case assessment normally needs to be done in each individual case.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

No there is no such requirement for the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

The aggrieved person may bring a claim for damages in the course of a criminal proceeding. However, the court may order that the claim shall be disposed of as a separate case in the manner prescribed for civil action if further joint adjudication with the criminal proceeding would cause major inconvenience. In addition, in case there already is a pending civil court case regarding the damages, the aggrieved person may not bring the same claim for damages in the course of the criminal proceedings because there may not be two court cases dealing with the same matter.

Switzerland

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Nature of criminal law norms and classification within legal system

As a basic principle, each individual is personally responsible for the protection of the results of his or her work efforts. For this purpose, *physical* work products are protected by the proprietary rights of the individual.

However, as *intellectual* work products are ubiquitous in nature, the producers of such work products require different protection mechanisms. One such mechanism consists of intellectual property rights such as patents, trademarks, copyrights and design rights (so-called "subjective" protection). The other mechanism is the "objective" protection of intellectual work efforts, i.e. sanctions against behaviour apt to impair intellectual work products, such as betrayal of secrets or industrial espionage. One instrument by which the mechanism of "objective" protection is incorporated into the legal system are the criminal law provisions in the Swiss Criminal Code and the Unfair Competition Act as listed below.

One purpose of the relevant provisions is the protection of trade secrets against unauthorised disclosure. Additionally, in particular the provisions of the Act Against Unfair Competition impose criminal sanctions on the unauthorised use and exploitation of trade secrets. Some provisions, finally, impose criminal liability in case of the unauthorised acquirement of trade secrets.

In the following you will find an overview of the respective legal provisions in the three official languages in Switzerland (German, French and Italian) as well as in an English translation. The latter is for convenience purposes only and not an official translation of the respective provision.

Provisions in the Swiss Criminal Code

There are four provisions dealing with trade secrets in the Criminal Code, arts. 162, 273, 320 and 321 Criminal Code.

Art. 162 Criminal Code imposes criminal liability on the betrayal of trade secrets. It provides the following:

Art. 162 - Verletzung des Fabrikations- oder Geschäftsgeheimnisses

> Wer ein Fabrikations- oder Geschäftsgeheimnis, das er infolge einer gesetzlichen oder vertraglichen Pflicht bewahren sollte, verrät,
>
> wer den Verrat für sich oder einen andern ausnützt,
>
> wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.
>
> Art. 162 - Violation du secret de fabrication ou du secret commercial
>
> Celui qui aura révélé un secret de fabrication ou un secret commercial qu'il était tenu de garder en vertu d'une obligation légale ou contractuelle,
>
> celui qui aura utilisé cette révélation à son profit ou à celui d'un tiers,

sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

Art. 162 - Violazione del segreto di fabbrica o commerciale

Chiunque rivela un segreto di fabbrica o commerciale, che aveva per legge o per contratto l'obbligo di custodire,

chiunque trae profitto per sè o per altri da questa rivelazione,

è punito, a querela di parte, con una pena detentiva sino a tre anni o con una pena pecuniaria.

Art. 162 - Breach of manufacturing or trade secrecy [1]

Any person who betrays a manufacturing or trade secret that he is under a statutory or contractual duty contract not to reveal,

any person who exploits for himself or another such a betrayal,

shall on complaint be liable to a custodial sentence not exceeding three years or to a monetary penalty.

In the system of the Criminal Code, art. 162 is classified under the sub-section "Offences against Property". This classification is, however, criticized by some legal scholars, as they argue that the provision aims to achieve the protection of confidentiality within organizations and not the protection of assets (cf. *below*; cf. also MARC AMSTUTZ/MANI REINERT, Art. 162 StGB, in: Niggli/Wiprächtiger (eds.), Basler Kommentar zum Strafrecht II, 2. ed., Basel 2007, N 1).

Art. 162 Criminal Code provides protection against the exploitation of trade secrets obtained in an unlawful manner only.

Art. 273 Criminal Code states:

Art. 273 - Wirtschaftlicher Nachrichtendienst

Wer ein Fabrikations- oder Geschäftsgeheimnis auskundschaftet, um es einer fremden amtlichen Stelle oder einer ausländischen Organisation oder privaten Unternehmung oder ihren Agenten zugänglich zu machen,

wer ein Fabrikations- oder Geschäftsgeheimnis einer fremden amtlichen Stelle oder einer ausländischen Organisation oder privaten Unternehmung oder ihren Agenten zugänglich macht,

wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe, in schweren Fällen mit Freiheitsstrafe nicht unter einem Jahr bestraft. Mit der Freiheitsstrafe kann Geldstrafe verbunden werden.

Art. 273 - Service de renseignements économiques

Celui qui aura cherché à découvrir un secret de fabrication ou d'affaires pour le rendre accessible à un organisme officiel ou privé étranger, ou à une entreprise privée étrangère, ou à leurs agents,

celui qui aura rendu accessible un secret de fabrication ou d'affaires à un organisme officiel ou privé étranger, ou à une entreprise privée étrangère, ou à leurs agents,

sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire ou, dans les cas graves, d'une peine privative de liberté d'un an au moins.

[1] Unofficial translation provided for information purposes by The Federal Authorities of the Swiss Confederation, cf. http://www.admin.ch/ ch/e/rs/311_0/a162.html.

En cas de peine privative de liberté, une peine pécuniaire peut également être prononcée.

Art. 273 - Spionaggio economico

Chiunque cerca di scoprire un segreto di fabbricazione o di affari per renderlo accessibile ad un organismo ufficiale o privato dell'estero, ovvero ad un'impresa od organizzazione privata estera, o ai loro agenti,

chiunque rende accessibile un segreto di fabbricazione o di affari ad un organismo ufficiale o privato dell'estero, ovvero ad una impresa od organizzazione privata estera, o ai loro agenti,

è punito con una pena detentiva sino a tre anni o con una pena pecuniaria o, nei casi gravi, con una pena detentiva non inferiore ad un anno. Con la pena detentiva può essere cumulata una pena pecuniaria.

Art. 273 - Industrial espionage [2]

Any person who obtains a manufacturing or trade secret in order to make it available to an external official agency, a foreign organisation, a private enterprise, or the agents of any of these, or,

any person who makes a manufacturing or trade secret available to an external official agency, a foreign organisation, a private enterprise, or the agents of any of these,

shall be liable to a custodial sentence not exceeding three years or to a monetary penalty, or in serious cases to a custodial sentence of not less than one year. Any custodial sentence may be combined with a monetary penalty.

Besides this, arts. 320 and 321 of Criminal Code impose criminal liablity on the violation of trade secrets which have been confided or become known to the offender in course of his official duties or an occupation for the aggrieved party:

Art. 320 – Verletzung des Amtsgeheimnisses

1. Wer ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Mitglied einer Behörde oder als Beamter anvertraut worden ist, oder das er in seiner amtlichen oder dienstlichen Stellung wahrgenommen hat, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Die Verletzung des Amtsgeheimnisses ist auch nach Beendigung des amtlichen oder dienstlichen Verhältnisses strafbar.

2. Der Täter ist nicht strafbar, wenn er das Geheimnis mit schriftlicher Einwilligung seiner vorgesetzten Behörde geoffenbart hat.

Art. 320 – Violation du secret de fonction

1. Celui qui aura révélé un secret à lui confié en sa qualité de membre d'une autorité ou de fonctionnaire, ou dont il avait eu connaissance à raison de sa charge ou de son emploi, sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

La révélation demeure punissable alors même que la charge ou l'emploi a pris fin.

2. La révélation ne sera pas punissable si elle a été faite avec le consentement écrit de l'autorité supérieure.

Art. 320 – Violazione del segreto d'ufficio

[2] Unofficial translation, cf. http://www.admin.ch/ch/e/rs/ 311_0/a273.html.

1. Chiunque rivela un segreto, che gli è confidato nella sua qualità di membro di una autorità o di funzionario o di cui ha notizia per la sua carica o funzione, è punito con una pena detentiva sino a tre anni o con una pena pecuniaria.

La rivelazione del segreto è punibile anche dopo la cessazione della carica o della funzione.

2. La rivelazione fatta col consenso scritto dell'autorità superiore non è punibile.

Art. 320 – Breach of official secrecy [3]

1. Any person who discloses secret information that has been confided to him in his capacity as a member of an authority or as a public official or which has come to his knowledge in the execution of his official duties shall be liable to a custodial sentence not exceeding three years or to a monetary penalty.

A breach of official secrecy remains an offence following termination of employment as a member of an authority or as a public official.

2. The offender is not liable to any penalty if he has disclosed the secret information with the written consent of his superior authority.

Art. 321 - Verletzung des Berufsgeheimnisses

1. Geistliche, Rechtsanwälte, Verteidiger, Notare, Patentanwälte, nach Obligationenrecht zur Verschwiegenheit verpflichtete Revisoren, Ärzte, Zahnärzte, Apotheker, Hebammen sowie ihre Hilfspersonen, die ein Geheimnis offenbaren, das ihnen infolge ihres Berufes anvertraut worden ist oder das sie in dessen Ausübung wahrgenommen haben, werden, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Ebenso werden Studierende bestraft, die ein Geheimnis offenbaren, das sie bei ihrem Studium wahrnehmen.

Die Verletzung des Berufsgeheimnisses ist auch nach Beendigung der Berufsausübung oder der Studien strafbar.

2. Der Täter ist nicht strafbar, wenn er das Geheimnis auf Grund einer Einwilligung des Berechtigten oder einer auf Gesuch des Täters erteilten schriftlichen Bewilligung der vorgesetzten Behörde oder Aufsichtsbehörde offenbart hat.

3. Vorbehalten bleiben die eidgenössischen und kantonalen Bestimmungen über die Zeugnispflicht und über die Auskunftspflicht gegenüber einer Behörde.

Art. 321 - Violation du secret professionnel

1. Les ecclésiastiques, avocats, défenseurs en justice, notaires, conseils en brevets, contrôleurs astreints au secret professionnel en vertu du code des obligations1, médecins, dentistes, pharmaciens, sages-femmes, ainsi que leurs auxiliaires, qui auront révélé un secret à eux confié en vertu de leur profession ou dont ils avaient eu connaissance dans l'exercice de celle-ci, seront, sur plainte, punis d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. [2]

Seront punis de la même peine les étudiants qui auront révélé un secret dont ils avaient eu connaissance à l'occasion de leurs études.

La révélation demeure punissable alors même que le détenteur du secret n'exerce plus sa profession ou qu'il a achevé ses études.

[3] Unofficial translation, cf. http://www.admin.ch/ch/e/rs/311_0/a320.html.

2. La révélation ne sera pas punissable si elle a été faite avec le consentement de l'intéressé ou si, sur la proposition du détenteur du secret, l'autorité supérieure ou l'autorité de surveillance l'a autorisée par écrit.

3. Demeurent réservées les dispositions de la législation fédérale et cantonale statuant une obligation de renseigner une autorité ou de témoigner en justice.

Art. 321 - Violazione del segreto professionale

1. Gli ecclesiastici, gli avvocati, i difensori, i notai, i consulenti in brevetti, i revisori tenuti al segreto professionale in virtù del Codice delle obbligazioni[1], i medici, i dentisti, i farmacisti, le levatrici, come pure gli ausiliari di questi professionisti, che rivelano segreti a loro confidati per ragione della loro professione o di cui hanno avuto notizia nell'esercizio della medesima sono puniti, a querela di parte, con una pena detentiva sino a tre anni o con una pena pecuniaria[2,3].

Sono parimente puniti gli studenti che rivelano un segreto di cui hanno avuto notizia nel corso dei loro studi.

La rivelazione del segreto è punibile anche dopo la cessazione dell'esercizio della professione o dopo la fine degli studi.

2. La rivelazione non è punibile, quando sia fatta col consenso dell'interessato o con l'autorizzazione scritta data, a richiesta di chi detiene il segreto, dall'autorità superiore o dall'autorità di vigilanza.

3. Rimangono riservate le disposizioni della legislazione federale e cantonale sull'obbligo di dare informazioni all'autorità o di testimoniare in giudizio.

Art. 321 - Breach of professional confidentiality[4]

1. Any person who in his capacity as a member of the clergy, lawyer, defence lawyer, notary, patent attorney, auditor subject to a duty of confidentiality under the Code of Obligations, doctor, dentist, pharmacist, midwife or as an auxiliary to any of the foregoing persons discloses confidential information that has been confided to him in his professional capacity or which has come to his knowledge in the practice of his profession shall be liable to a custodial sentence not exceeding three years or to a monetary penalty.

A student who discloses confidential information that has come to his knowledge in the course of his studies is also liable to the foregoing penalties.

A breach of professional confidentiality remains an offence following the termination of professional employment or of the studies.

2. No offence is committed if the person disclosing the information does so with the consent of the person to whom the information pertains or on the basis of written authorisation issued in response to his application by a superior authority or supervisory authority.

3. The federal and cantonal provisions on the duty to testify and on the obligation to provide information to an authority are reserved.

Fundamental legal values protected by criminal law provisions regarding trade secrets

The fundamental legal value protected by art. 162 Criminal Code (betrayal and exploitation of trade secrets) is *confidentiality*: Whoever betrays a secret violates his or her duty of loyalty to the owner of the trade secret. The owner of the trade secret shall be enabled to control the dissemination of the secret. Another justification lies in the protection of the *economic merits of businesses*, i.e. the internal information in

[4] Unofficial translation, cf. http://www.admin.ch/ch/e/rs/311_0/a321.html.

possession of the businesses. For further details cf. JEAN NICOLAS DRUEY, Information als Gegenstand des Rechts, Zürich/Baden-Baden 1995, p. 366.

Art. 273 Criminal Code (industrial espionage) particularly protects (public) interests of the Swiss Confederation, which is reflected by the classification of the provision under the sub-section "Felonies and Misdemeanours against the State and National Security". The protection of the Swiss national economy is a "byproduct" of the protection of national interests (cf. THOMAS HOPF, Art. 273 StGB, in: Niggli/Wiprächtiger (eds.), Basler Kommentar zum Strafrecht II, 2. ed., Basel 2007, N 5).

The fundamental legal value protected by art. 320 Criminal Code is the privacy of citizens as well as confidentiality, as far as government authorities require disclosure of secrets. Moreover, it protects government's interest in discretion of members of authorities and public officials when dealing with private and government secrets.

The legal values protected by art. 321 Criminal Code correspond to the ones protected by art. 162 Criminal Code. The special *relationship of confidentiality* in certain professional relationships, which may also arise out of private law, is protected by this rule.

Provisions in the Unfair Competition Act

According to Art. 23 Unfair Competition Act ("UCA"), deliberate infringements of arts. 4, 5 and 6 UCA also constitute criminal offenses:

> Art. 23 - Unlauterer Wettbewerb
> [1] Wer vorsätzlich unlauteren Wettbewerb nach Artikel 3, 4, 4a, 5 oder 6 begeht, wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.
> 2 Strafantrag stellen kann, wer nach den Artikeln 9 und 10 zur Zivilklage berechtigt ist.
>
> Art. 23 - Concurrence déloyale
> [1] Quiconque, intentionnellement, se rend coupable de concurrence déloyale au sens des art. 3, 4, 4*a*, 5 ou 6 est, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.
> [2] Peut porter plainte celui qui a qualité pour intenter une action civile selon les art. 9 et 10.
>
> Art. 23 - Concorrenza sleale
> [1] Chiunque, intenzionalmente, si rende colpevole di concorrenza sleale ai sensi degli articoli 3, 4, 4*a*, 5 o 6 è punito, a querela di parte, con una pena detentiva sino a tre anni o con una pena pecuniaria.
> [2] Può sporgere querela chiunque è legittimato all'azione civile secondo gli articoli 9 e 10.
>
> Art. 23 - Unfair Competition[5]
> [1] Anyone who intentionally commits an act of unfair competition as defined in Art. 3, 4, 5 or 6, shall upon petition, be punished with imprisonment oif up to three years or a fine of up to 100'000 CHF.
> [2] Anyone who is entitled to file a civil action under Art. 9 and 10 may petition for criminal prosecution.

Arts. 4, 5 and 6 UCA read as follows:

> Art. 4 - Inducement to breach or rescind of Contract
>
> Acting unfairly is, in particular, whoever:

[5] Unofficial translation of the Swiss Chamber of Commerce.

a. induces consumers to breach a contract in order to be able to conclude a contract with them himself;
b. induces employees, agents or other auxiliary persons to disclose or search out industrial or trade secrets of their employers or principals;
c. causes a purchaser or borrower, who entered into an instalment sale, a sale with payments in advance or a consumer loan, to rescind the contract, or who causes a purchaser to terminate a sale with payments in advance, in order to conclude such a contract with that purchaser or borrower himself.

Art. 4 - Verleitung zu Vertragsverletzung oder -auflösung

Unlauter handelt insbesondere, wer:
a. Abnehmer zum Vertragsbruch verleitet, um selber mit ihnen einen Vertrag abschliessen zu können;
b. …
c. Arbeitnehmer, Beauftragte oder andere Hilfspersonen zum Verrat oder zur Auskundschaftung von Fabrikations- oder Geschäftsgeheimnissen ihres Arbeitgebers oder Auftraggebers verleitet;
d. einen Käufer oder Kreditnehmer, der einen Vorauszahlungskauf oder einen Konsumkreditvertrag abgeschlossen hat, veranlasst, den Vertrag zu widerrufen, oder wer einen Käufer, der einen Vorauszahlungskauf abgeschlossen hat, veranlasst, diesen zu kündigen, um selber mit ihm einen solchen Vertrag abzuschliessen.

Art. 4 - Incitation à violer ou à résilier un contrat

Agit de façon déloyale celui qui, notamment:
a. incite un client à rompre un contrat en vue d'en conclure un autre avec lui;
b. ...
c. incite des travailleurs, mandataires ou auxiliaires à trahir ou à surprendre des secrets de fabrication ou d'affaires de leur employeur ou mandant;
d. incite un acheteur ou un preneur qui a conclu une vente avec paiements préalables ou un contrat de crédit à la consommation à révoquer ce contrat, ou un acheteur qui a conclu une vente avec paiements préalables à dénoncer celle-ci, pour conclure de son côté un tel contrat avec lui.

Art. 4 - Incitamento a violare o a rescindere un contratto

Agisce in modo sleale, segnatamente, chiunque:
a. incita il cliente a rescindere un contratto per stipularne uno con lui;
b. …
c. induce lavoratori, mandatari o altri ausiliari a rivelare o a spiare segreti di fabbrica o d'affari del loro datore di lavoro o del loro mandante;
d. incita il compratore o creditato che ha concluso una vendita a rate anticipate o un contratto di credito al consumo, a revocare il contratto oppure il compratore che ha concluso una vendita a rate anticipate, a disdirla, per stipulare il contratto con lui.

Art. 5 - Exploitation of the work of third parties

Acting unfairly is, in particular, whoever:
a. exploits, without authorization, work product entrusted to him, such as bids, calculations and blueprints;
b. exploits the work product of a third party such as bids, calculations and blueprints, although he should know that such work product was provided or made available to him without authorization;
c. appropriates and exploits, by the use of technical reproduction procedures, the work product of another which is ready to be marketed and who does so without making an appropriate effort himself.

Art. 5 - Verwertung fremder Leistung

Unlauter handelt insbesondere, wer:

a. ein ihm anvertrautes Arbeitsergebnis wie Offerten, Berechnungen oder Pläne unbefugt verwertet;
b. ein Arbeitsergebnis eines Dritten wie Offerten, Berechnungen oder Pläne verwertet, obwohl er wissen muss, dass es ihm unbefugterweise überlassen oder zugänglich gemacht worden ist;
c. das marktreife Arbeitsergebnis eines andern ohne angemessenen eigenen Aufwand durch technische Reproduktionsverfahren als solches übernimmt und verwertet.

Art. 5 - Exploitation d'une prestation d'autrui

Agit de façon déloyale celui qui, notamment:
a. exploite de façon indue le résultat d'un travail qui lui a été confié, par exemple des offres, des calculs ou des plans;
b. exploite le résultat du travail d'un tiers, par exemple des offres, des calculs ou des plans, bien qu'il sache que ce résultat lui a été remis ou rendu accessible de façon indue;
c. reprend grâce à des procédés techniques de reproduction et sans sacrifice correspondant le résultat de travail d'un tiers prêt à être mis sur le marché et l'exploite comme tel.

Art. 5 - Sfruttamento di una prestazione d'altri

Agisce in modo sleale, segnatamente, chiunque:
a. sfrutta, senza esserne autorizzato, il risultato affidatogli di un lavoro, per esempio offerte, calcoli o piani;
b. sfrutta il risultato del lavoro di un terzo, per esempio offerte, calcoli o piani, benché sappia che gli è stato affidato o reso accessibile senza esserne autorizzati;
c. riprende come tale, con mezzi tecnici di riproduzione, senza prestazione personale appropriata, e sfrutta il risultato del lavoro di un terzo, pronto a essere immesso sul mercato.

Art. 6 Violation of industrial and trade secrets

Acting unfairly is, in particular, whoever exploits or discloses to third parties industrial or trade secrets, which he has searched out or learned about in any unlawful matter.

Art. 6 Verletzung von Fabrikations- und Geschäftsgeheimnissen

Unlauter handelt insbesondere, wer Fabrikations- oder Geschäftsgeheimnisse, die er ausgekundschaftet oder sonst wie unrechtmässig erfahren hat, verwertet oder andern mitteilt.

Art. 6 Violation des secrets de fabrication ou d'affaires

Agit de façon déloyale celui qui, notamment, exploite ou divulgue des secrets de fabrication ou d'affaires qu'il a surpris ou dont il a eu indûment connaissance d'une autre manière.

Art. 6 Violazione di segreti di fabbrica e di affari

Agisce in modo sleale, segnatamente, chiunque sfrutta o comunica ad altri segreti di fabbrica o di affari che ha spiato o di cui è venuto a conoscenza in altro modo illecito.

For more detailed information on arts. 4, 5 and 6 please see the IP & Commercial Law Questionnaire, A.2.

Criminal Provisions in the Banking Act

Besides this, art. 47 Banking Act stipulates criminal sanctions in case of an unlawful disclosure of secrets by banks and their organs, employees, agents or liquidators.

Art. 47

[1] Imprisonment of up to three years or fine will be awarded to persons who deliberately:
a. disclose a secret that is entrusted to him in his capacity as body, employee, appointee, or liquidator of a bank, as body or employee of an audit company or that he has observed in this capacity;
b. attempts to induce such an infraction of the professional secrecy.
[2] Persons acting with negligence will be penalized with a fine of up to 250 000 francs.
[3] In the case of a repeat within five years of the prior conviction, the fine will amount to 45 day rates at a minimum.
[4] The violation of the professional secrecy also punishable after conclusion of the licensed or official responsibilities or the professional exercising duties is punishable.
[5] The federal and cantonal provisions on the duty to provide information to an authority remain reserved.
[6] Prosecution and judgment of offences pursuant to these provisions are incumbent upon the cantons. The general provisions of the Swiss Penal Code are applicable.

Art. 47

[1] Mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe wird bestraft, wer vorsätzlich:
a. ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Organ, Angestellter, Beauftragter oder Liquidator einer Bank, als Organ oder Angestellter einer Prüfgesellschaft anvertraut worden ist oder das er in dieser Eigenschaft wahrgenommen hat;
b. zu einer solchen Verletzung des Berufsgeheimnisses zu verleiten sucht.
[2] Wer fahrlässig handelt, wird mit Busse bis zu 250 000 Franken bestraft.
[3] Im Fall einer Wiederholung innert fünf Jahren nach der rechtskräftigen Verurteilung beträgt die Geldstrafe mindestens 45 Tagessätze.
[4] Die Verletzung des Berufsgeheimnisses ist auch nach Beendigung des amtlichen oder dienstlichen Verhältnisses oder der Berufsausübung strafbar.
[5] Vorbehalten bleiben die eidgenössischen und kantonalen Bestimmungen über die Zeugnispflicht und über die Auskunftspflicht gegenüber einer Behörde.

[6] Verfolgung und Beurteilung der Handlungen nach dieser Bestimmung obliegen den Kantonen. Die allgemeinen Bestimmungen des Strafgesetzbuches kommen zur Anwendung.

Art. 47

[1] Est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire celui qui, intentionnellement:
a. en sa qualité d'organe, d'employé, de mandataire ou de liquidateur d'une banque, ou encore d'organe ou d'employé d'une société d'audit, révèle un secret à lui confié ou dont il a eu connaissance en raison de sa charge ou de son emploi;
b. incite autrui à violer le secret professionnel.
[2] Si l'auteur agit par négligence, il est puni d'une amende de 250 000 francs au plus.

[3] En cas de récidive dans les cinq ans suivant une condamnation entrée en force, la peine pécuniaire est de 45 jours-amende au moins.
[4] La violation du secret professionnel demeure punissable alors même que la charge, l'emploi ou l'exercice de la profession a pris fin.
[5] Les dispositions de la législation fédérale et cantonale sur l'obligation de renseigner l'autorité et de témoigner en justice sont réservées.
[6] La poursuite et le jugement des infractions réprimées par la présente disposition incombent aux cantons. Les dispositions générales du code pénal sont applicables.

Art. 47

[1] È punito con una pena detentiva sino a tre anni o con una pena pecuniaria chiunque, intenzionalmente:
a. rivela un segreto che gli è confidato o di cui ha notizia nella sua qualità di membro di un organo, impiegato, mandatario o liquidatore di una banca, membro di un organo o impiegato di una società di audit;
b. ovvero tenta di indurre a siffatta violazione del segreto professionale.
[2] Chi ha agito per negligenza è punito con la multa sino a 250 000 franchi.
[3] In caso di recidiva entro cinque anni da una condanna passata in giudicato, la pena pecuniaria è di almeno 45 aliquote giornaliere.
[4] La rivelazione del segreto è punibile anche dopo la cessazione della carica, della funzione o dell'esercizio della professione.
[5] Sono fatte salve le disposizioni delle legislazioni federali e cantonali sull'obbligo di dare informazioni all'autorità e di testimoniare in giudizio.
[6] Il perseguimento e il giudizio delle azioni punibili in conformità di queste disposizioni competono ai Cantoni. Sono applicabili le disposizioni generali del Codice penale.

List of selected literature

GEORGES BINDSCHEDLER, Der strafrechtliche Schutz wirtschaftlicher Geheimnisse, Diss. Bern 1981

FREDERIC H. COMPTESSE, Begriff und Schutz des Geheimnisses im Schweizerischen Zivilgesetzbuch (Strafgesetzbuch), in: ZStrR 56 (1942) p. 264 et seqq.

JEAN NICOLAS DRUEY, Information als Gegenstand des Rechts, Zürich/Baden-Baden 1995

JEAN NICOLAS DRUEY, Das Fabrikationsgeheimnis - faktisches Gut oder Rechtsgut?, ZSR NF 92 (1973) I 451

Niggli/Wiprächtiger (eds.), Basler Kommentar zum Strafrecht II, 2. ed., Basel 2007 (arts. 162, 273, 321)

BERTRAND PERRIN, La protection pénale des données informatiques de l'entreprise, Der Schweizer Treuhänder 8/2011, p. 605 et seqq.

GÜNTER STRATENWERTH/GUIDO JENNY, Schweizerisches Strafrecht, Besonderer Teil I: Straftaten gegen Individualinteressen, 6. ed., Bern 2003 (§ 22)

Trechsel et al. (eds.), Schweizerisches Strafgesetzbuch, Praxiskommentar, Zürich/St.Gallen 2008 (arts. 162, 273, 321)

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

Betrayal and exploitation of secrets (art. 162 Criminal Code)

The criminal liability for betrayal of a secret, according to art. 162 para. 1 of Criminal Code, does *not depend on a particular purpose pursued by the infringer*. However, the behavior is only punishable if the infringer acts with intent and knowledge of the fact that the information concerned is secret, the existence of the obligation of confidentiality and the fact that the infringer must not divulge this information to the third party concerned.

As opposed to para. 1, the liability according to art. 162 para. 2 of Criminal Code requires the *purpose of utilizing the trade secret* which was unlawfully obtained. The offender must have the *intent to gain an advantage* for himself or herself or for a third person, which means that e.g. the mere passing on of a secret without the intent to obtain an advantage is not punishable. The offender must also be aware that the secret was unlawfully obtained for the behavior to be punishable by art. 162 para. 2 Criminal Code.

Industrial espionage (art. 273 Criminal Code)

The field of application of art. 273 of Criminal Code only comprises espionage and breach of secrecy for the purpose of *rendering the secret information accessible to a foreign destination*. Industrial espionage or breach of secrecy for the benefit of a domestic organization is not punishable under art. 273 Criminal Code. However, criminal liability may arise under the UCA.

Industrial espionage cannot be committed by negligence (i.e., it is only punishable when the offender has acted with intent).

Breach of official duties or professional confidentiality (arts. 320 and 321 Criminal Code)

The breach of official duties or professional confidentiality is punishable irrespective of the purpose for which it was committed. The accidental breach of secrecy is not punishable pursuant to these provisions.

Criminal Liability based on the UCA (arts. 4, 5, 6 UCA)

The provisions in the UCA do not establish any requirements as to the purpose that the infringer may necessarily pursue to be charged with violation of trade secrets. However, as the UCA protects fair and undistorted competition, any infringements of the UCA must have an impact on competition. As a consequence, the illicit exploitation of trade secrets, under arts. 4, 5 and 6 UCA, requires use for commercial, not merely private purposes. Use for personal purposes is not covered by these provisions.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

As a general rule, the violation of trade secrets can entail various criminal offenses cumulatively.

First, several provisions regarding the protection of trade secrets can be violated. A certain behavior can, for instance, meet all elements of art. 162 Criminal Code and art.

273 Criminal Code. In such a case, the criminal liability of both provisions is cumulated. Liability according to arts. 320 and 321 of Criminal Code, however, rules out punishment pursuant to art. 162 Criminal Code, but can again be cumulated with liability arising out of violation of art. 273 Criminal Code (for further details, cf. MARC AMSTUTZ/MANI REINERT, Art. 162 StGB, in: Niggli/Wiprächtiger (eds.), Basler Kommentar zum Strafrecht II, 2. ed., Basel 2007, N 29 et seqq.).

The relationship between the provisions of the Criminal Code and the UCA is not fully resolved in legal literature and, to our knowledge, no Supreme Court decisions relevant to that matter exist. For his reason, depending on the specific circumstances of the case, the criminal liabilities under the Criminal Code and the UCA may either be cumulated, or rule one another.

Second, the violation of trade secrets can entail other criminal offenses, not mainly protecting trade secrets. In the case of industrial espionage pursuant to 273 Criminal Code, for instance, the violation of trade secrets can likely entail theft or trespassing. In case of art. 162 Criminal Code, the elements of unauthorized penetration of a secured data system may be fulfilled. The additional criminal liability arising out of such "related" criminal offences can, as a general rule, be cumulated to the respective punishment under the provisions protecting trade secrets.

In additional to the criminal sanction, the owner of the trade secret may hold the offender liable for any damage suffered from the breach of secrecy. A violation of the provisions of Criminal Code (arts. 162, 273 and 321 Criminal Code) and/or the provisions of the UCA allows the infringed party to claim compensation for damages pursuant to art. 41 of the Swiss Code of Obligations,

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "fair use", "just cause", "de minimis threshold")?

Arts. 162, 273, 320 and 321 Criminal Code do not encompass "safe harbor" clauses specific to the acts threatened with punishment such as "fair use", "just cause", or "de minimis threshold".

However, an offender may use the general defenses as stipulated in art. 14 et seqq. Criminal Code, according to which the offender can justify the violation of a criminal law provision in particular in cases of self-defense and for legitimate acts in a situation of necessity.

Besides this, the disclosure of trade secrets can be justified if the disclosing party is legally obliged to render information or to testify in course of criminal proceedings.

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

No, the sole risk of dissemination or disclosure is generally not sufficient to trigger criminal liability under the relevant provisions.

The realization of the infringement (breach of secrecy and/or exploitation of the secret) or at least an attempt with intent to achieve this result (cf. below) is a precondition to criminal liability under said norms. Also, the criminal acts cannot be committed by negligence.

However, in case of attempt, i.e. when the result is not achieved, but the offender acted with knowledge and intent towards the occurrence of the result which is punished by

aforementioned provisions (e.g., a package containing secret information is willfully sent to a third party, but never received by the third party), the offender may still be subject to criminal liability (cf. art. 22 Criminal Code). According to art. 22 of Criminal Code, an offence is attempted if the offender takes steps which will immediately lead to the completion of the offence as envisaged by the offender. Merely preparatory acts, which will not immediately lead to the disclosure or non-authorized use of the trade secret, remain however unpunished.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

The provisions in the Criminal Code as well as the Banking Act protect against the unauthorized disclosure of the trade secrets (cf. arts. 162, 273, 320, 321 Criminal Code, art. 47 Banking Act). Exploitation of the trade secret is not a precondition for criminal liability under these provisions.

To entail liability according to art. 4 lit. c UCA, the trade secret must not even be disclosed. It is sufficient if the offender "induces" the employee, agent or other auxiliary persons to disclose the trade secret. IN other words, the accomplished attempt is sufficient.

Art. 6 UCA, on the other hand, rather focuses on the unauthorized exploitation of trade secrets. While the wording of art. 6 UWG refers to both, exploitation or "disclosure to a third party", the prevailing opinion among legal scholars is that the mere disclosure to any third party is not yet sufficient to fulfill this element. Moreover, the third party must intend to exploit the trade secret, or the disclosure must otherwise harm the secret carrier. Revealing the trade secret to a larger group is considered to harm the secret carrier.

Some of the violations can only be committed by certain professionals who typically act as secret carriers or often get in touch with secret information such as attorneys or accountants, and require that the offender must have obtained the trade secret in course of its official duties or professional activities or responsibilities (e.g., arts. 320, 321 Criminal Code, art. 47 Banking Act). With regard to betrayal of secrets (art. 162 Criminal Code), industrial espionage (art. 273 Criminal Code) or the provisions in the UCA (art. 4 lit. c, art. 5 and art. 6 UCA), the group of persons who may commit the offence is not limited to certain professions but these offenses can be committed by anybody.

Arts. 162 and 273 Criminal Code as well as art. 4 lit. c and 6 UCA use the term "manufacturing or business secret". According to the case law of the Swiss Federal Supreme Court[6],

(1) a secret exists if

   (a) the facts are unknown to the public,
   (b) the owner's interest of secrecy is legitimate and
   (c) the owner actually intends to keep the facts secret and

(2) a secret is considered a "manufacturing or business secret" if it relates to a manufacturing step (e.g. processes, construction plans, etc.) or information relevant to the business (e.g. strategy plans, cost structures, customer data, etc.).

[6] "Object of a secret according to [art. 162 Criminal Code] are all facts relating to a manufacturing step which are neither obvious nor publicly accessible and in the secrecy of which the owner has a legitimate interest and which the owner actually intends to keep secret." (SFSC 80 IV 22, 27 C. 2a).

This definition identically applies to arts. 162, 273. 320, 321 Criminal Code as well as arts. 4 lit. c, 6 UCA identically; however, art. 273 Criminal Code only provides for punishment in case of the dissemination of secrets with a so-called "domestic relation" ("*Binnenbeziehung"*). This means that the manufacturing or business secrets infringed must be subject to Swiss territorial sovereignty or directly concern the Swiss economy, neither of which is satisfied when protection solely of foreign individuals' or corporations' secrets is sought. Cross-border cases, on the other hand, satisfy this requirement as long as Swiss contracting or third parties' interest in confidentiality of business or manufacturing secrets is concerned (cf. THOMAS HOPF, Art. 273 StGB, in: Niggli/Wiprächtiger (eds.), Basler Kommentar zum Strafrecht II, 2. ed., Basel 2007, N 10 et seqq.).

Also, with regard to art. 273 of Criminal Code, information is considered to be secret and not publicly available as long as the information is unknown by the foreign addressees of the information, even if it is widely known in Switzerland (SFSC 104 IV 175, 177). Dissemination of information which is outside the scope of this definition is not punishable under arts. 162 and 273 of Criminal Code.

Arts. 320, 321 of Criminal Code and art. 47 of Banking Act, on the other hand, use the (broader) term "secret". The secret must not be a manufacturing and/or business secret, but it must have been entrusted to the offender in its respective professional capacity.

With regard to arts. 162, 273 of Criminal Code and arts. 4 lit. c, 6 UCA, the criminal liability does not depend on a particular personal quality of the infringer. Contrary to that, personal qualities are the key elements with regard to arts. 320, 321 of Criminal Code and art. 47 of Banking Act. Only the dissemination of secrets entrusted to a party in his professional capacity as for instance officer of a bank or attorney at law, to name just two, is covered by these provisions.

In all cases of trade secret violation sanctioned, the threat of punishment is almost identical: It is up to three years imprisonment or a monetary fine with regard to art. 162, 273, 321 of Criminal Code, art. 47 of Banking Act as well as art. 4 lit. c and 6 UCA, and only in serious cases of industrial espionage under art. 273 Criminal Code there is a minimum sentence of one year.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

Swiss criminal law provisions as well as the intellectual property law provisions (in particular the UCA) mainly use the term "trade and business secrets" and a coherent definition (please see above under A.7.).

The owner of an intellectual work product can use the specific instruments provided by intellectual property law to protect his or her work ("subjective" protection; cf. above A.1.); however, the owner will usually have to disclose the information in order to obtain specific rights (e.g., a patent may only be obtained by full public disclosure of the intellectual work product; copyright exists independently of disclosure, but is not apt to protect a secret, as it only grants the owner a right of exclusivity to the formal presentation in which an idea is "stored" and does not protect its content, i.e. the idea itself, against reproduction or use).

The "objective" protection of trade secrets incorporated by the criminal liability provisions (cf. above A.1.) does not rely on definitions or terms set out by intellectual property law. For instance, trade secrets do not have to patentable in order to profit

from the protection afforded by the criminal law provisions. In other words, trade secret protection afforded by criminal law does not depend on nor is it limited to "subjective" intellectual property rights.

When there is a case of betrayal or exploitation of trade secrets, there is not necessarily also an infringement of intellectual property rights, since there isn't any intellectual property right which protects secrets per se.

According to Art. 23 UCA, deliberate infringements of arts. 4, 5 and 6 UCA constitute criminal offenses.

If the requirements of these provisions are not fulfilled, the specific way of using a trade secret may still fall under the general clause of art. 2 UCA. This, however, requires special circumstances of the disclosure or exploitation of the trade secret. An infringement of the general clause of art. 2 UCA, however, does not trigger criminal liability.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

No. The core provisions which provide for criminal protection of trade secrets in Switzerland – arts. 162, 273 of Criminal Code and arts. 4 lit. c, 6 UCA – correspondingly use the term "trade and business secrets". Statutory Swiss law does not provide for a general definition of trade secrets, however case law set forth different criteria (see above under A. 7.) As long as these cumulative requirements are met, there is no limitation as to the items of the information protected as trade and business secret.

The protection of trade secrets provided by criminal law also applies regardless of the form in which the secret knowledge is stored.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

Trade secrets have to be within the definition provided under section A.7 above be protected under criminal law. As discussed in sections A.7 and A.8. above, the notion of manufacturing and business secrets according to criminal law is not dependent on intellectual property rights and includes patentable knowledge (e.g. formulas, construction plans etc.) as well as knowledge which is not patentable (e.g. manufacturing steps lacking novelty, customer lists, budget plans, etc.).

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Infringement of intellectual property rights such as patens, trademarks, designs and copyrights is generally subject to criminal liability if committed intentionally.

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

Violations of arts. 162, 321 Criminal Code and arts. 23, 4, 5, 6 UCA are *not* subject to prosecution *ex officio*, i.e. the violation is only prosecuted upon the request of the owner of the secret (regardless of whether the owner of the secret is a natural person or corporate entity).

Criminal acts, pursuant to art. 273 of Criminal Code, are prosecuted by the Federal Prosecutor. Even though the wording of the provision provides for prosecution *ex officio*, legal scholars suggest the prosecutor should not act unless the owner of the secret prompts and supports the investigation (cf. THOMAS HOPF, Art. 273 StGB, in: Niggli/Wiprächtiger (eds.), Basler Kommentar zum Strafrecht II, 2. ed., Basel 2007, N 25). This is motivated by practical reasons, and has never been explicitly confirmed by the Swiss Federal Criminal or Supreme Courts. Therefore, even if such a practice may imply that the request of the owner of the secret is a *de facto* precondition for prosecution, the Federal Prosecutor may always act *ex officio*, as art. 273 Criminal Code aims at protecting state and not private interests and falls under the category of "Felonies against the State and National Security".

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

No. As is generally the case in criminal trials in Switzerland, the court is free to interpret evidence in accordance with the views that it forms over the entire proceedings (cf. art. 10 para. 2 CPC). In order to establish the truth, the criminal justice authorities shall use all the legally admissible evidence that is relevant (art. 139 para. 1 CPC). The forms in which the evidence may appear are not limited.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

The prosecuting authority may, under certain preconditions, obtain a warrant to search premises, computer systems, etc.

However, the prosecutor is generally independent from *ex parte* petitions. Once the owner of the secret requests prosecution, the prosecutor administers the proceedings without depending on the owner's further petitions or orders.

To secure evidence, the prosecuting authority may, according to the general principles of admissibility of compulsory measures in criminal proceedings (cf. art. 196 et seqq. CPC), order searches (art. 241 et seqq. CPC) and/or seizures (art. 263 et seqq. CPC) under following general conditions:

- reasonable suspicion that an offence has been committed;
- the aim (i.e. the collection of evidence) cannot be achieved by less stringent measures;
- the seriousness of the offence justifies the search or seizure (proportionality principle).

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Yes, if the criminal act cannot be attributed to an individual due to deficiencies in the company's organization.

Art. 102 Criminal Code is classified under the Section "Corporate Criminal Liability" and states the following:

Art. 102 Strafbarkeit

[1] Wird in einem Unternehmen in Ausübung geschäftlicher Verrichtung im Rahmen des Unternehmenszwecks ein Verbrechen oder Vergehen begangen und kann diese Tat wegen mangelhafter Organisation des Unternehmens keiner bestimmten natürlichen Person zugerechnet werden, so wird das Verbrechen oder Vergehen dem Unternehmen zugerechnet. In diesem Fall wird das Unternehmen mit Busse bis zu 5 Millionen Franken bestraft.

(…)

[3] Das Gericht bemisst die Busse insbesondere nach der Schwere der Tat und der Schwere des Organisationsmangels und des angerichteten Schadens sowie nach der wirtschaftlichen Leistungsfähigkeit des Unternehmens.

[4] Als Unternehmen im Sinne dieses Titels gelten:
a. juristische Personen des Privatrechts;
b. juristische Personen des öffentlichen Rechts mit Ausnahme der Gebietskörperschaften;
c. Gesellschaften;
d. Einzelfirmen.

Art. 102 Punissabilité

[1] Un crime ou un délit qui est commis au sein d'une entreprise dans l'exercice d'activités commerciales conformes à ses buts est imputé à l'entreprise s'il ne peut être imputé à aucune personne physique déterminée en raison du manque d'organisation de l'entreprise. Dans ce cas, l'entreprise est punie d'une amende de cinq millions de francs au plus.

(…)

[3] Le juge fixe l'amende en particulier d'après la gravité de l'infraction, du manque d'organisation et du dommage causé, et d'après la capacité économique de l'entreprise.

[4] Sont des entreprises au sens du présent titre:

a. les personnes morales de droit privé;
b. les personnes morales de droit public, à l'exception des corporations territoriales;
c. les sociétés;
d. les entreprises en raison individuelle.

Art. 102 Punibilità

[1] Se in un'impresa, nell'esercizio di attività commerciali conformi allo scopo imprenditoriale, è commesso un crimine o un delitto che, per carente organizzazione interna, non può essere ascritto a una persona fisica determinata, il crimine o il delitto

è ascritto all'impresa. In questo caso l'impresa è punita con la multa fino a cinque milioni di franchi.

(…)

[3] Il giudice determina la multa in particolare in funzione della gravità del reato, della gravità delle lacune organizzative e del danno provocato, nonché della capacità economica dell'impresa.

[4] Sono considerate imprese ai sensi del presente articolo:
a. le persone giuridiche di diritto privato;
b. le persone giuridiche di diritto pubblico, eccettuati gli enti territoriali;
c. le società;
d. le ditte individuali.

Art. 102[7] Liability under the criminal law

[1] If a felony or misdemeanor is committed in an undertaking in the exercise of commercial activities in accordance with the objects of the undertaking and if it is not possible to attribute this act to any specific natural person due to the inadequate organization of the undertaking, then the felony or misdemeanor shall be attributed to the undertaking. In such cases, the undertaking shall be liable to a fine not exceeding 5 million francs.

(…)

[3] The court shall assess the fine in particular in accordance with the seriousness of the offence, the seriousness of the organizational inadequacies and of the loss or damage caused, and based on the economic ability of the undertaking to pay the fine.

[4] Undertakings within the meaning of this title are:

a. any legal entity under private law;
b. any legal entity under public law with exception of local authorities;
c. companies;
d. sole proprietorships.

Criminal liabilities of corporate entities only extend to felonies (offences which carry a custodial sentence of more than three years) and misdemeanors (offences which carry a custodial sentence not exceeding three years or a monetary penalty).

Therefore, a company might, for instance, be held liable for the exploitation of trade secrets according to art. 162 of Criminal Code.

Note, however, that criminal liability of corporate entities arises rather rarely in practice as the field of application of art. 102 para. 1 of Criminal Code is rather narrow.

2. If so, which type of liability arises for companies? Which penalties shall apply?

See art. 102 para. 1 of Criminal Code: The company would be liable to a fine not exceeding 5 million Swiss francs (amounting to approx. EUR 4.1m).

3. Which court may adjudicate cases of liability of companies for such trade secrets violations*?*

There is no jurisdiction particular to criminal proceedings against corporations. Cases against corporate entities will be adjudicated by the same courts which would decide cases against individuals.

[7] Unofficial translation, cf. http://www.admin.ch/ch/e/rs/311_0/a102.html.

Follow-up questions

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees.

As discussed in this section A.7 above, the owner's intent to keep the information secret is a constituting element of a trade secret. According to case law, the intent to keep the information secret must be *externally perceivable* (i.e. not only present in the mind of the secret owner; SFSC 103 IV 283). This view is contested by legal authors (for further details see MARC AMSTUTZ/MANI REINERT, Art. 162 StGB, in: Niggli/Wiprächtiger (eds.), Basler Kommentar zum Strafrecht II, 2. ed., Basel 2007, N 14).

A specific obligation or agreement between the offender and the secret carrier is required under art. 162 Criminal Code, as the secret must be under a statutory or contractual duty not to disclose. No such requirement exists under art. 273 Criminal Code, 4 lit. c, 5 and 6 UCA.

As to the status of an employee, the Swiss criminal law provisions regarding protection of trade secrets do not distinguish between employees and other secret carriers (please note, however, that art. 321a para 1 and para 4 Swiss Code of Obligations govern disclosure of trade secrets by employees during and after the term of the employment agreement; please see the IP & Commercial Law Questionnaire, A.2.). If the offender is an employee, he is however likely under a contractual obligation not to disclose, so that in case of disclosure of trade secrets the requirements set forth by art. 162 Criminal Code are likely met.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

With regard to criminal liability under arts. 162, 273, 320 and 321 Criminal Code, the offender does not have to qualify as competitor or potential competitor. The provisions in the Swiss Criminal Code instead concentrate on the *target course* of the violation: While with regard to art. 162 para. 1 and art. 321 Criminal Code secrecy must be only violated (and no particular purpose is required), art. 162 para. 2 Criminal Code is only fulfilled if the trade secret is disclosed *for the benefit of the offender or a third person* (regardless of whether the offender or the third party is a competitor or potential competitor of the owner of the secret). Art. 273 Criminal Code sets forth that the espionage must be carried out *for the benefit of a foreign organisation* (again, it is not relevant whether this organization is a competitor).

As far as arts. 4 lit. c, 5 and 6 UCA are concerned, the offender must not be a direct competitor of the secret carrier, however he must intend to use the trade secret for commercial purposes.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

Yes. The aggrieved person can initiate an adhesion claim ("*Adhäsionsklage"*), i.e. claim damages within the framework of the criminal proceedings (cf. art. 39 of the Code on Civil Procedure; arts. 118 et seqq. Criminal Procedure Code ["CPC"]). In such case, the civil lawsuit is incorporated into the criminal proceedings, meaning that the court competent for the criminal proceedings will also be competent for the civil claim. The

aggrieved person is not entitled to institute civil legal proceedings with two different courts, i.e. the claimant has to decide whether to bring forward an adhesion claim, or initiate separate civil proceedings. Once the claimant has opted for either option, he cannot revert to the other option, as the civil claim is *lis pendens*.

The United Kingdom

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

There is no criminal liability per se for trade secrets violation in the UK, however there are a number separate legislative and common law regimes which afford some criminal law protection for trade secrets. This limited criminal protection is achieved through the following legal avenues:

1.1 Theft

The primary legislation in the UK governing theft is the Theft Act 1968[1]. Section 1 of the Theft Act protects from the dishonest appropriation of property belonging to another where there is an intention to permanently deprive. In the leading case in this area *Oxford v Moss (1979)*[2], it was held in that, although intangible information falls within the definition of property in the Theft Act (section 4(1)), information does not constitute intangible property for the purposes of the section 4(1)[3] definition. This was reiterated in *R v Absolom*[4] where the taking of data specifying where oil could be found was held to be something which could not form the basis of a theft charge. Please also see our response to question 4 of the Intellectual Property and Commercial Law questionnaire for information of the nature and treatment of trade secrets as intellectual property rights.

Furthermore, where information is "stolen" it will be hard to fulfil the requirement to intend to permanently deprive (which is necessary to successfully bring a claim for theft). Firstly, in many cases the material on which the information is recorded will not be stolen, therefore there is no *deprivation* of the property. Secondly, where information is taken, copied and then returned, the intention to *permanently* deprive is absent.

Therefore there can be no claim for the theft of the confidential information or trade secrets themselves. However, where the material on which the information is transcribed is stolen there will be a claim (provided that the relevant elements in section 1 of the Theft Act are met). Whilst offering some protection, in practice a theft claim for the material on which the information is contained (which could be for example, a piece of paper or a USB stick) would therefore be for a relatively low value, and would not reflect the theft of the information.

The penalty for theft is up to seven years imprisonment. However for a low value claim (for example, for theft of a USB stick) imprisonment is unlikely.

1.2 Fraud

The Fraud Act 2006[5] contains three criminal actions which may be applicable when confidential information or trade secrets have been stolen:

[1] http://www.legislation.gov.uk/ukpga/1968/60/contents
[2] (1979) 68 Cr. App. R. 183 (High Court)
[3] In Oxford v Moss a student who obtained and then returned an exam paper (retaining the information for his use in the exam) was found to be not guilty of theft of the information.
[4] The Times, 14 September 1983
[5] http://www.legislation.gov.uk/ukpga/2006/35

a) fraud by false misrepresentation;
b) fraud by failing to disclose information; and
c) fraud by abuse of position[6].

These three offences are committed where a gain is obtained, or a loss is suffered by another, as a result of (i) a dishonest false misrepresentation, (ii) a dishonest failure to disclose (where legally required to disclose), or (iii) an abuse of a position. This gain or loss need not be permanent and can be a gain or loss of intangible property[7].

The penalties for these three fraud offences are up to ten years imprisonment, a fine, or both. For summary (less-serious) offences the maximum fine is capped at £5,000. Where the offence is more serious (which is likely in the case of a trade secrets violation), an unlimited fine can be applied.

1.3 Conspiracy to defraud

Under the common law, it is an offence to conspire to defraud. This offence is committed where two or more people agree to defraud another. "Fraud" is widely interpreted and includes, inter alia, dishonestly injuring a person's proprietary rights[8]. A clear drawback here is the necessary requirement for collusion between two people; a conspiracy to defraud cannot be committed by a single person.

1.4 The Computer Misuse Act

It is an offence under section 1 of the Computer Misuse Act 1990[9] to gain unauthorised access to information contained on a computer. To commit the offence, the person must know at the time of accessing the computer data that they are unauthorised to do so.

The leading UK court case has confirmed that the analysis as to whether a person is authorised to access information should not be based on the restrictions placed on the type of data but rather whether the information access was within the authority of the individual[10]. The authorisation relates to a particular programme/computer as opposed to the information itself. A person will have the authority to access information where that person has the ability to control access to the data. If the person is not able to control access but they have the authority from person who does they will be authorised. Therefore, if the person neither has the ability to control access nor the permission to access from the person who controls access the access will be unauthorised and an offence will be committed.

The penalties for breach of the Computer Misuse Act are up to two years imprisonment, a fine, or both. Where the offence is serious an unlimited fine can be applied. For less-serious breaches the maximum fine is £5,000.

1.5 The Data Protection Act

Under the Data Protection Act 1984[11] those holding personal data relating to an

[6] Sections 2,3,4 of the Fraud Act 2006, respectively
[7] Section 5 Fraud Act 2006
[8] Scott v Commissioner of Police of the Metropolis (1975) AC 819; (House of Lords); http://www.bailii.org/uk/cases/UKHL/1974/4.html
[9] http://www.legislation.gov.uk/ukpga/1990/18/contents
[10] R v Bow Street Stipendiary Magistrates, ex p Government of the United States of America (No 2) (1999) 3 WLR 620; (House of Lords, now called the Supreme Court)
[11] http://www.legislation.gov.uk/ukpga/1998/29/contents

individual on a computer must put certain prescribed safeguards into place in order to protect the data. It is a criminal offence to ignore or abuse these safeguards punishable by fine of up to £5,000 where the offence is less-serious or an unlimited fine where the offence is serious.

Personal data means any data relating to living individuals where the individual can be identified from the data (or from the data and other information which the person holding the data may come into contact with). Whilst this definition is seemingly quite wide, it will be very rare for a trade secret or confidential information to fall within the definition (and accordingly the protection of the Data Protection Act) as trade secrets are unlikely to be personal data in most circumstances.

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

No, as there is no specific UK criminal legislation protection for trade secrets there is no requirement for infringers of trade secrets to pursue certain purposes. However, in the case of theft, the infringer must intend to permanently deprive.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

See question A1 above for a list of general criminal offences which may be triggered for trade secret violations.

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "fair use", "just cause", "de minimis threshold")?

No, there are no exceptions or safe harbours which specifically apply in relation to the abuse of trade secrets.

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

No. For the limited criminal offences to occur there must be a positive criminal act. The threat of using information would not trigger criminal sanctions.

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

There is no different classification of the types of trade secrets violation in the UK.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

As set out in the responses to the questions on the Intellectual Property and Commercial law questionnaire, trade secrets are protected as a form of confidential information. As such, their protection is based on either (i) contractual protection, or (ii) protection under an equitable duty (where the information is confidential in nature and disclosed in

circumstances where a duty of confidence exists). The protection of trade secrets under English criminal law is however limited as set out in question A1. above. As the criminal protection related to only limited types of offences there will be circumstances where the unauthorised use of trade secrets will constitute a breach of confidential information but will not trigger a criminal offence.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

Criminal law generally does not protect the appropriation of trade secrets per se. As set out in the answer to question A1. above, theft of physical items containing trade secrets may constitute an offence, however the protection of trade secrets as information per se is limited.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

As there is no specific criminal regime governing trade secrets, there is no thresholds for the trade secrets to meet in order for them to be afforded protection.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

Yes, the following intellectual property rights are afforded criminal protection:.

Trade mark: section 92 of the Trade Marks Act 1994[12] contains a number of criminal offences in relation to the unauthorised / counterfeit use of registered trade marks. These offences are committed where a mark is used without the consent of the mark's proprietor. Given that is unlikely that a trade secret or confidential information will be the subject of a trade mark (as doing so would be submitting the mark to a public registered), it is questioned in practice what protection of trade secrets trade mark law will provide.

Copyright: There is some limited criminal protection for copyright. As a result, where trade secrets are obtained in a manner which breaches copyright, the following criminal protection may apply:

Under section 107 of the Copyright Designs and Patents Act 1988[13] it is an offence to (without the consent of the copyright holder) (i) make available for sale or hire, (ii) import into the UK (other than for private use), (iii) possess in the course of business with a view to committing an act infringing copyright, (iv) distribute (otherwise in the course of business) in a manner which is prejudicial to the copyright holder, or (v) in the course of business, sell, hire, offer for sale or hire, publically exhibit or distribute, something which is known, or suspected to infringe copyright.

In section 198 of the Copyright Designs and Patents Act there is an offence of dealing in illicit recordings where, a person without consent (i) makes available for sale or hire, (ii) imports into the UK (other than for private use), (iii) possesses in the course of business with a view to committing an act infringing copyright, (iv) distributes (otherwise in the

[12] http://www.legislation.gov.uk/ukpga/1994/26/contents
[13] http://www.legislation.gov.uk/ukpga/1988/48/body

course of business) in a manner which is prejudicial to the copyright holder, or (v) in the course of business, sells, hires, offers for sale or hire, publically exhibits or distributes, a recording which is or which is suspected to be an illicit recording.

The penalties for breach of sections 107 and 198 of the Copyright Designs and Patents Act are up to ten years imprisonment, a fine, or both.

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

In the UK criminal actions are brought by the Crown Prosecution Service ("CPS") (the public prosecution service). The CPS will make an assessment in each case whether or not to bring a criminal action. The CPS' assessment is twofold; first they will consider whether there is sufficient evidence to bring an action (the evidentiary test), and secondly it will be assessed whether there is a public interest in the prosecution (the public interest test).

Individuals and private organisations can also bring criminal proceedings14 however the CPS have the discretion to take over the litigation (and in some cases, have an obligation to do so - for example where the case is important or difficult). In light of this, and considering that private actions are rare, it is unlikely that criminal proceedings in the UK would be brought for a violation of trade secrets or confidential information other than by the CPS and only in relation to the limited criminal actions as set out in the response to question A1. above.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

No. Given that there is no stand alone legislative regime protecting trade secrets, there are no specific evidentiary rules in relation to the bringing evidence in court for a violation or theft of trade secrets. However, depending on which criminal cause of action is used, (for a list of potential actions see question A.1 above) different evidentiary burdens will apply. For example, in the case of theft it must be shown : (i) that there was an appropriation (taking) of property (i.e. physical property such as a piece of paper or memory stick), (ii) that the property belonged to another person, and (iii) that the person taking the property had the intention to "permanently deprive" its owner of the property.

The standard of proof applied in all criminal cases is that it is "beyond reasonable doubt" that the offence has been committed. This is distinct from the civil standard of proof, where it must generally be shown that it is more likely than not that a breach has occurred. This means that for a person to be guilty of a criminal offence in the UK the judge or jury must be near certain that the accused committed the criminal act. In addition, given that the offences set out in question A.1 above all require a specific mental state, (i.e. for theft the intention to permanently deprive) it will be more difficult to prove that a person is guilty. Where an offence is strict liability (there is no requirement to show a mental state) it is easier to prove that the criminal conduct occurred as evidence only needs to be adduced to show that the conduct took place.

[14] Section 6 Prosecution of Offences Act 1985
http://www.legislation.gov.uk/ukpga/1985/23/section/6

However, the criminal offences relating to trade secrets general require a mental element. Where the mental state of an individual must be proved, there will need to be clear evidence of the accused's subjective mental state.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

No, owners of trade secrets or confidential information cannot apply for such orders. It is only under civil law that an individual can apply for a search order (please refer to the response to question B(3) on the Commercial and IP law questionnaire for further details).

Where the police have a suspicion of criminal behaviour they can apply to court for an order to search premises[15]. Such orders will only be granted where there are reasonable grounds for believing that a serious offence has been committed and that there is no other way to obtain the information (for example, by obtaining consent). Police can only enter premises without a warrant in "serious" circumstances (for example to recapture someone who has escaped from custody, to save a life, or to deal with a breach of the peace)[16]. Where the police have made an arrest for a serious offence, they may enter premises to search for evidence where they believe that there evidence relating to the offence or if there is evidence relating to another serious offence[17].

Given that the potential criminal offences which may apply to trade secret violations as set out in section A1. are generally non-serious, it is unlikely that a police warrant to search premises for trade secret violations would be granted. In terms of police searches without a warrant, it is hard to perceive where such an action could ever be justified.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

In the UK companies have separate legal personalities and as a result are capable of being prosecuted for criminal acts. However, given that a company cannot be sent to prison, a company cannot be found guilty of an offence where the only sentence is prison. There are a number of areas where there is specific UK legislation creating criminal liability for companies (for example, corporate manslaughter under the Corporate Manslaughter and Corporate Homicide Act 2007). However, no such specific

[15] Section 8 Police and Criminal Evidence Act, http://www.legislation.gov.uk/ukpga/1984/60/section/8
[16] Section 17 Police and Criminal Evidence Act, http://www.legislation.gov.uk/ukpga/1984/60/part/II/crossheading/entry-and-search-without-search-warrant
[17] Section 18 Police and Criminal Evidence Act, http://www.legislation.gov.uk/ukpga/1984/60/section/18

legislative regimes apply to the criminal offences relating to trade secrets (as set out in question A1. above). Therefore, a company can only be guilty of one of the criminal offences set out in question A1. under the common law where (i) it is liable as a result of the indemnification principle or, (ii) it is vicariously liable for an act of its employee/agent.

A company will be liable for an offence under the indemnification principle where an offence is committed in the course of a company's business by a person who is a "controlling mind" of the company. In such a situation the act and mental state of the individual will be considered to be the act and intent of the company. Whether a person has the sufficient seniority to be considered the controlling mind of the company will depend on the circumstances[18]. A person will not constitute the controlling mind simply because they are a manager or executive. Therefore the individual involved will need to hold a very senior position at the company, and in general it will only be where the managing director or board of directors are involved that the company is held to be liable.

A company will be vicarious liability for the acts of its employees where the individual themselves would usually be liable[19]. In general, vicarious liability will apply where an employee is acting in the course of his or her employment. However, an employer will not be criminally liable for an offence committed by an employee where the employer has not aided, abetted, counseled or procured the offence[20].

For a company to be guilty of conspiracy (for example conspiracy to defraud, as set out in question A1.3 above) there must be two other human conspirators at least one of whom must be an officer of the company who is acting without the bounds of his or her authority.

2. If so, which type of liability arises for companies? Which penalties shall apply?

As a company cannot be sent to prison, the liabilities for the offences set out in question A1. are fines.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

In the UK Companies can be guilty of civil and criminal offences and can be fined in the relevant court in which the proceedings are brought, which will vary depending on the seriousness of the offence or the appeal stage of the litigation. Criminal offences relating to trade secrets violations are likely to be heard in the Magistrates Court or the Crown Court.

<u>Follow-up questions</u>

1. Has a specific obligation to keep secret the information to be expressed for a trade secret violation to occur? Please specify the possible distinction in this respect, if any, between employees of the company owning the secret and any other persons other than employees?

As set out in our previous response, there is no specific criminal legislation that expressly prevents the violation of trade secrets although a breach of a trade secret may

[18] Tesco Supermarkets Ltd v Nattrass (1972) AC 153; (House of Lords, now called the Supreme Court) http://www.bailii.org/uk/cases/UKHL/1971/1.html
[19] Mousell Bros Ltd v London and North Western Railway Co (1917) 2 KB 836; (High Court)
[20] R v Huggins (1730) 2 Ld Raym 1574; (High Court)

fall within other criminal provisions, such as the Theft Act 1968 and the Fraud Act 2006 depending upon the circumstances of the breach. A theft of an object containing information can constitute a theft whether or not that information has been expressly specified as being confidential or a trade secret. The breach relates to the taking of the object itself and not the information contained on it.

2. Has the offender to qualify as a competitor or potential competitor of the owner of the disclosed trade secret?

As above, the criminal provisions under English law do not expressly prevent a violation of a trade secret and therefore the status of a person breaching the Theft Act or Fraud Act (whether they be a competitor or potential competitor of the owner of a trade secret) is not relevant.

3. May the aggrieved person, in the course of a criminal proceeding, bring a claim for damages? If so, what are the consequences of such a claim with respect to the ongoing civil lawsuit for compensation?

Criminal Compensation Orders

Criminal compensation orders are administered under sections 130-133 of the Powers of Criminal Courts (Sentencing) Act 2000 (PCC(S)A).

Section 130(a) states that a court may make a compensation order requiring a convicted person to 'pay compensation for any personal injury, loss or damage' resulting from an offence. This will be 'of such amount as the court considers appropriate, having regard to any evidence and to any representations that are made by or on behalf of the accused or the prosecutor' - section 130(4).

Note that section 131(1) caps the maximum compensation order issued by a magistrates' court at £5000 although in the Crown Court the amount of compensation that can be claimed is unlimited.

While not expressly provided for under criminal legislation, criminal compensation may be sought for offences relating to stolen trade secrets, such as under the Theft Act 1968 and Fraud Act 2006 . However, as addressed above at Section A - Question 1, damages for such offences are unlikely to be substantial as, in respect of theft, they will provide compensation only for the stolen object carrying the trade secret (ie a USB stick) (as opposed to the nature of the information which it contains), and in respect of fraud will only relate to the loss suffered due to the fraudulent activity. In both cases it is unlikely that this will be based upon the value of the trade secret which may have been breached as a result of the theft/fraud.

Section 130(5) of the Act specifies that where the stolen property is recovered, in the case of an offence under the Theft Act 1968 or Fraud Act 2006, any damage to the property while out of the owner's possession shall be treated as 'having resulted from the offence, however and by whomever the damage was caused'.

Subject to sections 148-149 of the PCC(S)A, the Court may also issue a restitution order relating to stolen goods. Thus, where the offender is convicted of stolen goods, the court may order the restitution of those goods or the plaintiff's recovery of a 'sum not exceeding the value of the stolen goods' from the convicted offender. "Stolen" will be in accordance with theft defined under section 1(1) of the Theft Act 1968.

The *Sentencing for Fraud - Statutory Offences* Guidelines, issued under s170(9) of the Criminal Justice Act 2003, also provide useful guidance. Section 54 states that 'where it is difficult to ascertain the full amount of loss suffered by the victim, consideration should be given to making a compensation order for an amount representing the agreed or likely loss '.

Relationship with Civil Damages

Section 134 of the PCC(S)A examines the effect of the criminal compensation order on a 'subsequent award of damages in civil proceedings'. It states that such a criminal order will not affect the assessment of damages in civil proceedings. However, it specifies that the plaintiff may only recover an amount equal to the aggregate of 'any amount by which they exceed the compensation' and 'a sum equal to any portion of the compensation which he fails to recover' (section 130(2)(a)-(b)).

United States

The legal system in the United States comprises two general levels of law: US federal law governing the United States as a whole and the laws of the separate states (the "States"), the District of Columbia ("DC"), and self-governing US territories (the "Territories"). US federal law governs areas that, under the US Constitution, Congress is authorized to regulate. Other areas are left to regulation by the states. While Congress enacted some laws related to trade secrets, it has not enacted any legislation regulating trade secrets in the United States. Thus, trade secrets and the protection of confidential information are in general governed by each State, DC, and each Territory.

In 1979, the National Conference of Commissioners on Uniform State Laws (the "NCCUSL") proposed a uniform law on trade secrets, the Uniform Trade Secrets Act (the "UTSA"). The UTSA does not have the force of law but was proposed by the NCCUSL for adoption by the States, DC, and the Territories. In 1985, the NCCUSL amended the UTSA. Since then, almost all States, DC, Puerto Rico, and the US Virgin Islands have adopted the UTSA. At this time, the States of Massachusetts, New York, North Carolina, and Texas have not enacted the UTSA, although a bill for adoption of the UTSA was introduced this year in Massachusetts. Since the UTSA has the force of law only through positive enactment, the enacted versions of the UTSA in the various States, DC, and Territories may differ. In addition, since interpretation of the UTSA adopted by a State, DC, or a Territory is generally the province of the local courts, the interpretation of provisions of the enacted versions of the UTSA, even if they are identical or similar, may vary among the States, DC, and the Territories.

A survey and discussion of trade secret law in each of the fifty states, the various territories, and the District of Columbia is beyond the scope of the questionnaires. Thus, the responses to the questionnaires analyze trade secret law from the perspective of the States that may be deemed most significant economically for most international businesses: the UTSA (identifying differences thereto as adopted by California and Illinois, if applicable), New York, and Texas.

A. APPLICABLE REGULATORY FRAMEWORK

1. Is there criminal liability for trade secrets violation in your jurisdiction? If so, indicate its general nature, the potential penalties and the legal values protected under the relevant legal framework. To be more specific and have more details, please provide a list of the relevant literature on the matter.

Criminality of trade secret misappropriation is a matter of the law of the individual States. Some States have enacted specific statutes prohibiting the theft of trade secrets, such as California and Texas, while others amended their existing larceny statutes to include trade secrets, such as New York. In addition, U.S. federal law includes a trade secret theft statute.

California: California's criminal statute related to trade secrets covers a number of activities:

> Every person is guilty of theft who, with intent to deprive or withhold the control of a trade secret from its owner, or with an intent to appropriate a trade secret to his or her own use or to the use of another, does any of the following:
>
> (1) Steals, takes, carries away, or uses without authorization, a trade secret.
>
> (2) Fraudulently appropriates any article representing a trade secret entrusted to him or her.

> (3) Having unlawfully obtained access to the article, without authority makes or causes to be made a copy of any article representing a trade secret.
>
> (4) Having obtained access to the article through a relationship of trust and confidence, without authority and in breach of the obligations created by that relationship, makes or causes to be made, directly from and in the presence of the article, a copy of any article representing a trade secret.

Cal. Pen. Code § 499c(b). Trade secret is defined in the statute, but the definition is identical to the one in California's enactment of the UTSA. *See* Commercial and IP Law Questionnaire, question A.1. Violation of Section 499c(b) is theft and punishable as grand theft or petty theft. Cal. Pen. Code § 486. In the case of Section 499c(b), the distinction largely depends on whether trade secrets are personal property, and if so, whether the value thereof exceeds US$950. Cal. Pen. Code § 487. If so, a violation of Section 499c(b) constitutes grand theft and is punishable by imprisonment in county jail not exceeding one year and potentially a fine not exceeding US$1,000. Cal. Pen. Code §§ 489(b), 672. If not, a violation of Section 499c(b) is petty theft and punishable by a fine not exceeding US$1,000 and/or imprisonment in a county jail not exceeding six months. Cal. Pen. Code § 490. As discussed in response to question A.4 in the Commercial and IP Law Questionnaire, it is likely that trade secrets are deemed personal property in California. Thus, it is also likely that a violation of Section 499c(b) would be grand theft if the trade secrets' value exceeds US$950, which may likely be the case.

Individuals as well as corporations are persons liable for a crime. Cal Penal Code §§ 7, 26. In the event that a crime is punishable by imprisonment, such as Section 499c(b) or (c), the corporation may be fined. *People v. Charter Thrift & Loan*, 106 Cal. Rptr. 364, 365-66 (Cal. App. 2d Dist. 1973) (holding that "Section 672 of the Penal Code permits a corporation, convicted of grand theft, to be fined … whether or not, were the defendant an individual, an actual or potential term of imprisonment would be a prerequisite for the imposition of a fine").

In addition, the statute penalizes inducement of trade secret theft:

> Every person who promises, offers or gives, or conspires to promise or offer to give, to any present or former agent, employee or servant of another, a benefit as an inducement, bribe or reward for conveying, delivering or otherwise making available an article representing a trade secret owned by his or her present or former principal, employer or master, to any person not authorized by the owner to receive or acquire the trade secret and every present or former agent, employee, or servant, who solicits, accepts, receives or takes a benefit as an inducement, bribe or reward for conveying, delivering or otherwise making available an article representing a trade secret owned by his or her present or former principal, employer or master, to any person not authorized by the owner to receive or acquire the trade secret, shall be punished by imprisonment in a county jail not exceeding one year, or by imprisonment pursuant to subdivision (h) of Section 1170,[1] or by a fine not exceeding five thousand dollars ($5,000), or by both that fine and imprisonment.

Cal. Pen. Code § 499c(c).

New York: New York's larceny statute penalizes the larceny of "secret scientific material." N.Y. Pen. Law § 155.30(3). Secret scientific material is defined as:

[1] Cal. Pen. Code § 1170(h) sets forth enhanced punishment for felonies and repeat offenders.

> a sample, culture, microorganism, specimen, record, recording, document, drawing or any other article, material, device or substance which constitutes, represents, evidences, reflects, or records a scientific or technical process, invention or formula or any part or phase thereof, and which is not, and is not intended to be, available to anyone other than the person or persons rightfully in possession thereof or selected persons having access thereto with his or their consent, and when it accords or may accord such rightful possessors an advantage over competitors or other persons who do not have knowledge or the benefit thereof.

N.Y. Pen. Law § 155.00(6). Thus, the statute is arguably limited to theft of secret scientific tangible items. In addition, New York law prohibits:

> unlawful use of secret scientific material when, with intent to appropriate to himself or another the use of secret scientific material, and having no right to do so and no reasonable ground to believe that he has such right, he makes a tangible reproduction or representation of such secret scientific material by means of writing, photographing, drawing, mechanically or electronically reproducing or recording such secret scientific material.

N.Y. Pen. Law § 165.07. The term "appropriate" is defined as:

> (a) to exercise control over it, or to aid a third person to exercise control over it, permanently or for so extended a period or under such circumstances as to acquire the major portion of its economic value or benefit, or (b) to dispose of the property for the benefit of oneself or a third person.

N.Y. Pen. Law § 155.00(4). Since this definition is broader than the theft of a tangible item, it can be argued that the misappropriation of intangible knowledge is covered by Section 165.07. The punishment for a crime under Section 155.30(3) and the punishment for a crime under Section 165.07 is each not less than one year and not more than four years. N.Y. Pen. Law §§ 70.00(2)(e), (3)(b), 155.30, 165.07. A fine of not exceeding the greater of US$5,000 or double the amount of defendant's gaim from the commission of the crime may be imposed. N.Y. Pen. Law §§ 80.00(1), 155.30, 164.07. If the defendant is a corporation, a fine not exceeding the greater of US$10,000 or double the amount of defendant's gaim from the commission of the crime may be imposed. N.Y. Pen. Law §§ 80.10, 155.30, 165.07.

Texas: Under Texas law, a person is guilty of theft of trade secrets if that person

> without the owner's effective consent, … knowingly:
> (1) steals a trade secret;
> (2) makes a copy of an article representing a trade secret; or
> (3) communicates or transmits a trade secret.

Penal Code § 31.05(b). A trade secret is defined as

> the whole or any part of any scientific or technical information, design, process, procedure, formula, or improvement that has value and that the owner has taken measures to prevent from becoming available to persons other than those selected by the owner to have access for limited purposes.

Penal Code § 31.05(a)(4). The penalty for an individual is imprisonment of not more than 10 years or less than 2 years and/or a fine not to exceed US$10,000. Penal Code

§§ 12.34, 31.05(c). A corporation convicted of this crime is subject to a fine not to exceed US$20,000. Penal Code §§ 12.51(b)(1), 31.05(c). If the corporation gained money or property or caused loss as a result of the trade secret theft, which may often be the case, the fine may be in an amount fixed by the court not to exceed double the amount gained or the loss, whichever is greater. Penal Code § 12.51(c).

U.S. Federal Law: U.S. federal law penalizes the theft of trade secrets related to or in products within interstate or foreign commerce:

> Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly--
>
> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;
>
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
>
> (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
>
> (4) attempts to commit any offense described in paragraphs (1) through (3); or
>
> (5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,
>
> shall ... be fined under this title or imprisoned not more than 10 years, or both.

18 U.S.C. § 1832(a). The fine for an individual is not more than US$250,000. 18 U.S.C. §§ 3559(a)(3), 3571(b)(3). For an organization, the fine is not more than US$5 million. 18 U.S.C. § 1832(b). In addition, the statute includes a prohibition of economic espionage, which essentially involves trade secret theft with the intent or knowledge of benefiting any foreign government, foreign instrumentality, or foreign agent. 18 U.S.C. § 1831(a).

2. Do the relevant provisions establish any requirements as to the purposes that the infringer may necessarily pursue to be charged with violation of trade secrets? If so, has the infringer to pursue a specific purpose set forth by law when committing the offence (e.g. harming competitors, obtaining advantages from the use)?

As described in response to question A.1 above, the criminal statutes mostly do not require a particular purpose, although the criminal conduct has to be with the requisite intent or knowledge. An exception is the crime of economic espionage under 18 U.S.C. § 1831(a) who has as a particular element the intent or knowledge of benefiting a foreign power.

3. May the violation of trade secrets entail other criminal offences or only result in a civil lawsuit?

It is possible that the theft of trade secrets may entail other offenses. The trade secret theft offenses do not replace or preempt all other criminal offenses. For example, if the theft involves breaking and entering, the defendant may also have committed burglary. Or if the defendant provides trade secrets including defense information to a foreign power, the defendant may be guilty of espionage (18 U.S.C. § 794).

4. Do the relevant provisions establish any "safe harbor" clause with respect to the abuse of trade secrets? Are there any specific conditions under which the offender may not be prosecuted (such as the existence of a "fair use", "just cause", "de minimis threshold")?

The specific criminal statutes do not establish any express safe harbors if the elements of the crime are present in the defendant's action. In fact, California law specifically provides that return or intention to return the article that is the object of the trade secret theft is not a defense. Cal. Pen. Code § 499c(d).

5. May the sole risk of dissemination or disclosure of trade secrets give rise to criminal liability?

For a defendant to be guilty of the crimes identified under questions A.1 above, the defendant's act has to meet each of the elements of such crime. As described above, some of the crimes do not require actual dissemination or disclosure, or even the risk thereof. For example, under California's law, unauthorized use or unlawful copying is sufficient criminal conduct if the requisite intent is present. Cal. Pen. Code § 499c(b)(1), (3).

6. Which different types of violations of trade secrets are recognized in your jurisdiction (depending on, for instance, the personal qualities of the infringer or the type of items covered by trade secrets)? How, if at all, are they treated differently by the law?

As described above, different jurisdictions penalize a variety of conduct related to trade secrets.

7. Does the notion of trade secrets for the purposes of criminal law meet the requirements provided for by intellectual property law? Are there any conducts prohibited under intellectual property law (such as dissemination of confidential business information) which do not result in criminal offences?

As can be seen in the provisions described in response to question A.1 above, the definitions of trade secrets under the criminal statutes are identical or similar to trade secrets in the misappropriation of trade secret laws. The exception is New York, which focuses the crime on "secret scientific material," which is somewhat narrower insofar as it is focused on tangible items.

8. Are there any limitations as to the items (i.e. documents, know-how, ideas) covered by legal protection of trade secrets?

As described under question A.1 above, trade secrets are defined largely identical or similarly as trade secrets for civil trade secret misappropriation claims.

9. Have trade secrets to meet certain specific requirements in order to avail themselves of the relevant legal protection? Does the patentability of the items covered by trade secrets impact on the extent of the protection granted by law?

As described under question A.1 above, trade secrets are defined largely identical or similarly as trade secrets for civil trade secret misappropriation claims. Patentability is not a requirement.

10. Does your jurisdiction provide for criminal protection of other IP registered rights (e.g. such as patents, trademarks)?

U.S. federal law penalizes trafficking in counterfeit goods, labels, and documentation, which are trademark related crimes. 18 U.S.C. §§ 2318, 2320. In addition, U.S. federal law penalizes willful copyright infringement that was committed (i) for commercial advantage or private financial gain, or (ii) by reproducing or distributing during any 180-day period one or more copies or phone records of one or more copyrighted works having a total retail value of more than US$1,000, or (iii) by distributing a work prepared for commercial distribution by making the work publicly accessible on a computer network if the defendant knew or should have known that the work was intended for commercial distribution. 17 U.S.C. § 506(a)(1). The punishment is imprisonment and/or a fine that vary in quantity based on the type and degree of such infringement. 18 U.S.C. § 2319. However, none of these crimes necessitate that any trademark that may be subject to the counterfeit goods, labels, or documentation or that any copyright subject to criminal infringement has been registered.

B. CRIMINAL LITIGATION

1. May the offender be prosecuted at the sole initiative of the Public Prosecutor? Otherwise, has the holder of a secret to file a report of the offence with the Public Prosecutor in order to start a proceeding and thus enforce the violation of trade secrets? Are only certain subjects entitled to start a proceeding and/or claim any damages?

The response to this question also depends on State law. Generally, the owner of a trade secret may file a criminal complaint against the defendant. However, the public prosecutor (typically the district attorney) may also investigate *sua sponte* if the agency suspects that a crime has been committed.

2. Is there any specific evidence to be brought before a court in order to prove that an abuse of trade secrets has occurred?

The prosecution of a trade secret theft or other trade secret related crime of a State is subject to the general criminal procedure in effect in such State. This includes the evidentiary rules applicable in criminal proceedings in such State.

3. Defendants misusing trade secrets are often dishonest. May the holder apply for an ex parte order to search premises and computer systems for misappropriated data and to require the Defendant to provide information as to the whereabouts of documents and files containing such data? [in criminal proceedings] May the holder apply for an ex parte order to cease the risk of further consequences arising from the misuse of trade secrets, as well? May the holder ask for a precautionary seizure of the premises and computer systems to avoid the continuation of the offence and the perpetuation of the consequences thereof?

The State prosecuting a trade secret theft or other trade secret related crime has permissible means of search and seizure at its disposal. However, such means or the authority to use such means generally do not extend to private citizens, such as the owner of stolen trade secrets. As described in the Commercial and IP Law Questionnaire, questions B.2 and B.3, the owner may bring a civil suit and seek a preliminary injunction or temporary restraining order as part thereof.

C. CRIMINAL LIABILITY OF CORPORATIONS

1. May companies be liable for trade secrets violations committed by their agents, employees, contractors, consultants or representatives on their behalf or for their advantage?

Generally, companies may be liable for trade secret related crimes committed by their agents acting on behalf of the company.

2. If so, which type of liability arises for companies? Which penalties shall apply?

Companies are subject to the penalties described under the various statutes in response to question A.1 above.

3. Which court may adjudicate cases of liability of companies for such trade secrets violations?

The appropriate court having jurisdiction over trade secret related crimes depends on the prosecuting jurisdiction. Federal crimes are generally pursued through indictment or information against the defendant in a U.S. district court. States would prosecute such crimes under its laws in district or other courts as appropriate under its laws. There is typically not a particular trial court hearing only criminal cases, although in some States, the highest court hearing appeals in criminal cases is separate from the highest court hearing appeals in civil cases (*e.g.*, in Texas).