Security Journal (2020) 33:83–118
https://doi.org/10.1057/s41284-019-00200-x

ORIGINAL ARTICLE

Fighting industrial and economic espionage through criminal law: lessons to be learned from Austria and Switzerland

Cathrine Konopatsch[1,2]

Published online: 30 September 2019
© Springer Nature Limited 2019

Abstract

Empirical figures show that, especially in recent years, the frequency of industrial and economic espionage, and consequently its dangers and negative impact, has increased greatly worldwide. This has impacted not only the individual victims of the infringement of trade secrets, but also the national and global economies at large. This espionage cannot be tackled effectively through uncoordinated, stand-alone-actions of individual countries anymore. Instead, the global community must take a more holistic view and find universally acceptable strategies and standards, looking for best practices through the lens of comparative law. The paper compares and contrasts the legal approaches to the criminalisation of economic and industrial espionage in Switzerland and Austria. It aims to show the similarities and differences and to identify the strengths and weaknesses of each jurisdiction. The results are meant to enrich and to contribute to the discussions regarding efficient and commonly acceptable solutions to fighting economic and industrial espionage.

Keywords Economic espionage · Industrial espionage · White-collar crime · Crime against state interests · Protection of trade secrets · Private prosecutor

Introduction

Industrial and economic espionage is not a new phenomenon, but "in fact it has been around since the dawn of history" (Birmingham Post 2009). However, developments such as globalisation, greater outsourcing activities, longer delivery chains, and the frequent use of information and communication technology have introduced a new

✉ Cathrine Konopatsch
Cathrine.Konopatsch@fernuni.ch

[1] The Swiss Distance University, Brig, Switzerland

[2] The University of Berne, Berne, Switzerland

dynamic to the phenomenon of industrial and economic espionage, which has led to an increase in its frequency, its risks, and its dangers.

Reid (2016, p. 1) even speaks of "an epidemic of economic espionage". Similarly, the German Federal Criminal Police Office recently used a provocative phrase in order to stress that industrial and economic espionage has become a universal threat to all enterprises, irrespective of their size and branch of business, when stating that "rival companies do not sleep, but that they spy" (BKA 2018). There are still countries and enterprises that consider economic and industrial espionage a legitimate means of doing business and which frequently resort to it (Brenner and Crescenzi 2016; Verfassungsschutzbehörden 2014, p. 8; Trim 2002, p. 7; Reid 2016, pp. 26 and 41 et sequ.).

The concept of protecting trade secrets in specific legal provisions has a very long legal tradition in many countries. The significance of the protection of trade secrets stems from the fact that it is functionally related to the impact of innovation in the evolution of national economies and is a determining factor regarding the competitiveness of a country (cf. Directive (EU) 2016/943 recital no. 1 et sequ.). Therefore, in addition to civil remedies, many jurisdictions utilise specific criminal provisions to safeguard trade secrets.

Basically, compared to other legal remedies, criminal provisions have traditionally been considered the harshest measures in terms of restricting individual rights and freedoms in order to combat and prevent illegal conduct. Accordingly, criminal remedies should be the last resort of the legislature and only be applied if other legal or non-legal measures are insufficient (ultima ratio principle). In many European countries, the use of criminal remedies is considered necessary regarding specific forms of infringement of trade secrets. However, due to the lack of a common framework, the criminal protection of trade secrets differs from country to country in Europe (Baker and McKenzie 2013, p. 7; Carl and Kilchling Forthcoming). Until now, the European Union has no competence to harmonise criminal law in the area of economic and industrial espionage on the basis of Article 83(1) TFEU. However, the EU does have the competence to harmonise laws in the area of cybercrime on the basis of Article 83(1) TFEU.

The significantly growing international and cross-border dimensions of industrial and economic espionage pose a new, additional challenge to criminal law. Different terminology and the lack of commonly acceptable strategies and enforceable rules strongly undermine the national attempts to protect trade secrets—last but not least regarding international cooperation and legal assistance (cf. Reid 2016, p. 73; Kilchling and Carl 2016, p. 188; Carl 2017, p. 1317). The need for legal cooperation is well illustrated by two recent cases. The first involved a Chinese researcher based in Switzerland, who is accused by the USA of having stolen trade secrets. The second involved an Austrian employee who had stolen trade secrets from the Austrian subsidy of the AMSC corporate group, which has its headquarters in the USA. In the first case, the Chinese national is imprisoned in Switzerland and is going to be extradited to the US (swissinfo 2019b), whereas in the second case, the Austrian employee was not extradited to the USA, but instead was sentenced to 3 years of imprisonment in Austria (Zirm 2013).

Another problem is that legal assistance proves ineffective in cases where the requested state is involved in or has even initiated the acts of spying (Brenner and Crescenzi 2016; Fidler 2013).

By comparing relevant provisions across jurisdictions, we can critically assess and, if necessary, can optimise national provisions (cf. Jescheck 1981; Eser 1997; Weigend 2012, pp. 262 et sequ.; Kremnitzer 2011, pp. 30 et sequ.). A comparative approach also helps the global criminal law community to facilitate communication, to promote consensus, to identify existing similarities, and to agree on common legal strategies and law enforcement standards (Eser 2017, pp. 39, 61 et sequ.; Delmas-Marty 2003). Due to developments, which can be summarised under the keyword of progressive "internationalisation of law" (Eser 2017, p. 12; Jung 1998, p. 1) in general, and recently also of criminal law, "the call for comparative criminal law" (Eser 2017, p. 12) has probably never been louder (cf. Meyer 2011, pp. 88 et sequ.; Sieber 2006, pp. 79 et sequ.; Jung 2005, p. 3). Criminal law has grown out of its traditional role of being deeply rooted in a country's social mores and cultural preferences, and therefore is no longer largely immune to transnational assimilation and harmonisation. As a consequence, comparative criminal law is no longer a neglected discipline (cf. Heller and Dubber 2011, pp. 1 et sequ.).

Against this background, comparative law can be considered one key element in the global fight against economic and industrial espionage.

This paper shows that both European legislators (on the national and EU level) and individual enterprises are increasingly becoming aware of the dangers and risks of economic and industrial espionage. However, there still is a large research gap, which significantly undermines the legal fight against this phenomenon. The paper's focus lies on exploring the criminal offences of industrial and economic espionage in Austria and Switzerland and through a comparative perspective in outlining similarities and differences regarding the underlying legal concepts and the legal structure of these offences, as well as their procedural framework. It examines the strengths and weaknesses of the Austrian and Swiss criminal offences of economic and industrial espionage and explores whether there is any need for amendment.

Comparing the Austrian and the Swiss offences of industrial and economic espionage is interesting for various different reasons. First, Austria and Switzerland both have a very long tradition of having criminal offences on the books to punish economic and industrial espionage. They are geographic neighbours, comparable in size, are both neutral, and both belong to the civil law tradition. Due to their similarity of being neutral, the Austrian legislature even considered the Swiss criminal offence of economic espionage as a role model for the Austrian provisions in 1965 (Liebscher 1976, p. 272). Both countries are German-speaking, which means that there is no language barrier. Austria has been a member state of the European Union since 1995, and thus the Austrian economy and the Austrian legal order are strongly influenced by the European Union tradition, its policy, and its legislation. In contrast, Switzerland is not a member of the European Union, but it has been a member of the European Free Trade Association since 1995. Switzerland is home to the headquarters of many international companies, and therefore is the geographic base for a large amount of IP rights and trade secrets. Switzerland has been ranked first in the Global Innovation Index for the ninth consecutive year (Global Innovation

Index 2019, S. 19). Due to its position as the world champion regarding innovation, Switzerland is considered a very attractive target for economic and industrial espionage. Austria, in comparison, is ranked 21st in the Global Innovation Index (Global Innovation Index 2019, S. 35).

In order to perform a comparative analysis of the Swiss and Austrian criminal offences of economic and industrial espionage, the national legal frameworks and the jurisprudence of both countries have been examined. A wide variety of sources of information, such as court decisions, surveys, articles, legal journals, and other relevant materials have been studied.

Economic and industrial espionage in Europe: an unacknowledged crisis?…

…Not anymore…

Carl (2017, p. 1315) describes economic and industrial espionage in Europe as an unacknowledged crisis. However, especially over the past few years, the phenomenon of industrial and economic espionage and its related criminal regulations have gained increasing attention from both academics and non-academics—not least in the context of cybercrime (cf. Carl and Kilchling Forthcoming; Husmann 2015, pp. 60 et sequ.; Desai 2018, p. 482).

A recent study launched by the German Federal Ministry of Education and Research called WiSKoS—Economic and Industrial Espionage in Europe—shows that companies' awareness of the dangers and risks linked to economic and industrial espionage has increased strongly over the last few years. However, small and medium-sized enterprises still do not regularly have adequate safeguards in place to counter espionage (cf. Bollhöfer and Jäger 2018, p. 20).

The growing interest paid to economic and industrial espionage is also reflected by the various measures taken by many individual European countries at the national level, including Austria and Switzerland, as well as by the EU.

Austria

In Austria, for example, the Ministry of Interior, in cooperation with other institutions, has published a handbook on economic and industrial espionage (Austrian Ministry of Interior 2011) in order to raise companies' awareness of the dangers of espionage. In mid-2016, the Austrian legislature enacted a new State Protection Act (Federal Law Gazette I no. 2016/5) increasing, inter alia, the powers of the Federal Office of the Protection of the Constitution and Counter Terrorism, which is in charge of assessing dangers concerning national security, including espionage (cf. Salimi 2017, pp. 117 et sequ.; Heiβl 2016, no. 9 et sequ.). In its activity task report for the years 2013–2018, the Austrian government declared that special focus will be given to combating economic and industrial espionage (Austrian Government 2013), p. 87. In the recent governmental programme for 2017–2022, the Austrian government stressed its willingness to re-evaluate, inter alia, criminal offences—such as

industrial and economic espionage—which have an influence on the attractiveness of Austria as a business location (Austrian Government 2017, p. 43).

Switzerland

Similarly, the Swiss legislature enacted a new Federal Intelligence Service Act (Federal Gazette 2015, p. 7211), which has been in force since September 2017. The Act gives more powers to the Federal Intelligence Service, which, inter alia, is in charge of preventing and fighting economic espionage (cf. Isenring and Quiblier 2017, pp. 127 et sequ.; Seiler 2015, pp. 130 et sequ.). The Swiss Federal Intelligence Service has launched a programme called PROPHYLAX, which aims to raise public awareness of economic espionage (Swiss Federal Intelligence Service 2015). The Swiss Federal Intelligence Service offers information on commonly used spying methods and suspicious incidents and gives advice on security measures—not only by publishing the brochure PROPHYLAX, but also by visiting companies and giving presentations and advice on the subject. The Swiss Federal Intelligence Service has also issued a fact sheet on economic espionage (Swiss Federal Intelligence Service 2018). These steps have been triggered last, but not least, by the well-known case of the sale of Swiss bank data to foreign tax authorities (cf. BBC 2010; Miller 2019; NZZ 2010, 2012; Heine 2010/2011, pp. 525 et sequ.; Stratenwerth and Wohlers 2010, pp. 429 et sequ.).

The European Union

Even the European Parliament has acknowledged the need to enact a Directive on the protection of undisclosed know-how and business information (trade secrets) aiming to prevent their unlawful acquisition, use, and disclosure (2016/943, OJ L 157, 15.6.2016). This Directive is an important milestone concerning the legal protection of trade secrets, as prior to 2016 there was no EU legislation regarding uniform standards on the protection of trade secrets in the member states.

Background of the directive In many European countries, the legal protection of business and trade secrets has a long tradition and has developed into a well-established concept (Baker and McKenzie 2013, p. 1; Czapracka 2008, p. 231). However, generally, the national rules governing the protection of business and trade secrets against unlawful acquisition, use, or disclosure have been strongly shaped by the historical, legal, economic, and cultural background of each country and its specific regulatory needs (Baker and McKenzie 2013, p. 1).

Accordingly, the legal protection of business and trade secrets afforded by the European countries varies significantly (European Union Intellectual Property Office 2018, p. 7; Baker and McKenzie 2013, p. 2; Directive (EU) 2016/943 recital no. 6, 8; Ohly 2019, p. 441; Desai 2018, p. 481). The difference regarding the legal protection of trade secrets mirrors the lack of a uniform definition and the various interpretations given to the term ‘trade secrets’ as such (Baker and McKenzie 2013, p. 4; Sosnova 2016, p. 47).

Since the existing national differences amongst member states with respect to the protection of trade secrets has had a negative impact on the internal market (Directive (EU) 2016/943 recital no. 8), the EU introduced a Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use, and disclosure.

Aim and content of the Directive This Directive aims to create uniform standards for the protection of trade secrets within the member states. The EU member states had to comply with the Directive, at the latest, by 9 June 2018 (cf. Article 19 of the Directive). Member states have chosen different ways of implementing the Directive. Austria, for example, has amended its Act against Unfair Competition (Federal Law Gazette I no. 109/2018; Gassauer-Fleissner 2019). In Germany, a new statute came into force on 26 April 2019, called the Act on Trade Secrets or 'Geschäftsgeheimnisgesetz' in German terminology (Federal Law Gazette I p. 466; cf. Dann and Markgraf 2019; Hauck 2019; Ohly 2019; Scherp and Rauhe 2019; Schlund 2018).

The Directive offers minimum requirements, which means that member states may provide for more far-reaching protection of trade secrets (cf. Article 1(1) of the Directive). The Directive does not establish criminal sanctions, but only gives guidance on the civil remedies available to the owner of a trade secret (Directive (EU) 2016/943 recital no. 10; European Commission 2016). However, what is significant—especially in the context of this paper—is that the Directive offers a uniform definition of trade secrets.

In contrast to some member states, such as Austria or Germany, this Directive does not make a distinction between a trade secret and a manufacturing secret, but instead, uses the term 'trade secret' to embrace both categories. The definition used in the Directive corresponds to the definition of the World Trade Organisation Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) in Article 39(2) TRIPS. Article 2(1) of the Directive defines trade secrets as information that is not generally known or readily accessible, that has commercial value because it is a secret, and that has been subject to reasonable steps, under the circumstances, by the person lawfully in control of the information to keep it secret.

Whereas the definition of trade secrets provided for by the EU Directive corresponds to the definition of trade secrets traditionally known by some member states, like Portugal, Romania, the Czech Republic, Bulgaria, or Denmark (cf. European Union Intellectual Property Office 2018; Maaßen 2019, p. 354, fn. 22), for other EU member states, inter alia for Austria and Germany, however, the EU definition varies from the traditional understanding of trade secrets in legal practice. In Austria and Germany, for example, the understanding of trade secrets has basically been traditionally determined by subjective criteria, i.e. the will and the interests of the trade secret's owner to keep some specific pieces of information secret (cf. Baker and McKenzie 2013, p. 57; Köhler 2019, no. 17). In contrast to this, the definition of the Directive relies on objective criteria, inter alia, requiring measures to guarantee confidentiality in order for the information to qualify as a trade secret (cf. Austria p. 3; Busekist and Racky 2018, pp. 136 et sequ.; Trebeck and Schulte-Wissermann 2018, p. 1177; Leister 2019, pp. 75 et sequ.). This means that the legal protection afforded to trade secrets is made dependent on the fact that adequate measures to secure the

secrecy of the information in question had been taken (cf. Klötzer-Assion 2018, pp. 175 et sequ.; Passarge 2018, p. 145; Kary 2018; Midtgaard 2018, p. 792). The mere will of the owner of the secret or of the person having control over the information to keep the information secret is not enough anymore (cf. Bruckmüller and Krückl 2019; Hofmarcher and Kühteubl 2017).

What non-disclosure measures are necessary in order for information to qualify as a trade secret is determined on a case-by-case basis, depending on the circumstances, such as the relevance of the information in question and the person having control over the information (cf. Dann and Markgraf 2019, pp. 1775 et sequ.; Hauck 2019, p. 224; Maaßen 2019, pp. 354 et sequ.; Ohly 2019, p. 444; Köhler 2019, no. 17; Baranowski and Gaβl 2016, p. 2568; Scherp and Rauhe 2019, pp. 23 et sequ.; Hofmarcher 2018a, b, p. 784). For example, one can think of confidentiality agreements and measures of access control, such as password protection, and awareness and education programmes for employees (cf. Ohly 2019, p. 444; Sosnova 2016, pp. 52 et sequ.; Klötzer-Assion 2018; Trebeck and Schulte-Wissermann 2018, p. 1177).

The fact that secrecy protection is made dependent on adequate non-disclosure measures by the person having control over the trade secret is criticised by part of literature as it lays an additional burden on companies, creating the need to document the non-disclosure measures which were taken (Scherp and Rauhe 2019, pp. 23 et sequ.; Gassauer-Fleissner 2018, p. 258). Critics say that it is hard for the owners of the secret to know what measures they need to implement, so that their trade secrets are legally protected (cf. Passarge 2018, p. 145; Leister 2019, pp. 76 et sequ.). Some scholars also argue that enforcement of the law must not be made dependent on which non-disclosure measures the owner of the secret has implemented to secure the secrecy of the information in question (Passarge 2018, pp. 145 et sequ.). Passarge (2018, p. 147) even assumes that creating a definition of trade secrets which requires that the owner to take non-disclosure measures makes industrial espionage easier. Similarly, Voigt et al. (Voigt et al. 2019, p. 143) and Leister (Leister 2019, p. 76) believe that the requirements for the protection of trade secrets are tightened by the guidelines of the Directive.

However, only future practice will show whether the requirement of non-disclosure, i.e. that the person who has control over the information must take measures to protect it, will de facto change the legal protection of trade secrets (dissenting opinion: Leister 2019, p. 76). As already mentioned, the traditional criteria applied by some countries for information to qualify as a trade secret is the will and the interests of the owner of the secret to keep the information secret. Such will and interest can be demonstrated by the non-disclosure measures that were taken by the owner of the secret. In other words, due to their interests and will to keep information secret, most of the owners of the trade secret will have implemented non-disclosure measures of some kind anyway—even without the requirements of the Directive.

In the end, because the Directive allows national courts and authorities much discretion, one must observe how national courts and other authorities apply the criterion of non-disclosure measures.

Even though the Directive does not give any guidance on criminal sanctions as such, focusing instead on civil remedies, presumably the definition of trade secrets set up in the Directive will have an impact on the criminal provisions governing the

infringement of trade secrets. It would be hard to justify two different definitions in criminal and civil law regarding the term 'trade secret'. It is important to bear in mind that the definition of the term 'trade secret' determines the scope of criminal liability; in other words, the extent to which the violation of business secrets is criminalised depends on how trade secrets are defined.

The Directive just discussed is not binding on Switzerland, since it is not a member state of the EU. Therefore, in contrast to the EU member states, the Swiss legislature has no legally binding reason to change its traditional understanding of trade and manufacturing secrets. In Switzerland, in order for information to qualify as a trade secret protected by law, it must, inter alia, be information whose owner desires to keep it secret (for the Swiss definition of trade secrets cf. Schwarz 2013, § 19 no. 36 et sequ.; Niggli and Hagenstein 2019, Art. 162 no. 15 et sequ.; BGE 118 Ib 547 E. 5a; BGE 103 IV 283 E. 2b). In contrast with the EU Directive, the Swiss understanding of trade secrets does not necessarily require non-disclosure measures taken by the person having control over the information for the information to qualify as a trade secret. This is a profound difference between trade secret protection in Austria and Switzerland. Switzerland will have to decide whether to keep its traditional definition of trade and business secrets or whether to adjust its definition to the international standard, adopted in the EU Directive, in the TRIPS agreement and in the legislation of many countries worldwide.

Research gap

Even though much attention has recently been paid to the phenomenon of industrial and economic espionage and the risks and dangers resulting from it, there still is a large gap in empirical research on the topic and on its prevention (cf. Carl 2017, p. 1315; Kilchling and Carl 2016, p. 183).

In Austria and even more so in Switzerland, there are very few empirical studies and accordingly very little empirical data on economic and industrial espionage.

The Swiss studies which do contain data on industrial and economic espionage have been carried out by the consulting enterprises KPMG and PwC (KPMG 2013; PwC 2011). This means that the validity of the data is limited, since these studies have mainly been conducted for commercial reasons. However, the Swiss Federal Intelligence Service has recently ordered that an extensive empirical survey on economic espionage be conducted (Hostettler et al. Forthcoming).

In Austria, there are only three empirical studies on economic and industrial espionage so far (BM.I. et al. 2010, 2015; Corporate Trust 2014).

The WiSKoS study, which contains empirical data on economic and industrial espionage for Austria and Switzerland, has not yet been published (Wallwaey et al. 2019).

Generally, it is important to realise that in order to fight economic and industrial espionage efficiently and in order to create criminal law provisions that work in practice, a broad criminological understanding of this phenomenon is necessary. Studies should aim towards a profound knowledge concerning the offenders, the

victims, the modi operandi of the offenders, and the negative effects resulting from industrial and economic espionage.

So far, little research has been done on the criminal provisions of economic and industrial espionage. This is especially true regarding comparative criminal law. Most of the existing literature does not provide a very comprehensive and holistic in-depth view, but is, instead, limited to very specific issues in specific countries, like Ackermann-Blome and Rindell (2018), or only gives a general overview, like Reid (2016) and Carl et al. (2017), or is outdated, like Schaffheutle (1972) and Oehler (1981). In connection with the WiSKoS Study, a comprehensive comparative study on the criminal provisions on industrial and economic espionage including country reports of all EU member states and Switzerland is expected for 2019. Until now however, no comparative research on the Austrian and Swiss criminal provisions of economic and industrial espionage, as done herein, has been published.

Definitions of industrial and economic espionage

Similar to many other European countries (cf. Carl 2017, pp. 1317 et sequ.), neither Austria nor Switzerland has provided a legal definition of what constitutes industrial or economic espionage.

Austria

In German terminology, there is an inconsistency when referring to, and describing the phenomenon of economic and industrial espionage (cf. Bollhöfer and Jäger 2018, p. 17; Carl 2017, pp. 1317 et sequ.; Kilchling and Carl 2016, pp. 183 et sequ.).

The terms ‘industrial espionage’ (in German ‘Industrie- oder Betriebsspionage’ or ‘Konkurrenzausspähung’) and ‘economic espionage’ (in German ‘Wirtschaftsspionage’) can be found neither in Austrian legislation nor in Austrian case law. However, the handbook of the Austrian Ministry of Interior et al. provides a definition, basing the difference between industrial and economic espionage on the person who committed the act of spying. It defines economic espionage as actions by foreign intelligence services, spying on Austrian companies in order to strengthen the economy of their own countries, whereas industrial espionage is defined more broadly as companies illegally spying on rival companies (Austrian Ministry of Interior 2011, pp. 15 et sequ.).

Switzerland

In Switzerland, some Federal laws, such as the Article 10(4) of the Federal Act on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods Article 4(3) of the Embargo Act, or Article 28(4) of the War Material Act, use the term ‘economic espionage’, but do not provide a definition. In the fact sheet on economic espionage issued by the Swiss Federal Intelligence Service in 2017, a difference is

made between economic and industrial espionage (cf. Swiss Federal Intelligence Service 2017, p. 2).

However, in contrast to the Austrian handbook and the German approach (cf. Knickmeier forthcoming), in Switzerland, the differentiation between economic and industrial espionage is not based on whether the act of spying was committed by a foreign intelligence service, but on whether the Swiss economy, as such, is endangered by the act of spying. This means that even though the criminal offence of economic espionage (Article 273, Swiss Criminal Code) is deemed a 'crime against state interests', it not only criminalises acts of spying on behalf of foreign intelligence services, but under certain circumstances also espionage on behalf of foreign companies. This Swiss peculiarity, which was introduced at a very late stage of the legislative process on the initiative of Ernst Hafter, then Professor of Criminal Law at the University of Zurich (Hafter 1937, pp. 213 et sequ.; cf. Meyer 1955, pp. 315 and 322 et sequ.) without much debate, has significant implications for the practical application of the offence of economic espionage.

Due to this broad understanding of the offence of economic espionage, for example a person, who tried to get information about manufacturing methods of bicycle valves of a Swiss machine factory for a Belgian manufacturer, was found by the Federal Court to have committed the political offence against state interests according to Article 273 Swiss Criminal Code (Federal Court, Judgment December 10 1948, BGE 74 IV p. 206; Meyer 1955, p. 323).

Legal consequences resulting from the differentiation between economic and industrial espionage

This distinction between economic and industrial espionage leads to classifying industrial espionage as a white-collar crime, whereas economic espionage is considered a crime against the state (cf. Carl 2017, p. 1316; Kilchling and Carl 2016, pp. 187 et sequ.).

As will be described later, this distinction also amounts to different duties regarding combating, preventing, and sanctioning economic and industrial espionage. As the origins and aims of the act of spying are often not clear, it is frequently hard to decide which specific authority is in charge concerning a certain incident (cf. Carl 2017, p. 1316).

The distinction between economic and industrial espionage also has procedural consequences, as will be shown below. The classification might not only have negative effects on the efficiency of the domestic prosecution, but it might also have a negative impact on cross-border cooperation and legal assistance (cf. Carl 2017, p. 1317; Kilchling and Carl 2016, p. 188).

Against this background, some authors question whether the distinction between industrial and economic espionage is (still) adequate (Carl 2017, p. 1317; Kilchling and Carl 2016, p. 188). Industrial and economic espionage are characterised by largely identical modi operandi; the aim of industrial and economic espionage, i.e. illegally gathering trade secrets, is basically the same. Economic and industrial

espionage have mostly the same targets and victims, i.e. trade secrets and the owners of the secrets (Carl 2017, p. 1315).

Criminal offences of economic and industrial espionage in Austria and Switzerland

Most, but not all, European countries have specific civil and criminal laws to protect trade secrets (European Union Intellectual Property Office 2018, p. 415; Baker and McKenzie 2013, pp. 4, 7, 55; Desai 2018, p. 487; Carl et al. 2017, p. 94). Both Austria and Switzerland recognise special criminal provisions regarding the protection of trade secrets. In Austria and Switzerland, and in many other countries in Europe (Baker and McKenziet 2013, pp. 55 et sequ.), the main criminal provisions regarding the infringement of trade secrets are primarily established within the Criminal Code on the one hand, and within the Act against Unfair Competition on the other hand (Tables 1, 2).

Switzerland

In Switzerland, Article 162 Swiss Criminal Code contains the offence of the breach of manufacturing or trade secrecy. According to Article 162 Swiss Criminal Code, any person who betrays a manufacturing or trade secret that he/she is under a statutory or contractual duty not to reveal, and any person who exploits the same for himself/herself or for another person shall be punished upon complaint. The offence of industrial espionage contained in Article 162 Swiss Criminal Code is set out under the title of Offences against Property.

Other offences of industrial espionage can be found in Articles 4 lit. c, 6 each in conjunction with Article 23 of the Swiss Federal Act against Unfair Competition. Article 4 lit. c, in conjunction with Article 23 of the Swiss Federal Act against Unfair Competition, sanctions upon complaint any person who incites a company employee, a company commissioner, or other assisting persons to spy on the trade or manufacturing secrets of their employer or commissioner or to reveal manufacturing or trade secrets to unauthorised persons. Article 6 in conjunction with Article 23 of the Swiss Federal Act against Unfair Competition sanctions upon complaint any person who takes advantage of, or discloses, trade or manufacturing secrets, which he had learned by spying or that he had illegitimately obtained knowledge of in any other way.

The offence against economic espionage is contained in Article 273 of the Swiss Criminal Code. According to Article 273, any person shall be punished who spies on a manufacturing or trade secret in order to make it available to any external official agency, foreign organisation, foreign private enterprise, or to the agents of any of these, or who makes a manufacturing or trade secret available to an external agency, foreign organisation, foreign private enterprise, or to the agents of these.

Table 1 Legislative overview of the criminal offences of industrial espionage

	Austria		Switzerland	
	S. 123 of the Criminal Code	**S. 11** of the Act against Unfair Competition	**Art. 162** of the Criminal Code	**Art. 4 lit. c, 6, 23** of the Act against Unfair Competition
Source: Criminal Code	**X**		**X**	
Source: Competition Law		**X**		**X**
Legal assets protected	Individual legal assets: business and trade secrets	Individual assets Collective legal interests: protection of fair competition	Individual legal assets (exactly which ones unclear, this is contested in literature)	Individual assets Collective legal assets: protection of fair competition
Offender	Can be anyone	**S. 11(1)**: only employees **S. 11(2)**: can be anyone	**Art. 162(1)**: only person under an obligation of secrecy **Art. 162(2)**: can be anyone	Can be anyone
Conduct	Spying on a business or trade secret	Disclosure or use of a business or trade secret without authorisation	Disclosure or use of a business or trade secret	**Art. 4 lit. c**: to initiate employee to spy on or to disclose a trade secret **Art. 6**: to take advantage of or to disclose a trade secret
Requirement of offender to act with intent	**X**	**X**	**X**	**X**
Requirement of a complaint in order to start prosecution	**X**	**X**	**X**	**X**
Right to file a complaint	Aggrieved person	Aggrieved person	Aggrieved person	Persons who have the right to file a civil complaint and Under certain conditions, certain specified organisations and the Swiss Federation
In charge of prosecution	Private prosecutor who is the aggrieved person	Private prosecutor who is the aggrieved person	Public prosecutor	Public prosecutor
Penalty	Imprisonment for up to 2 years	Imprisonment for up to 3 months or monetary penalty up to 180 daily penalty units	Imprisonment for up to 3 years or monetary penalty	Imprisonment for up to 3 years or monetary penalty

Table 1 (continued)

	Austria		Switzerland	
	S. 123 of the Criminal Code	**S. 11** of the Act against Unfair Competition	**Art. 162** of the Criminal Code	**Art. 4 lit. c, 6, 23** of the Act against Unfair Competition
Criminal liability of companies	**X** **S. 3** Act of Corporate Criminal Liability Monetary fine up to 70 daily penalty units; One daily penalty unit ranges from EUR 50 to EUR 10.000	**X** **S. 3** Act of Corporate Criminal Liability Monetary fine up to 40 daily penalty units; One daily penalty unit ranges from EUR 50 to EUR 10.000	**X** On the conditions of **Art. 102(1)** of the Criminal Code: only if it is not possible to attribute the act to any specific natural person due to the inadequate organisation of the undertaking Monetary fine of up to CHF 5 million	**X** On the conditions of **Art. 102(1)** of the Criminal Code: only if it is not possible to attribute the act to any specific natural person due to the inadequate organisation of the undertaking Monetary fine of up to CHF 5 million

Table 2 Legislative overview of the criminal offences of economic espionage

	Austria		Switzerland
	S. 124 of the Criminal Code	**S. 256** of the Criminal Code	**Art. 273** of the Criminal Code
Source: Criminal Code	**X**	**X**	**X**
Legal assets protected	Collective legal assets, such as the Austrian economy Disputed in the literature whether individual legal assets are also protected	Collective legal assets: state interests Disputed in the literature whether individual legal assets are also protected	Collective legal assets Disputed in the literature whether individual legal assets are also protected
Offender	**S. 124(1)**: can be anyone **S. 124(2)**: person who is obliged to protect secrecy of the business or trade secret	Can be anyone	Can be anyone
Conduct	**S. 124(1)**: to spy on a business or trade secret in order to take advantage of it, to use it or to analyse it abroad **S. 124(2)**: revealing a business or trade secret so that it can be exploited, used, or analysed abroad	to build, to operate, or to support a secret intelligence service operating against Austrian interests	**Art. 273(1)**: to seek to obtain a business or trade secret in order to make it available to an external official agency, a foreign organisation, a private enterprise, or to the agents of any of these **Art. 273(2)**: to make a manufacturing or trade secret available to an foreign official agency, a foreign organisation, a private enterprise, or the agents of any of these
Requirement of offender to act with intent	**X**	**X**	**X**
Ex officio prosecution	**X**	**X**	**X**
Procedural peculiarity	–	–	Political offence: prosecution needs authorisation of the Federal Council
Penalty	imprisonment of up to 3 years	imprisonment of up to 3 years	imprisonment up to 3 years (in serious cases a minimum of 1 year of imprisonment), if necessary, combinable with a monetary penalty

Table 2 (continued)

	Austria		Switzerland
	S. 124 of the Criminal Code	**S. 256** of the Criminal Code	**Art. 273** of the Criminal Code
Jurisdiction	Austria also asserts jurisdiction even if the act is committed abroad, irrespective of the laws applicable at the scene of the crime, and irrespective of the nationality of the offender and the victim (S. 64(1) of the Criminal Code)	Austrian also asserts jurisdiction even if the act is committed abroad, irrespective of the laws applicable at the scene of the crime, and irrespective of the nationality of the offender and the victim (S. 64(1) of the Criminal Code)	Swiss jurisdiction given even if the act is committed abroad irrespective of the nationality of the offender and the victim (Art. 4 of the Criminal Code)
Criminal liability of companies	**X** S. 3 of the Act of Corporate Criminal Liability Monetary fine of up to 85 daily penalty units; One daily penalty unit ranges from EUR 50 to EUR 10,000	**X** S. 3 of the Act of Corporate Criminal Liability Monetary fine up to 85 daily penalty units; One daily penalty unit ranges from EUR 50 to EUR 10,000	**X** On the conditions of **Art. 102(1)** of the Criminal Code: only if it is not possible to attribute the act to any specific natural person due to the inadequate organisation of the undertaking Monetary fine of up to CHF 5 million

Article 273 Swiss Criminal Code is set out under the title 'Offences against the State and National Defence'. This systematic classification is justified by the fact that Article 273 is only applicable if the (intended) recipient of the secret is non-Swiss (cf. Konopatsch et al. 2019; Bazzi 2015, no. 254 et sequ.; Schmidt 1981, p. 221) and is not a private individual (cf. Husmann 2019, Art. 273 no. 59 et sequ.; Schwarz 2013, § 19 no. 142). A recent and very well-known conviction based on Article 273 is the one made by the Swiss Federal Court based on the sale of Swiss banking data to the German tax authorities (BGE 141 IV 155 E. 4.3.2; Eicker 2010, 2011).

It is interesting to note that similar cases of spying on Swiss banking institutions in order to gain information for foreign, especially German, tax authorities were the reason for the introduction of a criminal offence of economic espionage in Article 4 of the 'Spitzelgesetz' ('Espionage Act') in 1935 (Hafter 1937, p. 215). This provision was the successor to Article 273 regarding the offence of economic espionage.

Moreover, the violation of banking secrecy (Article 47 of the Swiss Banking Act), the violation of professional secrets in relation to securities dealers (Article 43 of the Swiss Stock Exchange Act), and the offence contained in Article 66 in conjunction with Article 81 of the Federal Act on Patents for Innovation are categorised as criminal offences of economic or industrial espionage. The criminal offence of the violation of banking secrecy is peculiar, compared to all other offences of industrial and economic espionage in both Austria and Switzerland, because for violations of banking secrecy, negligence is sufficient to constitute criminal liability.

Austria

The offence of spying regarding a business or trade secret (Section 123 of the Austrian Criminal Code) and the offence of spying regarding a business or trade secret on behalf of foreign countries (Section 124 of the Austrian Criminal Code) are set out under the title 'Violations of Privacy and Professional Confidentiality'.

Section 123(1) sanctions, upon complaint, spying to discover a business or trade secret in order to take advantage of it, pass it to a third party, or to reveal it to the general public.

Other offences of industrial espionage are contained in Section 11 of the Austrian Act against Unfair Competition. Section 11(1) sanctions any employee of an enterprise who, without authorisation and for competitive purposes, discloses to others, any business or trade secret, which due to his employment has been entrusted to him, or has been made accessible to him during the terms of his employment. Section 11(2) criminalises anyone who, without authorisation and for competitive purposes, uses or discloses to others, any business or trade secret which he has received through information as set forth in para. 1, or by an act of his own, and which is illegal or contrary to public policy.

The EU Directive described above does not oblige the legislatures of the member states to change the criminal provisions on the protection of trade secrets. Therefore, the Austrian Act against Unfair Competition has only been amended regarding the civil remedies available to the owner of the trade secret, in order to implement the Directive (cf. Sections 26a et sequ. Austrian Act against Unfair Competition). This

means that the criminal offences regarding industrial espionage contained in the Austrian Code against Unfair Competition have not been amended when implementing the Directive. The criminal provisions still recognise the distinction between business and manufacturing secrets. The definition of trade secrets set forth by the Directive, which—as described above—mainly relies on objective criteria, did not make its way into the criminal provisions. However, as already stated, it is not justified to use different legal definitions for defining trade secrets.

Section 124(1) Austrian Criminal Code criminalises espionage regarding business or trade secrets in order to take advantage of them abroad, to use them abroad, or to analyse them abroad. In contrast to Section 123(1) of the Austrian Criminal Code, the act of spying has to be carried out on behalf of a foreign country (explanatory remarks to the government bill 1965, p. 9; Konopatsch and Hilf 2019). Section 124(2) Austrian Criminal Code sanctions the revealing of a business or trade secret which the offender is obliged to keep secret, so that it can be exploited abroad or so that it can be used or evaluated abroad. Section 124 criminalises any economic treason against Austria as a country (explanatory remarks to the government bill 1965, p. 9; Austrian Supreme Court 11 Os 74/09f). The explanatory remarks to the government bill consider Section 124 to govern an extraordinarily severe form of economic espionage (explanatory remarks to the government bill 1965, p. 9).

Another offence of economic espionage contained in Section 256 of the Austrian Criminal Code sanctions anyone who builds a secret intelligence service to operate against Austrian interests, anyone who operates such a service, or anyone who in any way supports such a service. Section 256 is set out under the title ‘Treason’.

Similarities and differences between the criminal offences of industrial and economic espionage under Austrian and Swiss Law

The following analysis will cover aspects of the structure, characteristic features, and content of the offences of industrial and economic espionage under Austrian and under Swiss law, as well as aspects of the procedural framework of each country. There are remarkable similarities regarding the legal conception and the legal structure of the criminal offences of industrial and economic espionage in Austria and Switzerland.

A long tradition of criminal offences of industrial and economic espionage

Especially considering the rapidly changing modi operandi of industrial and economic spies—which is also due to technical progress—it might be surprising that neither the Austrian nor the Swiss criminal offences of economic and industrial espionage have been amended in content for decades.

Both countries have a very long legal tradition regarding specific criminal offences of industrial and economic espionage. Figures 1, 2 set out a timeline of the legislative developments in Switzerland and Austria.

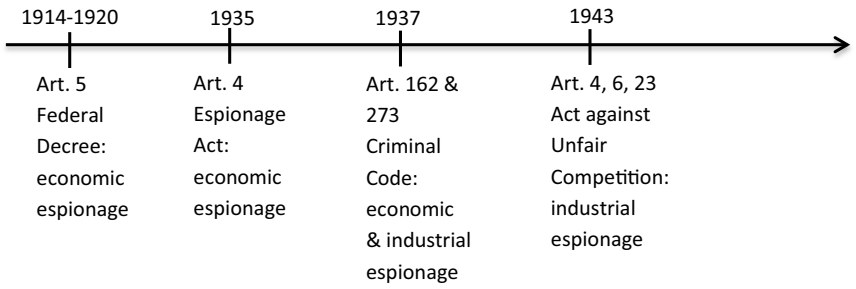

Fig. 1 Timeline of legislative developments in Switzerland—federal level

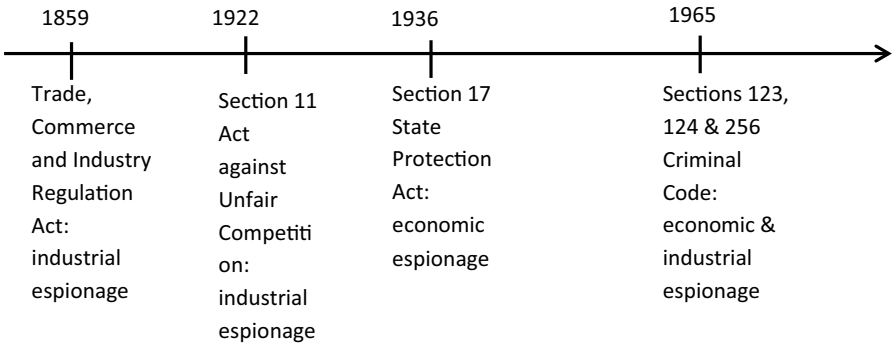

Fig. 2 Timeline of legislative developments in Austria

In Switzerland, the first criminal offence regarding espionage at the federal level dates back to the beginning of World War I and was contained in Article 5 of the Federal Decree of August 6 1914 (cf. Meyer 1955, p. 305; Pfenninger 1918, pp. 134 et sequ.; Thilo 1917, pp. 185 et sequ.). Due to the specifically war-related background, this offence was only in force until 1920.

In 1935, the Espionage Act was introduced, which contained in its Article 4 the criminal offence of economic espionage. Article 4 of the Espionage Act was then included in Article 273 of the new Swiss Federal Criminal Code of 1937; however, there was an important amendment insomuch as Article 273 of the Swiss Criminal Code not only covers espionage in favour of a foreign authority but also espionage in favour of foreign enterprises.

Both the Swiss Federal Criminal Code in its first version of 1937 and the first version of the Swiss Federal Act against Unfair Competition of 1943 contained offences regarding industrial espionage. Prior to these federal laws, some cantonal laws included criminal provisions on economic and industrial espionage.

In Austria, the oldest criminal provision regarding industrial espionage can be traced all the way back to 1859 (Thiele 2016, § 11 UWG no. 1; Brunstein, 1887, pp. 7 et sequ.). In 1923, this provision was incorporated into the new Act against Unfair Competition.

In 1936, the criminal offence of economic espionage was introduced in Section 17 of the Austrian State Protection Act which in 1965 was then included in Section 256 Austrian Criminal Code. In 1965, another offence of economic espionage (Section 124) and the offence of industrial espionage (Section 123) were also introduced in the Austrian Criminal Code.

Criminal liability

Many criminal offences of industrial and economic espionage in Austrian and Swiss law only require that the offender act in the way described by statute for the offence to be completed (Tables 1, 2). It is not necessary that damages result from the act, i.e. the owner need not suffer any commercial loss nor must any undue distortion of competition be proven. This means that acting as described by the offence is enough to constitute criminal liability for the completed offence and not just for its attempt. The Austrian and Swiss doctrine characterises such offences as 'schlichte Tätigkeitsdelikte' ('offences by commission') and 'abstrakte Gefährdungsdelikte' ('offences of abstract endangerment').

This classification is uncontested in literature and jurisprudence regarding, for example, Article 273(1) of the Swiss Criminal Code (cf. Husmann 2019, Art. 273 no. 71), regarding Article 162(1) of the Swiss Criminal Code (cf. Niggli and Hagenstein 2019, Art. 162 no. 36; Stratenwerth et al. 2010, § 22 no. 7), regarding Section 123 and Section 124 of the Austrian Criminal Code (cf. Konopatsch and Hilf 2019; Lewisch 2017, § 123 no. 1; Thiele 2007, § 124 no. 9), or regarding Section 256 of the Austrian Criminal Code (cf. Eder-Rieder 2010, § 256 no. 3).

The legal structure just described results in a broad scope of criminal liability, especially if the act demanded by the offence is not clearly specified by statute and if it is given a broad understanding in practice. This is true, for example, for offences under Sections 123 and 124 of the Austrian Criminal Code. Some Austrian scholars even criticise these criminal provisions as being too imprecise and unclear, creating problems regarding the necessary standards of the principle of legal certainty in criminal law (Thiele 2007, § 123 No. 10; Wessely 2013, § 123 No. 1; Birklbauer et al. 2017, §§ 122-124 no. 7).

Adequate limitations on the meaning of the term 'spying' are therefore called for both in literature and in case law (cf. Konopatsch and Hilf 2019; Lewisch 2017, § 123 no. 5 et sequ.; Wessely 2013, § 123 no. 3; Köck 2010, pp. 78 et sequ.; Burgstaller 1980, p. 18). Thiele writes that more precise wording by the legislature is necessary (Thiele 2007, § 123 no. 13).

Others criticise Article 273 of the Swiss Criminal Code for its insufficiently clear wording of the offence (Husmann 2019, Art. 273 no. 69; Trechsel and Vest 2018, Art. 273 no. 11).

Another problem with the concept of offences by commission concerns jurisdictions. With regard to the principle of territoriality for determining the jurisdiction, it is only the act of spying as such and not any effect resulting from it that is relevant. Therefore, some authors recommend the amendment of the principle of territoriality, especially with regard to cybercrime (Eicker 2013, § 3 no. 5; cf. also Cassani 1996, pp. 251 et sequ.).

However, with regard to the offences of economic espionage, Austrian and Swiss criminal laws claim jurisdiction even if the act of spying was committed abroad and irrespective of the nationality of the victim and the offender (Graf 2016, p. 198) (Table 2). The underlying justification is that state interests are concerned in these cases.

Persons who can qualify as an offender

Some criminal offences of industrial and economic espionage in Austria, as well as in Switzerland, require that the offender have certain characteristics specified by statute in order to be criminally liable (Tables 1, 2). These offences are called 'Sonderdelikte' in German terminology. Regarding Article 162(1) of the Swiss Criminal Code, for example, only a person who is under a statutory or contractual duty not to reveal the trade or manufacturing secret in question can qualify as an offender.

In contrast to this, other offences of industrial and economic espionage in Austrian and Swiss law—such as Article 162(2) of the Swiss Criminal Code, Article 273 of the Swiss Criminal Code or Sections 123 and 124 of the Austrian Criminal Code—do not require that the offender has specific features. This means that any person can become criminally liable no matter whether he has specific characteristics, i.e. no matter whether he is an employee of the owner of the secret (Tables 1, 2).

Legal assets protected

In Austria, as well as in Switzerland, there is uncertainty about precisely which legal assets are protected by the criminal offences of economic and industrial espionage (Tables 1, 2).

Regarding Article 162 of the Swiss Criminal Code, for example, some authors consider economic secrecy as such as the legal asset which is protected by the offence, whereas other authors deem the property of the enterprise as protected, and the Swiss Federal Court (BGE 118 Ib 547 E. 5a) has stated that it is the company which owns the secret that is protected (for the discussion cf. Niggli and Hagenstein 2019, Art. 162 no. 3 et sequ.).

Regarding the offence of economic espionage provided for in Article 273 of the Swiss Criminal Code, both case law and literature have called into question whether only state interests are protected or whether in addition individual legal assets, like the right of companies to secrecy and confidentiality, are protected (Konopatsch and Hilf 2019).

Section 124 of the Austrian Criminal Code is another example showing difficulties, which lead to academic discussions on how to determine what legal assets are protected by the offence. According to the explanatory remarks to the government bill, to the prevailing literature, and to the case law, it is (exclusively) collective legal assets, such as the Austrian economy, specific branches of the Austrian economy or Austrian competitiveness towards foreign countries, which are protected by Section 124 of the Austrian Criminal Code (cf. explanatory remarks 1965, p. 10; Austrian Supreme Court, 11 Os 74/09f; Wessely 2013, § 124 StGB no. 7; Schmid 1981, 184; Bertel et al. 2018, § 124 StGB no. 15; Fabrizy 2018, § 124 StGB no. 3). Accordingly, the Austrian Supreme Court has found that acts in contravention of Section 124 of the Austrian Criminal Code are an offence against state security (Austrian Supreme Court 11 Os 74/09f). However, some authors consider not only collective assets, but also individual assets, specifically, the confidentiality of business or trade secrets, to be protected by Section 124 of the Austrian Criminal Code. This opinion is justified inter alia by the systematic setting out of Section 124 under the title 'Violations of Privacy and Professional Confidentiality' (cf. Schramböck 2002, p. 23; Schmidt 1981, p. 184).

The discussion about the interests protected is not one of a mere academic or theoretical nature, but instead, it has an important impact on the understanding and on the practical application of the law on each offence. Just as importantly, as will be shown below—the question has a decisive influence on the procedural framework. For example, regarding Article 273 of the Swiss Criminal Code, it is only possible to consider the owner of the trade secrets a party to the criminal proceedings if the criminal statute is considered to protect individual legal assets too (Husmann, Article 273 StGB no. 106).

Furthermore, only in cases where solely interests of individual persons are at stake, might it be justified to make prosecution dependent on the initiative of the person whose interests have been violated by the offender. In cases where only, or mainly, collective interests, such as national security or the national economy are at stake, it is not justified to make prosecution dependent on the decision of any individual person.

Moreover, if the law is seen to only protect individual legal assets, then the owner of the legal assets could endorse the violation of trade secrecy by having given his or her consent to reveal the trade secret. In this case, criminal liability is excluded. However, if the offence is considered also to protect collective legal assets, criminal liability is not excluded even if all private persons involved, including the secret owner, gave their consent to reveal the trade secret.

Procedural framework

As in many other European countries, the criminal offences of economic and industrial espionage in Austria and in Switzerland have some particularities regarding the conditions for prosecution and for the commencement of a criminal proceeding (cf. Baker and McKenzie 2013, pp. 75 et sequ.) (Tables 1, 2).

General remarks

From a procedural point of view, it is important to note that generally in Austria and Switzerland, criminal proceedings regarding the offences of *economic* espionage are initiated ex officio by the public prosecutor. However, the commencement of criminal proceedings regarding the offences of *industrial* espionage, such as Section 123 of the Austrian Criminal Code, Section 11 of the Austrian Act against Unfair Competition, Article 162 of the Swiss Criminal Code and Articles 4 lit. c, 6 in conjunction with Article 23 of Swiss Federal Act against Unfair Competition, require that a criminal complaint be lodged by a person entitled to do so, in order for criminal proceedings to be started (Table 1). This means that the criminal proceedings are not commenced *ex officio*, but only *ex parte* by the person entitled to file a complaint, who is usually the aggrieved person.

The underlying legal justification for requiring a criminal complaint by an individual person aggrieved by the offence, in order for criminal proceedings to start, is similar in Austria and Switzerland. Mostly, it is considered decisive that either the interests affected by the offender are deemed to be of a very personal nature or the degree of wrongdoing is seen as small (cf. Trechsel and Jean-Richard-dit-Bressel 2018, Art. 30 no. 1; Riedo 2019, Vor Art. 30 StGB no. 7 et sequ.; Horak 2009, p. 213).

Regarding the offence of industrial espionage, the Swiss legislature justified requiring a private complaint because they did not want to expose the injured party to the publicity attached to a criminal trial against his or her will (Expertenkommission, 1895, pp. 14–18; Meyer 1955, p. 304).

It is questionable whether requiring a criminal complaint by the aggrieved person as a crucial prerequisite in order to begin criminal proceedings is wise in all cases of industrial espionage (dissenting opinion Heimgartner 2018, Art. 23 UWG no. 54). This requirement seems especially questionable when surveying the tremendous damage caused by industrial espionage and considering the fact that it is often difficult to determine whether an incident should be considered industrial or economic espionage.

Even though both Austria and Switzerland require a complaint from a person to initiate industrial espionage proceeding, the two countries do still have some fundamental differences.

Switzerland

Industrial espionage: prosecution on complaint In Switzerland, authorities must inform the aggrieved person about his or her right to file a criminal complaint. The right to file a complaint expires three months after the person entitled to file a complaint discovers the identity of the suspect (Article 31 of the Swiss Criminal Code).

The costs of the criminal proceedings may only be imposed on the person who filed the complaint if he or she wilfully, or with gross negligence, initiated the proceedings, or complicated the proceedings (Article 427(2) of the Swiss Code of Criminal Procedure).

According to Article 216(1) of the Swiss Code of Criminal Procedure, the public prosecutor may summon the complainant and the accused to a hearing with the aim of achieving a settlement. If an agreement is reached, the public prosecutor will abandon the proceedings (Article 216(3) of the Swiss Code of Criminal Procedure). Riedo (2019, Vor Art. 30 no. 15) rightly points out that the legal structure requiring that offences be prosecuted only upon complaint increases the number of private settlements.

According to Article 303(1) of the Swiss Code of Criminal Procedure, it is only after a complaint by the entitled person has been filed that the preliminary investigation procedure can start. Prior to this, the authorities in charge may only adopt measures to secure evidence when urgently necessary (Article 303(2) of the Swiss Code of Criminal Procedure). After the complaint had been filed, it is the police and the public prosecutor who are in charge of the investigation. According to Article 118(2) of the Swiss Code of Criminal Procedure, the entitled person who has filed the complaint then becomes a party to the criminal proceedings, meaning that he or she has the procedural rights of a party, such as the right to be heard.

The offences of industrial espionage which are provided for in the Swiss Federal Act against Unfair Competition (i.e. Article 4 lit. c and Article 6—each in conjunction with Article 23 of the Swiss Federal Act against Unfair Competition) contain some particularities regarding the entitlement to file the criminal complaint, which is necessary to start criminal proceedings (Table 1). According to Article 23(2) of the Swiss Federal Act against Unfair Competition, the entitlement to file a criminal complaint is made dependent on the entitlement to file a civil claim. This is quite rightly criticised by some scholars, as it means that criminal prosecution is made dependent on the legal possibility of filing a civil claim (Killias and Gilliéron 2013, Art. 23 no. 38 et sequ.; Schaffner and Spitz 2016, Art. 23 No. 75; Pedrazzini and Pedrazzini 2002, no. 26.09; dissenting opinion: Riedo 2004, pp. 269 et sequ.). According to Article 9 of the Swiss Federal Act against Unfair Competition, any person whose economic interests are endangered or violated by an act of unfair competition is entitled to file a civil claim.

Additionally, Article 10 of the Swiss Federal Act against Unfair Competition declares that some organisations specified by law and, under certain conditions, the Swiss Federation itself are entitled to make a civil claim and, thus, to file a criminal complaint to commence criminal proceedings. According to Article 10(3) of the Swiss Federal Act against Unfair Competition, the Swiss Federation is only entitled to file a civil claim, and thus to file a criminal complaint, if public interests are at stake, to be precise, if the reputation of Switzerland abroad is threatened or violated or if the collective interests of Swiss nationals are affected. The Swiss Federation is granted a broad scope of discretion regarding its decision to file a complaint (Jositsch and Conte 2015, pp. 443 et sequ.). The State Secretariat for Economic Affairs, which represents the Swiss Federation, regularly files such complaints (David and Jacobs 2012, no. 543). In 2013, for example, the State Secretariat for Economic Affairs filed 28 such complaints (Jositsch and Conte 2015, p. 441). In 2018, it filed 18 (SECO 2018) such complaints and in 2017 it filed 23 complaints (SECO 2017).

The rules granting the Swiss Federation the right to file a criminal complaint, which is necessary to commence a criminal proceeding, are a Swiss procedural

particularity. This concept is problematic as the line between the legal categories of offences prosecuted ex officio and offences prosecuted only upon complaint by a person affected by the offence is blurred (Jositsch and Conte 2015, p. 443; Killias and Gilliéron 2013, Art. 23 UWG no. 41; Baudenbacher and Glöckner 2001, Art. 23 UWG no. 17).

Economic espionage: a political offence The offence of economic espionage provided for in Article 273 of the Swiss Criminal Code shows a procedural particularity as well (Table 2). It is categorised as a 'political offence' (Schwarz 2013, § 19 no. 22; Husmann 2019, Art. 273 StGB no. 103 et sequ.). This means that its prosecution must be authorised by the Federal Council (Article 66(1) of the Act on the Organisation of the Federal Prosecution Authorities).

The Federal Council has delegated its right to grant or to deny the authorisation to prosecute to the Federal Department of Justice. The authorisation to prosecute, for example, was denied on grounds of national interests in the case of the transfer of Swiss banking data to the U.S. authorities by SWIFT (Husmann 2019, Art. 273 StGB no. 103).

Furthermore, it is interesting to note that Article 30(1) of the Swiss Regulation on Swiss Citizenship states that a person who has been found guilty of economic espionage (Article 273 of the Swiss Criminal Code) is considered to have substantially affected the interests and the reputation of Switzerland. In such a case, according to Article 30(2) of the Swiss Regulation on Swiss Citizenship, the offender's Swiss citizenship can be revoked subject to certain conditions (Husmann 2019, Art. 273 StGB no. 109; von Rütte 2017, pp. 211 et sequ.). According to the explanatory report of the Federal Council, the withdrawal of Swiss citizenship is an administrative sanction independent from a criminal penalty.

Despite this clear classification as an administrative sanction, the Explanatory Report also acknowledges that the character of the sanction is similar to a penalty (Explanatory Report 2016, p. 33; von Rütte 2017, p. 212).

Austrian offences of industrial espionage: prosecution on request

In Austria, Section 123(2) of the Austrian Criminal Code and Section 11(3) of the Austrian Act against Unfair Competition state that the offence of industrial espionage shall only be prosecuted at the request of the affected person (Table 1). This type of offence is called 'Privatanklagedelikte' in German terminology, meaning that the individual person not only initiates the prosecution but is responsible for the prosecution too. This legal concept amounts to a private prosecution. Private prosecution constitutes an exception to the procedural principle of *ex officio* prosecution by the public prosecutor (Horak 2009, p. 213).

The person entitled to request prosecution is free to decide whether to prosecute or not (Engin-Deniz 2015, p. 81). In cases of private prosecution, no preliminary investigation procedure takes place (Section 71(1) of the Austrian Code of Criminal Procedure; Explanatory Remarks to the Government Bill 2004, p. 102). This means that the person whose legal assets have been affected by the offender, referred

to as the 'private prosecutor', has to collect the evidence necessary to file a charge (Konopatsch and Hilf 2019).

According to Section 71(3) in conjunction with Section 211(1) of the Austrian Code of Criminal Procedure, the charge has to include the name and personal details of the accused, the title of the offence, and the factual circumstances of the offence. Furthermore, it has to provide information regarding the entitlement to file the charge. The duty to give information regarding the entitlement to bring a charge is meant to protect against unsubstantiated charges (Explanatory Remarks to the Government Bill 2004, p. 103).

According to Section 71(5) of the Austrian Code of Criminal Procedure, the private prosecutor basically has the same rights as the public prosecutor. However, the private prosecutor is only entitled to apply for compulsory measures where it is necessary to secure evidence or to secure an order concerning property. This means that the private prosecutor cannot use compulsory measures for investigative purposes (Engin-Deniz 2015, p. 82). The private prosecutor does not have any authority to give instructions to the police (Korn and Zöchbauer 2017, § 71 StPO no. 19; Engin-Deniz 2017, p. 229). He/she is not entitled to apply for detention or for custody (Section 71(5) of the Austrian Code of Criminal Procedure).

Recently, the Austrian Supreme Court has ruled that the private prosecutor has no right to be present during the house search, which the police conduct at his or her request, in order to secure evidence in relation to industrial espionage (Austrian Supreme Court, August 23 2017, 15 Os 7/17v, ÖBL-LS 2018/5). Hofmarcher (2018a, b, p. 58) and Engin-Deniz (2017, p. 228) consider the decision of the Austrian Supreme Court as further weakening the position of the private prosecutor as he/she has to rely on the police, who conduct the house search to fully understand his/her request regarding the evidence requested.

The Austrian Supreme Court has stated that basically, the private prosecutor is entitled to obtain access to the files as long as he/she can show a legitimate interest for obtaining access. However, according to the Austrian Supreme Court, the interest of the private prosecutor in gaining access to the files has to be balanced, on a case to case basis, against the interests of the accused in denying the private prosecutor access to the files (Austrian Supreme Court, decision of August 23 2017, 15 Os 7/17v; Hofmarcher 2018a, b, p. 57). In the specific case just mentioned, the accusation was based on industrial espionage (Section 123 of the Austrian Criminal Code). The accused person requested that the private prosecutor be denied access to the files, which were seized during a raid of the office of the accused. The accused argued that the private prosecutor was a rival enterprise, which might obtain trade secrets pertaining to the accused if it were to be given access to the seized files.

The case just described shows, once more, that the concept of the private prosecutor, provided for under Austrian law, is not an adequate legal instrument to deal with industrial espionage.

Furthermore, in general, the fact that there is no official investigative procedure, and that the private prosecutor has to investigate the circumstances of a suspicious incident on his own, in order to be able to apply for compulsory measures and to file the complaint, lays a substantial procedural burden on the private prosecutor (cf. Engin-Deniz 2015, p. 82; Korn and Zöchbauer 2017, § 71 StPO no. 19). It is only

possible for the private prosecutor to proceed if he/she is able to present a suspect; it is not possible for him/her to apply for compulsory measures in order to find a suspect (Konopatsch and Hilf 2019).

In contrast with the public prosecutor, the private prosecutor is not subject to the principle of objectivity, so that he or she has no obligation to investigate incriminating and exculpatory circumstances with equal care (Korn and Zöchbauer 2017, § 71 StPO no. 21).

Taking on the role of a private prosecutor is not only unattractive due to the lack of an investigation procedure but also due to the provisions regarding the procedural costs. According to Section 390(1) of the Austrian Code of Criminal Procedure, all costs of the criminal proceeding fall on the private prosecutor if the accused is not found guilty.

Generally, it is questionable if the concept of the private prosecutor, as such, is convincing or should be amended or even abolished. Some scholars even argue that the concept of the private prosecutor is one reason for the limited practical relevance of the offence of industrial espionage (cf. Zipf 1981, § 122 StGB no. 16).

However, limited practical relevance is also true for the offence of economic espionage as defined in Section 124 and Section 256 of the Austrian Criminal Code, which are both prosecuted *ex officio* (Konopatsch and Hilf 2019).

The concept of private prosecution likely increases the number of out-of-court-settlements regarding industrial espionage. Furthermore, the individual person, whose interests have been affected by the act of industrial espionage, will usually choose civil remedies to enforce his/her claim(s) rather than initiate criminal proceedings.

Generally, it must be stressed that in Austrian criminal law, it is decisive whether the act of spying was actually carried out (or at least is considered to have been carried out) either on behalf of a foreign country/enterprise or on behalf of a domestic (Austrian) enterprise. In cases of foreign espionage, it is the public prosecutor who is in charge, while in domestic cases it is the private prosecutor who must bring the case. However, for the individual whose interests have been aggrieved by the offender, the damage has been done, no matter the nationality of the spying entity. This legal situation was noted in an Austrian newspaper article, which stated that Austrian companies, in cases of industrial espionage, are left to cope alone. Only when the act of spying is conducted on behalf of a foreign enterprise/country, does Austrian justice take severe action in its battle against espionage (Marko 2017).

Conviction rates

It has to be stressed that in Austria, the official Court Crime Statistics ('gerichtliche Kriminalstatistik') do not reflect the actual circumstances regarding the conviction rate for economic and industrial espionage. The statistics only show a conviction if the offence, upon which the conviction is based, is the one which is decisive for determining the sentence.

Furthermore, the Court Crime Statistics only provide separate data for some and not for all offences. They do not break the data down into separate categories for

offences falling under Sections 123 and 124 of the Austrian Criminal Code. Instead, they generally only provide cumulative data for Sections 122 to 124 of the Austrian Criminal Code. The same is true for the offence of industrial espionage according to Section 11 of the Austrian Act against Unfair Competition. The Austrian Court Crime Statistics only provide data regarding all criminal offences contained in the Austrian Act against Unfair Competition in total.

Between 1976 and 2017, the Austrian statistics show 43 convictions based on Sections 123 to 124 of the Austrian Criminal Code, which is an average conviction rate of 1.02 per year. Regarding the offence of economic espionage according to Section 256 of the Austrian Criminal Code, the Austrian Court Crime Statistics show 12 convictions between 1976 and 2017, which is an average conviction rate of 0.29 per year.

In Switzerland, the statistics published by the Federal Statistical Office show 39 convictions based on the offence of economic espionage according to Article 273 of the Swiss Criminal Code and 135 convictions based on the offence of industrial espionage according to Article 162 of the Swiss Criminal Code between 1984 and 2017.

As in Austria, the Swiss statistics on criminal convictions do not provide separate data for the offence of industrial espionage, according to Articles 4 lit. c, 6, each in conjunction with Article 23(1) of the Swiss Act against Unfair Competition, but only on all criminal offences contained in the Swiss Act against Unfair Competition as a whole.

Additionally, there is the problem that cases of industrial and economic espionage are statistically under-represented. Unclear cases are regularly statistically classified under other categories, such as cybercrime or theft, without any reference to economic and industrial espionage (Carl 2017, pp. 1316 et sequ.).

Regarding the figures just described, the criminal conviction rate for offences of industrial and economic espionage is still very limited in Austria and Switzerland.

However, empirical findings suggest that industrial and economic espionage is a far more significant problem than the figures regarding the conviction rate would indicate. According to an Austrian study conducted by the BM.I. et al. 30% of the companies polled reported having been victims of economic and industrial espionage (BM.I. et al. 2010, p. 11). According to findings of the WiSKoS study, every third enterprise in Germany claimed to have been a target of industrial or economic espionage (Bollhöfer and Jäger 2018, pp. 1 et sequ.).

A primary reason for the low conviction rate is the reluctance of victim companies to inform the competent authorities about the offences they observed. Empirical studies show that in Austria only between 13% and 25% of the victims of industrial and economic espionage actually informed the public authorities about the incident (BM.I. et al. 2010, p. 11, 2015, pp. 11, 23). These findings correspond to the findings of other European studies and literature (Bollhöfer and Jäger 2018, pp. 4, 37 et sequ.; cf. also Anderson et al. 2013) and also to U.S. findings (Orozco 2013, p. 896).

According to the WiSKoS study (cf. Bollhöfer and Jäger 2018, pp. 59 et sequ.; Knickmeier forthcoming), the main reason that German companies did not report suspicious incidents is that the damage assumed to have been caused by economic or industrial espionage was deemed to be only minor (58%). The second

most mentioned reason for not reporting is that companies are not clear about the costs and benefits of cooperating with the authorities. The third most common reason for not reporting was that the affected company had doubts about whether the person(s) responsible for the espionage could be identified (40%). Companies' insecurities regarding figuring out the appropriate authority in charge ranked fourth (40%). Finally, many companies (fifth most ranked answer) considered pursuing criminal prosecution as more complex than undertaking internal solutions (31%).

According to the Austrian study conducted by the BM.I. et al. (2015, p. 23), the main reason that incidents of economic and industrial espionage go unreported is that companies do not believe that there is sufficient evidence against the offender (58,2%). Ranked second was that companies do not believe in the success of criminal proceedings, i.e. do not believe they will end with a conviction (45,1%). Companies also mentioned that the third most important factor was that companies do not trust prosecution authorities (28,4%). Finally, in fourth and fifth place were the fact that some companies were not aware that economic and industrial espionage constituted criminal offences (23,7%) and that some companies feared a loss of reputation if they reported the espionage (13,7%).

These findings correspond to a recent case of economic espionage already mentioned in the introduction, in which a Chinese national, who was employed as a researcher at the Friedrich-Miescher-Instituts located in Switzerland, was accused by the U.S. of helping to steal trade secrets on behalf of a Chinese, state-financed company. U.S. prosecutors estimate that the trade secrets stolen are worth up to CHF 545 million and the U.S. Department of Justice has characterised the case as an instance of "economic warfare" (swissinfo 2019a, b). Even though the U.S. authorities had informed the Swiss Institute about the incidents already in 2017, the Swiss institute decided not to initiate any criminal proceedings in Switzerland, arguing that its financial loss was only minor and that the Institute had internal policies and procedures on how to prevent data theft (Settelen 2019). Meanwhile, the Chinese researcher is in prison in Switzerland, awaiting extradition to the U.S., which has already been approved by the Swiss Federal Office of Justice (swissinfo 2019b).

In general, a comprehensive in-depth discussion on the reasons for underreporting is missing in Austrian literature.

This is even more true for Switzerland. There are no empirical figures available about the reasons for companies not reporting incidents of economic or industrial espionage to authorities.

The low conviction rate is not specific to Austria and Switzerland but is also true in most other countries worldwide too (cf. Reid 2016; Orozco 2013, pp. 892 et sequ.).

In order to fight economic and industrial espionage efficiently, the problem of under-enforcement and underreporting has to be addressed and tackled. Some scholars have come up with new, somewhat drastic propositions. Orozco (Orozco 2013, pp. 908 et sequ.), for example, recommends introducing a duty to report national security-related technology theft. He wants to amend the U.S. Economic Espionage Act to introduce a new offence, which would sanction the non-reporting of any violation of the Economic Espionage Act with a fine or imprisonment. According to

Orozco, such a duty to report incidents of economic espionage could be justified due to the endangerment of national security.

Instead of introducing such a duty to report, it would be more realistic and more commonly accepted to improve the cooperation between enterprises, which have become a target of economic and industrial espionage, and state authorities by creating a relationship of trust and learning from each other's experiences.

Conclusions

This paper has examined the criminal offences of economic and industrial espionage in Austria and in Switzerland by analysing the basic understanding, the legal structure, the underlying legal concepts, and the legal framework of these offences, as well as their practical importance regarding conviction rates. The legal comparison between the Austrian and the Swiss legal order shows significant similarities in some respects and fundamental differences in other respects.

In Austria and in Switzerland, the topic of industrial and economic espionage has been given increasing attention by the legislature, scholars, and practitioners, especially over the last few years. Austria and Switzerland have a long history of recognising the criminal offences of industrial and economic espionage. Although industrial and economic espionage has changed dramatically, especially regarding the modi operandi of spies and the increasingly international dimensions of spying, so far neither the Austrian nor the Swiss legislature has made any recent amendments regarding the criminal offences of economic and industrial espionage.

In Austria and Switzerland, the offences of industrial and economic espionage are contained in the Criminal Code on the one hand, and in the Act against Unfair Competition on the other hand. Many of these offences lead to a broad scope of criminal liability due, inter alia, to their legal structure, and to the use of imprecise wording which gives the law enforcement authorities room for various interpretations. On the one hand, the complexity of industrial and economic espionage, coming in many different forms and rapidly changing manifestations, requires the code regarding economic and industrial espionage to give law enforcement at least some flexibility in order to be able to respond effectively. On the other hand, the broad wording of some offences of industrial and economic espionage can result in a lack of legal certainty. Legal provisions must be sufficiently clear to enable people who are subject to them to regulate their conduct accordingly. The requirements of the principle of legal certainty are especially high in the area of criminal law. By and large, the desire to formulate the offences as precisely as possible has to be weighed against the need to provide for provisions which enable the law enforcement authorities to combat economic and industrial espionage efficiently.

In both the Austrian and Swiss system, the offences of industrial espionage usually need some sort of initiative from the person aggrieved by the offender in order to have the criminal proceedings started. This means that the legal concept of prosecution on request is well known in Austria and Switzerland. However, there are fundamental differences regarding the procedural consequences resulting from this concept. In Switzerland, it is the public prosecutor who conducts the investigation

procedures, whereas in Austria regarding offences prosecuted only on request, there is no public prosecutor but only a private prosecutor, who is the person who is entitled to file the criminal complaint. The position of the private prosecutor under Austrian law is disadvantageous, as there is no official investigation procedure, which means that the private prosecutor has to collect the necessary evidence on his/her own. Furthermore, the private prosecutor has a substantial risk of having to bear the costs resulting from the criminal proceedings. The legal concept of the private prosecutor and its interpretation in practice unnecessarily weaken the protection of trade secrets in Austria.

In Austria, the new legal definition of trade secrets provided for by the EU Directive on the protection of undisclosed know-how and business information will certainly have an impact worth monitoring on the civil and criminal remedies for the protection of trade secrets.

While both jurisdictions have weaknesses in this area of the law, especially in the procedural framework of the offences of industrial and economic espionage, these weaknesses can and should be easily amended.

Overall, it has to be stressed that the phenomenon of economic and industrial espionage poses new challenges for criminal law and criminal proceedings. In order to achieve success in fighting industrial and economic espionage through the means of criminal law, victims must inform the law enforcement authorities and further cooperate with them. Cooperating with authorities has to be made as easy as possible for victims. This means, inter alia that the victims of trade secret infringement should clearly know which authority is in charge. It is necessary to ensure that victims of trade secret infringements do not see criminal proceedings as an additional burden. That means, for example, that the provisions governing the criminal proceedings have to guarantee that trade secrets are adequately protected during the course of the proceedings. The EU Directive on the protection of trade secrets provides guidelines to preserve the confidentiality of trade secrets in the course of the proceedings (Article 9 of the Directive). However, because of the scope of the Directive, these rules only apply to civil proceedings available to the owner of the trade secret.

Until now neither the Austrian nor the Swiss legislature, nor the law enforcement authorities have exploited the full potential of criminal law to contribute to the fight against economic and industrial espionage.

References

Ackermann-Blome, N., and J. Rindell. 2018. Should Trade Secrets be Protected by Private and/or Criminal Laws? A Comparison Between Finish and German Laws. *Journal of Intellectual Property Law Practice* 13 (1): 78–87.

Anderson, R., C. Barton, R. Böhme, R. Clayton, M. van Eeten, M. Levi, T. Moore, and S. Savage. 2013. *The Economics of Information Security and Privacy*, 265–300. Berlin: Springer.

Austrian Government. 2013. Erfolgreich. Österreich – Arbeitsprogramm der österreichischen Bundesregierung für die Jahre 2013 bis 2018. https://www.justiz.gv.at/web2013/file/2c94848642ec5e0d0142fac7f7b9019a.de.0/regprogramm.pdf. Accessed 1 Mar 2019.

Austrian Government. 2017. Zusammen. Für unser Österreich – Regierungsprogramm 2017–2022. https://www.bundeskanzleramt.gv.at/documents/131008/569203/Regierungsprogramm_2017–2022.pdf/b2fe3f65-5a04-47b6-913d-2fe512ff4ce6. Accessed 1 Mar 2019.

Baker & McKenzie. 2013. Study on Trade Secrets and Confidential Business Information in the Internal Market—Final Study, April 2013, Prepared for the European Commission, Ref. Ares(2016)98815—08/01/2016.

Baranowski, A., and R. Gaβl. 2016. Anforderungen an den Geheimnisschutz nach der neuen EU-Richtlinie. *Betriebs-Berater* 2563–2569.

Baudenbacher, C., and J. Glöckner. 2001. Art. 23 UWG. In *Lauterkeitsrecht – Kommentar zum Gesetz gegen den unlauteren Wettbewerb (UWG)*, ed. C. Baudenbacher. Basel: Helbing Lichtenhahn Verlag.

Bazzi, C. 2015. *Internationale Wirtschaftsspionage: Eine Analyse des strafrechtlichen Abwehrdispositivs der Schweiz*. Zürich: University of Zurich.

BBC. 2010. HSBC Admits Huge Swiss Bank Data Theft. 11 March. http://news.bbc.co.uk/2/hi/business/8562381.stm. Accessed 4 Mar 2019.

Bertel, C., K. Schwaighofer, and A. Venier. 2018. StGB. In *Österreichisches Strafrecht – Besonderer Teil I*, 14th ed, 75–168b. Vienna: Springer.

Birklbauer, A., M.J. Hilf, and A. Tipold. 2017. StGB. In *Strafrecht – Besonderer Teil I*, 4th ed, 75–168b. Vienna: Springer.

Birmingham Post. 2009. Industrial Espionage has Existed Since Dawn of Time, 16 April. https://www.birminghampost.co.uk/business/industrial-espionage-existed-dawn-time-3947455. Accessed 30 Mar 2019.

BKA. 2018. Pressemitteilung vom 06.12.2018: Die Konkurrenz schläft nicht, sie spioniert. https://www.bka.de/SharedDocs/Pressemitteilungen/DE/Presse_2018/pm181206_WISKOS.pdf;__blob=publicationFile&v=5. Accessed 27 Mar 2019.

BM.I., IV, FH Campus Wien, and WKO. 2015. Wirtschafts- und Industriespionage in österreichischen Unternehmen 2015. https://www.bvt.gv.at/401/files/StudieWirtschafts-undIndustriespionageinoesterreichischenUnternehmen2015.pdf. Accessed 26 Mar 2019.

BM.I., IV, WKO, and FH Campus Wien. 2010. Gefahren durch Wirtschafts- und Industriespionage für die österreichische Wirtschaft – Studie 2010. https://www.bvt.gv.at/401/files/Studie_WIS_Executive_Summary.pdf. Accessed 23 Mar 2019.

Bollhöfer, E., and A. Jäger. 2018. Wirtschaftsspionage und Konkurrenzausspähung – Vorfälle und Prävention bei KMU im Zeitalter der Digitalisierung. https://wiskos.de/files/pdf4/M3_Komplett_Online_neu_doi.pdf. Accessed 5 Mar 2019.

Brenner, S.W., and A.C. Crescenzi. 2016. State-Sponsored Crime: The Futility of the Economic Espionage Act. *Houston Journal of International Law.* 28: 389–465.

Bruckmüller, G., and K. Krückl. 2019. Wenn Mitarbeiter Firmendaten "mitnehmen". Die Presse, January 21. https://diepresse.com/home/recht/rechtallgemein/5565732/Wenn-Mitarbeiter-Firmendaten-mitnehmen. Accessed 28 Feb 2019.

Brunstein, J. 1887. *Der Schutz des Fabrikations- und Geschäftsgeheimnisses*. Vienna.

Burgstaller, M. 1980. Der strafrechtliche Schutz wirtschaftlicher Geheimnisse. In *Geheimnisschutz im Wirtschaftsleben*, ed. H.G. Ruppe. Vienna: ORAC.

Busekist, K., and F. Racky. 2018. Hinweisgeber- und Geschäftsgeheimnisschutz – ein gelungener Referentenentwurf? *Zeitschrift für Rechtspolitik*, 135–138.

Carl, S. 2017. An Unacknowledged Crisis—Economic and Industrial Espionage in Europe. In *Europe in Crisis: Crime, Criminal Justice and the Way Forward. Essays in honour of Nestor Courakis. Vol. II: Essays in English, German, French, and Italian*, ed. C. Spinellis et al., 1315–1326. Athens: Sakkoulas Publications.

Carl, S., and M. Kilchling, eds. Forthcoming. *Economic and Industrial Espionage in Germany and Europe: History, Developments and Present Legislative Frameworks in a Comparative Perspective*.

Carl, S., M. Kilchling, S. Knickmeier, and E. Wallwaey. 2017. Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa – Eine rechtsvergleichende Betrachtung, Forschung aktuell, Freiburg i.Br. https://wiskos.de/files/pdf4/WISKOS_RIB.pdf. Accessed 29 Mar 2019.

Cassani, U. 1996. Die Anwendbarkeit des schweizerischen Strafrechts auf internationale Wirtschaftsdelikte (Art. 3–7 StGB), *Schweizerische Zeitschrift für Strafrecht*, 237–262.

Corporate Trust. 2014. Cybergedon. https://www.corporate-trust.de/wp-content/uploads/2016/06/CT-Studie-2014_DE.pdf. Accessed 26 Mar 2019.

Czapracka, K.A. 2008. Antitrust and Trade Secrets: The U.S. and the EU Approach. *Santa Clara Computer & High Technology Law Journals* 24: 207–273.

Dann, M., and J.W. Markgraf. 2019. *Das neue Gesetz zum Schutz von Geschäftsgeheimnissen, NJW*, 1774–1779.

David, L., and R. Jacobs. 2012. *Schweizerisches Wettbewerbsrecht: Eine systematische Darstellung des Gesetzes gegen den unlauteren Wettbewerb und des Kartellgesetzes, sowie der wettbewerbsrechtlichen Nebengesetze und der Grundsätze der Schweizerischen Kommission für die Lauterkeit in der Werbung*, 5th ed. Bern.

Delmas-Marty, M. 2003. The Contribution of Comparative Law to a Pluralist Conception of International Criminal Law. *Journal of International Criminal Justice* 1: 13–25.

Desai, S. 2018. Shhh—It's a Secret: A Comparison of the United States Defend Trade Secrets Act and European Union Trade Secrets Directive. *Georgia Journal of International and Comparative Law* 46: 481–513.

Eder-Rieder, M. 2010. StGB. In *Salzburger Kommentar zum Strafgesetzbuch*, ed. O. Triffterer, C. Rosbaud, and M. Hinterhofer, 256. Vienna: LexisNexis.

Eicker, A. 2010. Zur Strafbarkeit des Kopierens und des Verkaufs sowie des Ankaufs von Bankkundendaten als schweizerisch-deutsches Tatgesehen. *Jusletter* 30 (08): 2010.

Eicker, A. 2011. Ist die im Ausland geäusserte Bereitschaft, in der Schweiz illegal erlangte Daten anzukaufen, wirklich als Staatsschutzdelikt verfolgbar? *Jusletter* 30 (01): 2011.

Eicker, A. 2013. § 3: Der räumliche und zeitliche Geltungsbereich des nationalen Wirtschaftsstrafrechts. In *Wirtschaftsstrafrecht der Schweiz*, ed. J.B. Ackermann and G. Heine, 57–82. Bern: Stämpfli.

Engin-Deniz, E. 2015. *Angriffs- und Verteidigungsrecht im Privatanklageverfahren*, 81–86. Vienna: Medien & Recht.

Engin-Deniz, E. 2017. *OGH: Kein Recht des Privatanklägers auf Teilnahme an der gerichtlich angeordneten Durchsuchung und Sicherstellung*, 225–230. Vienna: Medien & Recht.

Eser, A. 1997. The Importance of Comparative Legal Research for the Development of Criminal Sciences. In *Law in Motion: Recent Developments in Civil Procedure, Constitutional, Contract, Criminal, Environmental, Family & Succession, Intellectual Property, Labour, Medical, Social Security, Transport Law*, ed. R. Blancpain, 492–517. The Hague: Kluwer.

Eser, A. 2017. *Comparative Criminal Law*. München: C. H. Beck.

European Commission. 2016. Trade Secrets. http://ec.europa.eu/growth/industry/intellectual-property/trade-secrets_en. Accessed 28 Feb 2019.

European Union, Directive (EU) 2016/943 of the European Parliament and the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure, OJ L 157, 15.6.2016. 1–18.

European Union Intellectual Property Office. 2018. The Baseline of Trade Secret Litigation in the EU Member States. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2018_Baseline_of_Trade_Secrets_Litigations_in_EU_Member_States/2018_Baseline_of_Trade_Secrets_Litigations_in_EU_Member_States_EN.pdf. Accessed 26 Jun 2019.

Expertenkommission. 1895. *2 Verhandlungen über den Vorentwurf zu einem schweizerischen Strafgesetzbuch*.

Explanatory remarks to the government bill (Austria). 1965. Addenda to the Stenographic Protocol of the National Council No. 650, 10th Legislation Period.

Explanatory remarks to the government bill (Austria). 2004. Addenda to the Stenographic Protocol of the National Council No. 25, 22th Legislation Period. https://www.sbg.ac.at/ssk/stpo/2004_i_19_rv25_erl.pdf. Accessed 27 Mar 2019.

Explanatory remarks to the government bill (Austria). Addenda to the Stenographic Protocol of the National Council No. 375, 26th Legislation Period. 1–11. https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00375/fname_722341.pdf. Accessed 28 Feb 2019.

Explanatory Report of the Federal Council (Switzerland). 2016. Entwurf zur Verordnung zum Bürgerrechtsgesetz, April 2016. https://www.so.ch/fileadmin/internet/vwd/vwd-agem/pdf/Buergerrecht/VO_bund_bericht.pdf. Accessed 26 Mar 2019.

Fabrizy, E.E. 2018. *Strafgesetzbuch: StGB samt ausgewählten Nebengesetzen – Kurzkommentar*, 13th ed. Vienna: Manz.

Fidler, D.P. 2013. Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies. *Insights* 17 (10).

Gassauer-Fleissner, C. 2018. Der Entwurf für eine UWG-Novelle zur Umsetzung der RL zum Schutz von Geschäftsgeheimnnissen. *ÖBl*, 256–259.
Gassauer-Fleissner, C. 2019. Die letzten Geheimnisse um die Umsetzung der GeschäftsgeheimnisRL sind gelüftet. *ÖBl*, 60–62.
Global Innovation Index. 2019. 12th Edition. https://www.globalinnovationindex.org/Home. Accessed 27 Jul 2019.
Graf, D. 2016. *Strafbewehrter Geheimnisverrat im grenzüberschreitenden Kontext, Schweizerische Juristen-Zeitung*, 193–200.
Hafter, E. 1937. Wirtschaftsspionage und Wirtschaftsverrat. *Festgabe Fritz Fleiner zum 70*, 203–225. Zürich: Geburtstag.
Hauck, R. 2019. *Was lange währt … – Das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) ist in Kraft, GRUR-Prax*, 223–225.
Heimgartner, S. 2018. Art. 23 UWG. In *UWG Kommentar*, ed. R. Heizmann and L.D. Loacker. Zürich: Dike.
Heine, G. 2010/2011. *Entwendete und staatlich angekaufte Bankdaten – viel Lärm um nichts?*, 525–544. London: ASA.
Heiβl, G. 2016. *PStSG – Polizeiliches Staatschutzgesetz – Kurzkommentar*. Vienna: Vorbemerkungen.
Heller, K.J., and M.D. Dubber. 2011. Introduction: Comparative Criminal Law. In *The Handbook of Comparative Criminal Law*, ed. K.J. Heller and M.D. Dubber, 1–11. Stanford: Stanford University Press.
Hofmarcher, D. 2018a. *Der Privatankläger muss draußen bleiben – kein Recht auf Teilnahme an Hausdurchsuchungen, ecolex*, 57–58.
Hofmarcher, D. 2018b. *Entwurf zur Umsetzung der GeschäftsgeheimnisRL, ecolex*, 783–786.
Hofmarcher, D., and S. Kühteubl. 2017. Geschäftsgeheimnisse: Unternehmen müssen handeln. Der Standard, 10 March. https://derstandard.at/2000053793210/Geschaeftsgeheimnisse-Unternehmen-muessen-handeln. Accessed 28 Feb 2019.
Horak, M. 2009. *Das neue Privatanklageverfahren – Schwierigkeiten in der Praxis und neue Reformpläne, Österreichische Juristen-Zeitung*, 212–217. Vienna: Manz.
Hostettler, U., et al. Forthcoming. *Studie "Wirtschaftsspionage in der Schweiz" im Auftrag des Nachrichtendienstes des Bundes*.
Husmann, M. 2015. Wirtschaftlicher Nachrichtendienst: Schutz kollektiver Rechtsgüter – Bedrohung für den Einzelnen. In *TOP secret – Geheimnisschutz und Spionage: 8. Schweizerische Tagung zum Wirtschaftsstrafrecht*, ed. J.B Ackermann and M.J. Hilf, 59–112.
Husmann, M. 2019. Art. 273 StGB. In *Basler Kommentar Strafrecht II*, 4th ed, ed. M.A. Niggli and H. Wiprächtiger. Basel: Helbing Lichtenhahn Verlag.
Isenring, B., and L. Quiblier. 2017. *Der Preis der Sicherheit, Sicherheit & Recht*, 127–140.
Jescheck, H.H. 1981. The Significance of Comparative Law for Criminal Law Reform. *Hastings International and Comparative Law Review*. 5: 1–25.
Jositsch, D., and M. Conte. 2015. *Strafbestimmungen im Bundesgesetz gegen den unlauteren Wettbewerb, Zeitschrift für Immaterialgüter-Informations- und Wettbewerbsrecht*, 437–446. Zürich: Schulthess Juristische Medien.
Jung, H. 2005. *Wertende (Straf-)Rechtsvergleichung – Betrachtungen über einen elastischen Begriff, Goltdammer`s Archiv für Strafrecht*, 2–10.
Jung, H. 1998. Grundfragen der Strafrechtsvergleichung. *JuS* 1–7.
Kary, C. 2018. Geschäftsgeheimnisschutz wird anspruchsvoller. Die Presse, 26 June. https://diepresse.com/home/wirtschaft/recht/5454720/Novelle_Geschaeftsgeheimnisschutz-wird-anspruchsvoller. Accessed 28 Feb 2019.
Kilchling, M., and S. Carl. 2016. Wirtschaftsspionage im globalen Markt: Sind die Ermittlungsstrukturen in Deutschland noch zeitgemäβ? In *Grenzenlose Sicherheit? – Gesellschaftliche Dimensionen der Sicherheitsforschung*, ed. P. Zoche et al., 183–196.
Killias, M., and G. Gilliéron. 2013. Art. 23 UWG. In *Basler Kommentar zum Bundesgesetz gegen den unlauteren Wettbewerb*, ed. R.M. Hilty and R. Arpagaus. Basel: Helbing Lichtenhahn Verlag.
Klötzer-Assion, A. 2018. *Mein Geheimnis, Dein Geheimnis: EU-Geheimnisschutzrichtlinie und deren Umsetzung in nationales (Straf)Recht, WiJ*, 175–181.
Knickmeier, S. Forthcoming. Spies Without Borders? Overview About the Phenomenon of Economic and Industrial Espionage and Outcomes of Criminal Proceedings in Germany and Selected European Countries. *Security Journal*.
Köck, E. 2010. *Wirtschaftsstrafrecht*. Vienna.

Köhler, H. 2019. Vorbemerkungen vor §§ 17 bis 19: Schutz von Geschäftsgeheimnissen. In *Gesetz gegen den unlauteren Wettbewerb*, 37th ed, ed. H. Köhler et al. München: Beck.

Konopatsch, C., and M.J. Hilf. 2019. Austria. In *Economic and Industrial Espionage in Germany and Europe: History, Developments and Present Legislative Frameworks in a Comparative Perspective*, ed. S. Carl and M. Kilchling, 15–34. Berlin.

Konopatsch, C., M. Rentsch, P. Stocker, and M.J. Hilf. 2019. Switzerland. In *Economic and Industrial Espionage in Germany and Europe: History, Developments and Present Legislative Frameworks in a Comparative Perspective*, ed. S. Carl and M. Kilchling, 575–593. Berlin.

Korn, G., and P. Zöchbauer. 2017. StPO. In *Wiener Kommentar zur Strafprozessordnung*, 2nd ed, ed. H. Fuchs and E. Ratz, 71. Vienna: Manz.

KPMG-AG. 2013. E-crime – Computerkriminalität mit Kennzahlen für Österreich und die Schweiz. https://www.kpmg.at/uploads/media/eCrime_Studie.pdf. Accessed 26 Mar 2019.

Kremnitzer, M. 2011. Some Reflections on Comparative Criminal Law. In *Strafrechtsvergleichung als Problem und Lösung*, ed. S. Beck et al., 29–40. Baden-Baden: Nomos.

Leister, A. 2019. *"Angemessene Geheimhaltungsmaßnahmen" – Handlungsbedarf in der Praxis durch Neudefinition des Geschäftsgeheimnisbegriffs, GRUR-Prax*, 75–77.

Lewisch, P. 2017. StGB. In *Wiener Kommentar zum Strafgesetzbuch*, 2nd ed, ed. F. Höpfel and E. Ratz, 121–124. Vienna: Manz.

Liebscher, V. 1976. Die Wirtschaftsdelikte im österreichischen Strafrecht. *Zeitschrift für die gesamte Strafrechtswissenschaft* 88: 261–280.

Maaßen, S. 2019. *"Angemessene Geheimhaltungsmaßnahmen" für Geschäftsgeheimnisse, GRUR*, 352-360.

Marko, R. 2017. Bei Inlandsspionage werden Betriebe alleingelassen, Der Standard, 28 March. https://derstandard.at/2000054861389/Bei-Inlandsspionage-werden-Betriebe-alleingelassen. Accessed 25 Mar 2019.

Meyer, F. 2011. Internationalisierung und Europäisierung des Rechts als Herausforderung der Rechtsvergleichung. In *Strafrechtsvergleichung als Problem und Lösung*, ed. S. Beck et al., 87–102, Baden-Baden: Nomos.

Meyer, H.H. 1955. Banking Secret and Economic Espionage in Switzerland. *The George Washington Law Review* 23: 284–327.

Midtgaard, A. 2018. *Defining a "Trade Secret": In the US and the EU, Ecolex*, 791–792.

Miller, H. 2019. EX-UBS Employee Charged with Data Theft on Trail in Switzerland, Bloomberg 7 January. https://www.bloomberg.com/news/articles/2019-01-07/ex-ubs-employee-charged-with-data-theft-on-trial-in-switzerland. Accessed 4 Mar 2019.

Ministry of Interior et al. 2011. TOP SECRET: Wirtschafts- und Industriespionage – Handbuch KNOW-HOW-Schutz für die österreichische Wirtschaft. http://www.bvt.gv.at/401/files/Handbuch_WIS.pdf. Accessed 1 Mar 2019.

Niggli, M.A., and N. Hagenstein. 2019. Art. 162 StGB. In *Basler Kommentar Strafrecht II*, 4th ed, ed. M.A. Niggli and H. Wiprächtiger. Basel.

NZZ. 2010. *Bankdaten-Diebstahl*. Zürich: Neue Zürcher Zeitung.

NZZ. 2012. *Hehlerei mit Bankdaten im Visier*. Zürich: Neue Zürcher Zeitung.

Oehler, D. ed. 1981. *Der strafrechtliche Schutz des Geschäfts- und Betriebsgeheimnisses in den Ländern der europäischen Gemeinschaft sowie in Österreich und der Schweiz*. Cologne.

Ohly, A. 2019. *Das neue Geschäftsgeheimnisgesetz im Überblick, GRUR*, 441–451.

Orozco, D. 2013. Amending the Economic Espionage Act to Require the Disclosure of National-Security-Related Technology Thefts. *Catholic University Law Review* 62: 877–912.

Passarge, M. 2018. *Der Entwurf eines Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) – Das Gegenteil von gut gemacht ist gut gemeint, Compliance Berater*, 144–147.

Pedrazzini, M.M., and F.A. Pedrazzini. 2002. *Unlauterer Wettbewerb – UWG*, 2nd ed. Bern.

Pfenninger, H.F. 1918. Das Vergehen des unerlaubten Nachrichtendienstes. *Zeitschrift für Schweizerisches Recht*, 134–167.

PwC. 2011. Cybercrime in the Spotlight. Swiss Economic Crime Survey. https://www.ub.unibas.ch/digi/a125/sachdok/2012/BAU_1_6031831.pdf. Accessed 26 Mar 2019.

Reid, M. 2016. A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing With This Global Threat? *University of Miami Law Review* 70 (1): 1–73.

Riedo, C. 2004. *Der Strafantrag*. Basel: Helbing Lichtenhahn Verlag.

Riedo, C. 2019. Vor Art. 30. In *Basler Kommentar Strafrecht II*, 4th ed, ed. M.A. Niggli and H. Wiprächtiger. Basel: Helbing Lichtenhahn Verlag.

Salimi, F. 2017. *Der polizeiliche Staatsschutz – Schutz oder Bedrohung der Freiheit – Eine Analyse aus polizeirechtlicher Sicht, ÖJZ*, 115–121.
Schaffner, D., and P. Spitz. 2016. Art. 23 UWG. In *Bundesgesetz gegen den unlauteren Wettbewerb (UWG) – Stämpflis Handkommentar*, 2nd ed, ed. P. Jung and P. Spitz. Bern: Stämpfli Verlag AG.
Schafheutle, K. 1972. *Wirtschaftsspionage und Wirtschaftsverrat im deutschen und schweizerischen Strafrecht*. Freiburg i.Br.
Scherp, D., and D. Rauhe. 2019. *Datenklau!? Entwurf eines Gesetzes zum Schutz von Geschäftsgeheimnissen – Teil 1, Compliance Berater*, 20–24.
Schlund, M. 2018. *Schutz von Geschäftsgeheimnissen: alte Tatbestände in neuem Gewand, NJW-Spezial*, 376–377.
Schmidt, E. 1981. Der strafrechtliche Schutz des Geschäfts- und Betriebsgeheimnisses in der Schweiz. In *Der strafrechtliche Schutz des Geschäfts- und Betriebsgeheimnisses in den Ländern der europäischen Gemeinschaft sowie in Österreich und der Schweiz*, ed. D. Oehler, 199–233. Cologne.
Schramböck, M. 2002. *Der Schutz von Geschäfts- und Betriebsgeheimnissen mit Exkurs zur Rechtslage in den USA – Praxishandbuch*. Vienna: Manz.
Schwarz, J. 2013. Geheimnisschutz und Spionagestrafrecht. In *Wirtschaftsstrafrecht in der Schweiz: Hand- und Studienbuch*, ed. J.B. Ackermann and G. Heine, 555–609. Bern: Stämpfli.
SECO. 2018. Statistische Angaben zu den Beschwerden. https://www.seco.admin.ch/seco/de/home/Werbe_Geschaeftsmethoden/Unlauterer_Wettbewerb/statistische_angaben.html. Accessed 16 Aug 2019.
SECO. 2017. Statistische Angaben zu den Beschwerden. https://www.seco.admin.ch/seco/de/home/Werbe_Geschaeftsmethoden/Unlauterer_Wettbewerb/statistische_angaben.html. Accessed 16 Aug 2019.
Seiler, M. 2015. *Balance zwischen Sicherheit und Freiheit*, 130–133. Digma.
Settelen, M. 2019. Chinesische Forscher könnte demnächst wegen Wirtschaftsspionage an die USA ausgeliefert werden, Neue Zürcher Zeitung, 10 July. https://www.nzz.ch/wirtschaft/chinesischer-wissenschafter-koennte-demnaechst-an-die-usa-ausgeliefert-werden-ld.1494789. Accessed 30 Jul 2019.
Sieber, U. 2006. Strafrechtsvergleichung im Wandel – Aufgaben Methoden und Theorieansätze der vergleichenden Strafrechtswissenschaft. In *Strafrecht und Kriminologie unter einem Dach*, ed. U. Sieber and H.-J., 78–151. Berlin.
Sosnova, N. 2016. EU Directive Proposal: Trade Secrets. *Marquette Intellectual Property Law Review* 20: 45–77.
Stratenwerth, G., G. Jenny, and F. Bommer. 2010. *Schweizerisches Strafrecht, Vol. I: Straftaten gegen Individualinteressen*, 7th ed. Bern: ZStrR.
Stratenwerth, G., and W. Wohlers. 2010. *Schwarzgeld – Strafbarkeitsrisiken für die Mitarbeiter Schweizer Banken*, 429–446. Bern: ZStrR.
Swiss Federal Intelligence Service. 2015. PROPHYLAX. https://www.vbs.admin.ch/de/themen/nachrichtenbeschaffung/wirtschaftsspionage.detail.publication.html/vbs-internet/de/publications/nachrichtendienst/Prophylax.pdf.html. Accessed 1 Mar 2019.
Swiss Federal Intelligence Service. 2017. Faktenblatt vom 01.09.2017 "Was macht der NDB gegen Spionage?". https://www.vbs.admin.ch/de/themen/nachrichtenbeschaffung/wirtschaftsspionage.detail.document.html/vbs-internet/de/documents/faktenblaetter/nachrichtendienst/Faktenblatt-Spionage-de.pdf.html. Accessed 5 Mar 2019.
Swiss Federal Intelligence Service. 2018. Merkblatt "Wirtschaftsspionage". https://www.vbs.admin.ch/de/themen/nachrichtenbeschaffung/wirtschaftsspionage.detail.document.html/vbs-internet/de/documents/nachrichtendienst/wirtschaftsspionage/Merkblatt-Wirtschaftsspionage-d%20.pdf.html. Accessed 1 Mar 2019.
Swissinfo. 2019a. Chinese researcher in 'economic warfare' cases loses appeal, 8 July. https://www.swissinfo.ch/eng/extradition_chinese-researcher-in–economic-warfare–case-loses-appeal-/45083604. Accessed 30 Jul 2019.
Swissinfo. 2019b. Swiss agree to extradite Chinese researcher in US corporate espionage case, 16 July. https://www.swissinfo.ch/eng/economic-warfare_swiss-approve-extradition-of-chinese-researcher-in-us-corporate-espionage-case-/45099950. Accessed 30 Jul 2019.
Thiele, C. 2007. StGB. In *Salzburger Kommentar zum Strafgesetzbuch*, ed. O. Triffterer, C. Rosbaud, and H. Hinterhofer, 122–124. Vienna: Manz.
Thiele, C. 2016. UWG. In *UWG online: Kommentar zum Gesetz gegen den unlauteren Wettbewerb*, ed. A. Wiebe and G.E. Kodek. Vienna: Manz.
Thilo, E. 1917. *Die Bekämpfung der Spionage in der Schweiz, Schweizerische Juristen-Zeitung*, 185–191.

Trebeck, J., and L. Schulte-Wissermann. 2018. *Die Geheimnisschutzrichtlinie und deren Anwendbarkeit – Auswirkungen auf Compliance and Whistleblowing im deutschen Arbeitsrecht, NZA*, 1175–1180.
Trechsel, S., and H. Vest. 2018. Art. 273 StGB. In *Schweizerisches Strafgesetzbuch: Praxiskommentar*, ed. S. Trechsel and M. Pieth. Zürich: Dike.
Trechsel, S., and M. Jean-Marc-dit-Bressel. 2018. Art. 30 StGB. In *Schweizerisches Strafgesetzbuch: Praxiskommentar*, ed. S. Trechsel and M. Pieth. Zürich: Dike.
Trim, P. 2002. Counteracting Industrial Espionage Through Counterintelligence: The Case for a Corporate Intelligence Unit and Collaboration with Government Agencies. *Security Journal* 15: 7–24.
Verfassungsschutzbehörden des Bundes und der Länder. 2014. Wirtschaftsspionage – risiko für Unternehmen, Wissenschaft und Forschung. Report, Bundesamt für Verfassungsschutz und die Verfassungsschutzbehörden der Länder. https://www.verfassungsschutz.de/embed/broschuere-2014-07-wirtschaftsspionage.pdf. Accessed 8 Jul 2019.
Voigt, P., V. Hermann, and J.F. Grabenschröer. 2019. *Das neue Geschäftsgeheimnisgesetz – praktische Hinweise zu Umsetzungsmaßnahmen für Unternehmen, Betriebs-Berater*, 142–146.
Von Rütte, B. 2017. *Das neue Bürgerrechtsgesetz*, 202–214. Anwaltsrevue.
Wallwaey, E., E. Bollhöfer, and S. Knickmeier. 2019. *Wirtschaftsspionage und Konkurrenzausspähung: phänomenologie, Strafverfolgung und Prävention in ausgewählten europäischen Ländern*. Berlin: Springer.
Weigend, T. 2012. Criminal Law and Criminal Procedure. In *lgar Encyclopedia of Comparative Law*, 2nd ed, ed. J.M. Smits, 261–278. Cheltenham: Edward Elgar.
Wessely, W. 2013. StGB. In *Handbuch Strafrecht – Besonderer Teil*, vol. 1, ed. I. Mitgutsch and W. Wessely, 122–124. Vienna: Manz.
Zipf, H. 1981. StGB. In *Wiener Kommentar zum Strafgesetzbuch*, 1st ed, ed. F. Höpfel and E. Ratz, 122. Vienna: Manz.
Zirm, J. 2013. Spionage: "Das war versuchter Firmenmord", die Presse, August 22. https://diepresse.com/home/wirtschaft/international/1444292/Spionage_Das-war-versuchter-Firmenmord?from=suche.intern.portal. Accessed 30 Jul 2019.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.