Cybercrime in Selected European Countries

Filip Radoniewicz

Abstract This study does not claim to exhaust all the abundant comparative legal issues. Therefore, it has been limited to discussing the penal provisions of eight European countries, without going into detailed considerations on issues related to e.g. form of offences committed or the liability of legal persons. The overarching intention was to present as diverse regulations as possible.

All countries whose regulations were discussed have signed and ratified the Convention on Cybercrime and are members (except United Kingdom) of the European Union, which resulted in their obligation to implement Framework Decision 2005/222 on attacks against information systems, and the need to adapt their regulations to the provisions of Directive 2013/40, which has replaced this decision.

1 Introduction

Firstly, it should be emphasised that the present study does not claim to exhaust the whole of the complex comparative-law issue, particularly as only one of over twenty Chapters has been devoted to it. Therefore, it has been narrowed down to discussing the substantive penal-law regulations of several European countries, without entering into detailed deliberations on the issues related to, for example, the stages of a crime, and forms of accessory liability for a crime, or the liability of legal persons, while the overriding intention was to present as diverse regulations as possible.¹

All the states, whose regulations have been discussed here, signed and ratified the Convention on Cybercrime, and they are, or were (the United Kingdom), Member States of the European Union, which is why their regulations are based on Council

¹For more information about cybercrime law in other European countries see Radoniewicz (2016), pp. 359–421.

F. Radoniewicz (✉)

Akademickie Centrum Polityki Cyberbezpieczeństwa/Academic Center for Cybersecurity Policy, Akademia Sztuki Wojennej w Warszawie/War Studies University in Warsaw, Warsaw, Poland

e-mail: filip.radoniewicz@radoniewicz.eu

Framework Decision 2005/222/JHA of the 24th of February 2005 concerning attacks against information systems and Directive 2013/40/EU of the European Parliament and of the Council of the 12th of August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ EU L 218, 14.08.2013, p. 8.). Consequently, similar solutions have been adopted in these countries.

As regards an offence involving illegal access, most legislators make the offender's penal liability conditional on the elimination of safeguards designed to protect against unauthorised access to the data or system. Such a requirement was introduced in Czech, Estonian, French and German regulations.

Regarding the remaining offences, which are the subject of this study (assaults on the integrity of computer data and computer systems and networks, computer eavesdropping and the production, possession and distribution of hacking tools), the regulations in question demonstrate certain similarities, differing mainly in the level of detail and types of aggravated crimes and, with regard to offences against the integrity of data and computer systems, in the introduction of the requirement for the offender to cause a consequence (Spain), the significant importance of the data to the victim (Germany), and action with the intent to cause harm (Spain).

Unique solutions are found in the laws developed on the basis of English Law (Computer Misuse Act of 1990). Several countries followed suit, including Malta, whose regulations are discussed in this chapter, and some non-European countries, such as Singapore.²

The texts of the penal laws under discussion, in addition to respective Government websites, are available, for example, via the Council of Europe's Legislationline service³ and on the website of the World Intellectual Property Organisation.⁴

2 The Czech Republic

The Czech Penal Code⁵ is the most recent of the discussed laws. It was adopted on the 8th of January 2009,⁶ and entered into force after a *vacatio legis* period of almost one year, on the 1st of January 2010. The Czech legislator included computer-related

²The Act No. 19/1993 of 30 August 1993—Computer Misuse and Cybersecurity Act, as amended by the Act of 31 July 2007 (Chapter 50A), <http://statutes.agc.gov.sg>, accessed on 15.12.2020.

³www.legislationline.org, accessed on 15.12.2020.

⁴<http://www.wipo.int/wipolex>, accessed on 15.12.2020.

⁵The Penal Code of the Czech Republic of 8 January 2009 (Zákon trestní zákoník; Trestní zákoník), Zákon č. 40/2009 Sb., <http://aplikace.mvcr.cz/sbirka-zakonu>, accessed on 15.12.2020.

⁶This happened after the Czech Republic signed the Convention on Cybercrime, which took place on 9 February 2005, but before its ratification, which took place on 22 August 2013 (for the Czech Republic, the Convention entered into force on 1 December 2013).

crimes, being the subject of this study, in two chapters of the Code. The vast majority of them, namely the offences of unauthorised access, unauthorised alteration of data, disruption of networks and the development and distribution of “hacking tools”, have been classified as offences against property (Division V of the Code). Computer eavesdropping has been rightly considered to be an attack on the right to privacy, and therefore it is laid down in Chapter 2 “Offences against personal interests and the secrecy of private life and correspondence” of Division II of the Code, entitled “Offences against freedom, personal interests and privacy of private life and correspondence.” The discussion regarding the Czech regulation should begin with this issue.

Computer eavesdropping is categorised in Section 182(1) (b), and Subsection (c) of that Section defines the basic type of such an offence. According to these provisions, imprisonment of up to two years or a prohibition of an activity (*zákaz činnosti*) may be imposed on an offender who committed an intentional breach of the confidentiality of communication (data, text, images, sounds), which may be attributed to a particular participant in the data exchange process or user to whom the data are transferred via electronic communication networks or via private transmission of computer data to, from or within a computer system, including by analysing electromagnetic emissions generated by the computer system in connection with the data transfer. The same sanction shall be imposed on anyone who, with the intention of causing damage to a third party or of gaining an illegal advantage for himself or a third party, discloses information (constituting a secret) not intended for him or her, which he or she obtained from a letter, telegram, telephone conversation or transmission via electronic communication network, or who uses such information (Section 182(2)). The Czech Penal Code is quite strict and prescriptive.⁷ There are numerous types of aggravated crimes, and computer eavesdropping may serve as a good example here. When identifying its aggravated type under Section 182(3), the legislator indicated as aggravating circumstances the commission of the acts referred to in Section 182(1) or 182 (2) within an organised group, acting with a malicious intent or with the aim of causing significant damage,⁸ or with the intention of obtaining a substantial benefit for the offender or for a third party. Such an offence is punishable by imprisonment for a period of six months to three years or a prohibition of an activity. Whereas, if the perpetrator of the act described in Section 182(1) or 182(2) is a public officer, or causes large-scale damage or, while committing the act, intends to obtain a considerable benefit for himself/herself or for a third party, he/she shall be liable under Section 182(4), which provides for a term of imprisonment of between one and five years or a fine. Pursuant to Section 182(5), a similar sanction (i.e. imprisonment of between one and five years, a fine and, moreover, a prohibition of an activity) is imposed on a person, who being an

⁷More on the Czech Penal Code in W. Radecki, *Nowy czeski kodeks karny*, Prok. i Pr. 2009, No. 7-8, p. 185 et seq.

⁸A significant damage—as defined in Article 138(1) of the Czech Penal Code—is a damage of at least CZK 500,000, and a large-scale damage is damage of at least CZK 5,000,000.

employee of a postal or telecommunications service provider, computer system operator or anyone engaged in rendering communication services:

- (1) commits an act referred to in Section 182(1) or 182 (2), or
- (2) intentionally facilitates the commission of the said acts by a third party, or
- (3) alters or loses a document sent by post or courier service or a message sent privately as computer data, by telegraph, telephone or other similar means.

The above offence has an aggravated type, representing a (particularly) serious crime.⁹ In accordance with Section 182 (6), the perpetrator, whose conduct meets the criteria of an offence under Section 182 (5), and causes large-scale damage or who acts with the intention of obtaining substantial benefits for himself/herself or a third party, shall be subject to the penalty of imprisonment for a period of three to ten years.

The group of computer crimes listed in Division V of the Code includes the unauthorised access to the computer system or its part (Section 230). Infringement of security measures constitutes a condition for the perpetrator to be indicted for such offence. The offence is subject to imprisonment for a period of up to two years, a prohibition of an activity or the forfeiture of movable property.

The second offence mentioned in this Section is the act of obtaining access by the perpetrator to a computer system or information medium (there is no requirement that such access be unauthorised) and:

- (1) the unlawful use of data stored in that computer system or on that information medium, or
- (2) the unlawful erasure or other destruction or damage, alteration, deletion of data or rendering the data stored on that computer system or on that information medium unusable, or
- (3) falsification or alteration of data stored in a computer system or information medium in order to make it appear to be accurate, or make the system or medium treat it as if it were accurate, whether or not such data are directly legible and understandable, or
- (4) unlawful input of data into a computer system or onto an information medium or otherwise affects computer software or hardware or other technical device for data processing.

The perpetrator of this offence shall be liable to a term of imprisonment of up to three years, a prohibition of activity or the forfeiture of property.

The offences discussed above, as well as computer eavesdropping, have a wide range of aggravated types. They are defined, first and foremost, in Section 230(3), under which it is stipulated that the penalty of imprisonment for a period of six

⁹Pursuant to Section 14(2) of the Czech Penal Code, misdemeanours include all unintentional acts and those intentional acts for which the penal law provides for a prison sentence with an upper limit of up to five years. Serious crimes include all those offences that are not misdemeanours. On the other hand, particularly serious crimes are all those which are punishable by imprisonment, the upper limit of which is at least ten years (Section 14(3)).

months to four years shall be imposed on a person who commits the act referred to in Section 230(1) or 230(2) with the intention of causing damage to a third party, or other harm, or of obtaining a substantial benefit for himself/herself or a third party, or with the intention of limiting the operation of a computer system or other technical device used for data processing. Secondly, pursuant to Section 230(4), the offence referred to in Section 230(1) or 230(2) shall be punishable by a term of imprisonment of one year to five years or by a fine, if the offender:

- (1) acted as a member of an organised group,
- (2) caused significant damage,
- (3) caused by his conduct a serious disruption in the activities of a State administration body, local government body, court or other public authority,
- (4) obtained a significant benefit for himself or for a third party,
- (5) caused a serious disruption of the activities of a legal person or natural person acting as an entrepreneur.

On the other hand, pursuant to Section 230(5), the offender who, as a result of the committed offence, has caused large-scale damage or thus obtained for himself/herself or a third party significant benefits, shall be subject to a penalty of imprisonment for a period of three to eight years. As already indicated above, due to the level of the sanction, this offence is classified as a serious crime.

Section 231 of the Czech Penal Code criminalises acts related to the development of, and trade in, hacking tools. Under this provision, the penalty of imprisonment for a period of up to two years, prohibition of activity or forfeiture of property shall be imposed on anyone who, with the intention of violating the secrecy of correspondence, an offence under Section 182(1)(b) and 182(1)(c) or of obtaining access to a computer system or information medium, an offence under Section 230(1) and 230(2), produces, markets, imports, exports, transports, offers, arranges, disposes of, or otherwise makes available to himself/herself or a third party, distributes or stores:

- (1) any device or component, tool or other means, including a computer program designed or adapted to gain unauthorised access to an electronic communication network, computer system or parts thereof, or
- (2) a computer password, access code or other similar means by which it is possible to access a computer system or parts thereof.

The Czech legislator provided for two types of aggravated offences. The first, referred to in Section 231(2), is punishable by imprisonment of up to three years, a prohibition of activity or the forfeiture of property, and the aggravating features include the offender's commitment of the act within an organised group or the obtaining of a significant benefit by the offender for himself/herself or for a third party. The second type, provided for in Section 231(3), is punishable by imprisonment for a term of between six months and five years, and the aggravating feature includes the offender's obtaining for himself/herself or for a third party a benefit of considerable value.

According to Section 232 of the Czech Penal Code, the offence of damage to a computer system and information medium and interference with a computer device

due to negligence (unintentionally) is an offence, which is not covered by any other legislation. It is applicable to a person who violates, with gross negligence, his or her obligations arising from his or her employment, profession, position or function, whether by law or by contract, and:

- (1) destroys, damages, alters or otherwise renders unusable data stored in a computer system or on an information medium, or
- (2) interferes with software or hardware on a computer or other technical data processing device,

resulting in a significant damage to the property of a third party.

This offence is subject to a maximum of six months' imprisonment, prohibition of activity and/or forfeiture of property. Section 232(2) provides for its aggravated type depending on the value of the damage caused, in the case of causing large-scale damage, the offender may be sentenced to imprisonment of up to two years (and a prohibition of activity or forfeiture of property).

3 Estonia

Estonian Penal Code (Karistusseadustik)¹⁰ was adopted on the 6th of June 2001 and became valid into force on the 1st of September 2002. The Republic of Estonia is one of the earliest countries to ratify the Convention on Cybercrime, it did so on the 12th of May 2003 (the Convention on Cybercrime entered into force on the 1st of July 2004). The offences covered by this study are listed in Chapter 13 "Offences against property", Division 1 "Offences against ownership", Subdivision 2 "Damage to property" (Sections 206 and 207 of the Estonian Penal Code) and in Division 2 ("Offences against all types of property"), Subdivision 3 "Unlawful use" (Sections 216¹, 217).

Furthermore, Section 206 defines the offence of impacting computer data by illegally altering, deleting, or damaging computer data in a computer system, or rendering such data inaccessible. This act is punishable by a fine or imprisonment of up to three years. Nevertheless, where the offence in question is:

- (1) directed against the data processed in a significant number of computer systems or programs or devices specified in Section 216¹ (hacking tools) were used to commit thereof;
- (2) an act committed within a group;

¹⁰The Penal Code of the Republic of Estonia (RT I 2001, 61, 364). The text is available on the website of the official journal, Riigi Teataja (<https://www.riigiteataja.ee>). Since 1 June 2010, Riigi Teataja has been published exclusively on the Internet. English translations of some legislation, including the Penal Code, are available on this website (and updated relatively frequently).

- (3) targeted against data processed in a computer system of strategic significance for the State;
- (4) it has caused significant damage;

the perpetrator shall be subject to a fine or up to five years' imprisonment (Section 206(2)).

Illegal interference with a computer system or disruption of its operation, consisting of downloading data from it, sending data to it, deleting, damaging or altering the data processed therein or rendering such data inaccessible, constitutes an offence under Section 207(1). It is subject to a financial penalty or imprisonment of up to three years. The aggravated type is provided for in Section 207(2). The aggravating features are similar to those of the act under Section 206(2):

- (1) the offence was directed against a significant number of computer systems or was committed using the programs or devices or as defined in Section 216¹¹;
- (2) the offence was committed within a group;
- (3) the impact of the act includes an influence on, or interference with, a computer system of strategic or public service significance;
- (4) the offence caused substantial damage.

However, the sanction is identical to that provided for in the case of the offence under Section 206(2), it is a financial penalty or a penalty of imprisonment of up to five years.

Division 2, which refers to offences against all types of property, includes the provision laid down in Section 217 (Subdivision 3 "Unlawful use") under which unlawful access to a computer system by eliminating or circumventing security measures is punishable as a criminal offence. The sanction for this offence is a fine or imprisonment of up to three years. However, if the perpetrator has caused significant damage, gained access to a computer system processing information constituting State secrets (or other qualified types thereof) or the computer system, to which he gained access is of strategic significance, he or she shall be sentenced to imprisonment for a period of up to five years.

Furthermore, Section 216¹ criminalises conducts, which are preparatory activities to the commission of computer crimes, consisting of supplying, preparing, possessing, distributing or disclosing in any other way, in order to be used to commit an offence indicated in this provision (i.e. defined in Section 206, 207, 213¹¹ or 217), or with the intention of facilitating its perpetration by a third party, a device or a computer program created or adapted specifically for committing the offences referred to in this provision or the means of gaining access to a computer system. The perpetrator of such an act shall be subject to a financial penalty or to

¹¹This provision defines the offence of computer fraud, consisting in causing financial loss as a result of gaining unauthorised access to a computer program or data or altering, deleting, destroying or blocking access to a computer program or data or otherwise interfering unlawfully with the processing of data in order to obtain a financial benefits.

imprisonment of up to two years. The forfeiture of property directly derived from the committed crime, as defined in Section 83, may be ordered against the offender.

On the other hand, among the offences against fundamental freedoms (Part 2 in Chapter 10 “Offences against civil and political rights”); Section 156(1) stipulates the offence of violating the secrecy of correspondence “by letter or via other means of communication”. The perpetrators of this act are only subject to a fine. It appears that the term “other means of communication” can be understood as electronic means of communication. As regards the aggravated type (Section 156 (2)), this offence is punishable by a fine or a penalty of up to one year’s imprisonment and the aggravating feature is the perpetrator’s exercising his or her powers.¹²

4 France

The current French Penal Code of 1992¹³ (Code Pénal) replaced the Napoleonic Code Pénal (so-called Ancien Code Pénal) of 1810. Computer-related crimes were already included in its original version, and are defined in Chapter III (“Offences against automated data processing systems”), Title II (“Other offences against property”) of Book III (“Crimes and misdemeanours against property”), in the provisions of Articles 323-1 to 323-8, which derive their current wording from the amendments to the Code Pénal made under Acts 2004-575 of the 21st of June 2004, 2009-526 of the 12th of May 2009, 2012-410 of the 27th of March 2012, 2013-1168 of the 18th of December 2013, 2014-1353 of the 13th of November 2014 and 2015-912 of the 24th of July 2015.

Article 323-1 defines the offence of fraudulent obtaining (*frauduleusement*)¹⁴ of an access to all or part of an automated data-processing system or to maintain access to such a system. The latter characteristic refers to the perpetrator’s behaviour consisting in obtaining authorised access (i.e. on the basis of his or her powers) and then gaining access to parts of the system to which he or she is not authorised to enter. The offence under Article 323-1 is punishable by two years’ imprisonment and a fine of 60,000 EUR. When the behaviour of the offender causes destruction or

¹²Furthermore, in this chapter, the following acts have been criminalised: unlawful disclosure of personal data under Article 157, under Article 157¹—disclosure of sensitive personal data, and under Article 157²—identity theft understood as using the identity of a third party in order to gain access to data or cause harm to another person or conceal the offence.

¹³The Penal Code of the French Republic was adopted in sections. The first four books (as Acts No: 92-683; 92-684; 92-685 and 92-686) were published in Official Journal No. 169 of 23.07.1992. Book V was adopted under Act No. 92-1336 and published in Official Journal No. 296 of 23 December 1992 [cf. Rogacka-Rzewnicka (2004), pp. 456–457]. The text of the Code is available in the official Legifrance database: <http://www.legifrance.gouv.fr> (accessed on 15.11.2020).

¹⁴For the occurrence of this offence, it is not required that the offender breaks the security measures, provided that the fraudulent (deceptive) nature of his or her act is proven, which may be evidenced by circumventing the security features by e.g. using spyware or a Trojan horse and thus entering into possession of a password or access code to the system. Cf. Féral-Schuhl (2010), pp. 915–916.

alteration of the data stored in this system or any disruption (deterioration) in the functioning of the system, the offender shall be liable to a penalty of three years' imprisonment and a fine of up to 100,000 EUR (Article 323-1(2)).

Article 323-1(3) provides for an aggravated type of both of the above mentioned offences. The aggravating features include the type of system and the nature of the data processed therein. In the event of the State system where personal data are processed, the offenders are liable to a five-year imprisonment sentence and a fine of 150,000 EUR.

Another offence against automated data processing systems is to hinder or interfere with the operation of such a system, as specified in Article 323-2. The perpetrator is punishable by imprisonment for a period of five years and a fine of 150,000 EUR. As in the case of the offence involving fraudulent access, considering the type of the system attacked and the nature of the data processed in it (the State system processing personal data), the legislator provided for an aggravated type of such an offence, punishable by imprisonment for a period of seven years and a fine of 300,000 EUR.

Article 323-3 criminalises the act of maliciously entering data into an automated data-processing system or of fraudulently downloading, retaining, copying, transmitting, deleting or altering data within that system. The perpetrator of such an act is punishable by five years' imprisonment and a fine of 150,000 EUR. Likewise, as in the aforementioned offences, the constituent feature of the aggravated type of the offence is the nature of the object affected by the commission of the offence, in the case of a State system that automatically processes personal data. This act is punishable by imprisonment for a period of seven years and a fine of 300,000 EUR (Art. 323-3(2)).

By means of an amendment under Act No. 2004-575, following the adoption of the Convention on Cybercrime,¹⁵ the provision in Art. 323-3-1 relating to "hacking tools" was added. On this basis, a given conduct is punishable if it is performed without a legal basis (i.e. unauthorised), which may in particular include conducting research or ensuring information security, involving the import, possession, sale, transmission or making available (including via the Internet) of any device, tool, computer program (or data of any kind) designed or specially adapted to commit one or more of the offences referred to in Articles 323-1 to 323-3. As regards the penalty envisaged, an unusual solution was applied. The perpetrators are subject to a punishment for the offence for which a "hacking tool" can be used. If it can be applied in several offences, such a perpetrator is subject to the most severe penalty. Therefore, he or she is treated virtually as an accomplice in committing an offence (somewhat equivalent to aiding in the commission of a crime in the Polish legal code), with the significant difference, however, that his or her liability is not of an accessory nature, i.e. it does not matter whether the "hacking tool" was used to commit the offence, or in the case of committing such an offence, whether the perpetrator's guilt was proven.

¹⁵Representatives of France participated in the work on the Convention on Cybercrime. It was signed by them on 23 November 2001, ratified on 10 January 2006 and entered into force for France on 1 May 2006.

Attempting to commit any of the above mentioned offences is punishable by law. The offender shall be liable, as it is the case in Polish law, within the limits provided for the offence actually committed (Article 323-7).

Article 323-4 criminalises membership in a criminal group or arrangement formed in order to prepare one or more of the offences referred to in Articles 323-1 to 323-3-1. Participation in such a group is punishable on the grounds of its undertaking at least one act demonstrating such an objective for its establishment, subject to the penalty provided for the act, which the members of the group or association intended to commit. In the event that the preparatory measures the group has taken could lead to acts bearing the features of several offences, and it is therefore necessary to choose the specific legal basis for the penalty, the provision stipulating that the most severe penalty shall apply. Under the Act 2014-1353 of the 13th of November 2014, Article 323-4-1 was added, specifying an aggravated type of offences as defined in Articles 323-1 to 323-3-1. The aggravating feature includes the fact that an offence has been committed against a public data processing system within an organised group, which is punishable by ten years' imprisonment and a fine of 300,000 EUR.

In Code Pénal, there are other offences against data or data processing systems. First and foremost, emphasis should be placed on Chapter VI ("Offences against personal rights"), Title II ("Offences against persons"), Book II ("Serious crimes and offences against persons"). In Section IV ("Violation of secrecy"), in par. 2 ("Violation of secrecy of correspondence"), in Article 226-15(2), the offence of computer eavesdropping is defined as an intentionally malicious act of interception, diversion, use or disclosure of correspondence sent, transmitted or received via an electronic communications network or the installation of devices intended for that purpose. The punishments for this offence include one year of imprisonment and a fine of 45,000 EUR. But when it is committed by the spouse or cohabiting partner of the victim or the partner linked to the victim by a civil solidarity pact, this act is punishable by two years' imprisonment and a fine of 60,000 EUR. . Section V ("Violations of personal rights resulting from the processing of computer files") consolidates the provisions criminalising unlawful processing of personal data (in particular, acts performed in breach of Act No. 78-17 of the 6th of January 1978 concerning information technology, computer files and freedoms).

5 Germany

In the Penal Code of 1871 in force in Germany (Strafgesetzbuch—StGB)¹⁶ the offences in question have been defined in Chapter XV, which contains offences against private secrecy (computer espionage, Section 202a, interception of data,

¹⁶German Penal Code of 15 May 1871 (Strafgesetzbuch—StGB) as published on 13 November 1998 (BGBl. I S. 3322). Its contents (also in English, but not fully updated) can be accessed on the Internet via Gesetze im Internet (<http://www.gesetze-im-internet.de>).

Section 202b, offences related to hacking tools, Section 202 c) and in Chapter XXVII among offences involving damage to property (data alteration, Section 303a, and computer sabotage, Section 303 b).

The offence of computer espionage as defined in Section 202a (*Ausspähen von Daten*) entails unauthorised access by the perpetrator, for himself/herself or for a third party, to data not intended for them, provided that his or her actions are accompanied by the infringement of the specific security measures protecting against unauthorised access. In Subsection 2 of the aforementioned Section, it is clarified that only data, which are stored or transmitted electronically or magnetically or in any other imperceivable (*nicht unmittelbar wahrnehmbar*—not perceivable by the senses) manner shall be considered as data. Computer espionage is punishable by imprisonment for a period of up to three years or a fine.

The next offence listed in Chapter XV, interception of data (*Abfangen von Daten*) as defined in Section 202b of the StGB, shall be committed by anyone who intercepts data, for himself/herself or a third party (within the meaning of Section 202a (2) of the StGB), which is not intended for them during their non-public transmission or electromagnetic emissions generated by a data processing system during such transmission, without authorisation. The perpetrator of such an offence shall be subject to imprisonment of up to two years or a fine, unless a more severe penalty is provided for in specific legislation.

In accordance with Section 202c of the StGB, the development and distribution of hacking tools is punishable as a criminal offence. Under this provision, it is prohibited to undertake preparatory activities leading to the commission of the offences referred to in Section 202a and Section 202b, consisting of the development or procurement (for oneself or for a third party), selling or transferring to a third party, disseminating, or making available in any other way, passwords or other security codes enabling access to data within the meaning of Section 202a (2), or computer programs designed to commit a criminal offence. This offence is punishable by imprisonment of up to one year or a fine. Pursuant to Section 202b (2), the provisions of Section 149(2) and (3) apply accordingly to this offence.¹⁷ In other words, the perpetrator is not punished if the following two conditions are met jointly. First, the offender will resign from committing the planned offence and, at the same time, will prevent the threat of a third party's continuing preparations for, or perpetrating, the offence, or prevents the completion of the offence. Secondly, at the same time (also on a voluntary basis) the offender shall destroy or render unusable the instruments intended to commit the offence (if they still exist and are suitable for such use), or notify the State authorities of their existence or deliver such tools to the responsible authorities. On the other hand, in a situation when the danger of preparing for, or committing, an offence has been prevented without the intervention of the perpetrator, or its commission has been made impossible, and thus the perpetrator is unable to fulfil the first condition for avoiding punishment specified in Section 202c, such condition is nonetheless deemed satisfied if the perpetrator

¹⁷Section 149 of the StGB criminalises preparatory actions for the crime of money counterfeiting.

demonstrates with his or her conduct that he or she voluntarily and zealously sought to achieve this.

As mentioned, subsequent offences against data and computer systems have been classified by the German legislator as property destruction offences (Chapter XXVII). In Section 303a, the offence of data modification as unlawful deletion, blocking, alteration or rendering useless has been identified. The perpetrator of this offence is subject to a penalty of imprisonment of up to two years or a fine. In accordance with Subsection 2, attempting to commit this act is punishable and, in accordance with Subsection 3, Section 202c shall apply accordingly to preparation for committing such offence.

The offence of computer sabotage referred to in section 303b is an act committed by a person who significantly (materially) interferes with the processing of data, which are essential to a third party through:

- (1) committing the act referred to in Section 303a (1), or
- (2) entering or transmitting data with the intention of causing harm to a third party, or
- (3) destroying, damaging, rendering useless, suppressing or modifying an electronic data-processing system or data carrier.

The perpetrator is subject to imprisonment of up to three years or a fine. Attempting is punishable (Section 303b(3)). However, on the basis of Subsection. 5, Section 202c may apply accordingly in the case of preparation for committing such offence.

Section 303b (2) and (4) provides for aggravated types of computer sabotage. In the first case, the aggravating feature is the weight of the data processed in it. If the undisturbed functioning of the system is of significant importance to someone else's economic activities, another person's company or a State office, the perpetrator shall be subject to a penalty of imprisonment of up to five years or a fine. In the second case (which is in fact of the aggravated type of act under Subsection. 2), the aggravating feature involves particularly serious circumstances of the offence under Subsection 2. Their occurrence results in the possibility of sentences ranging from six months' to ten years' imprisonment. The legislator decided that such particularly serious incidents usually occur in a situation where the perpetrator:

- (1) causes substantial financial loss, or
- (2) has made proceeds from criminal activities a stable source of income or is a member of a criminal organisation, which has been formed to commit the offence of computer sabotage on a continuous basis, or
- (3) through crime, he or she disrupts the provision of vital goods or services to the population, or impairs the security of the State.

To conclude the discussion on *Strafgesetzbuch*, it is worth mentioning Section 269. It may be applied (in some cases in conjunction with Section 303a) to aggravate the liability for IP-spoofing. In its basic type (Section 269 (1)), it is an

offence punishable by imprisonment of up to five years or a fine,¹⁸ imposed on a person who, for the purpose of fraudulent legal transactions, collects or modifies evidentiary data by falsifying or altering a document, which could be made in the course of the transaction or which uses such data.¹⁹

6 The United Kingdom

The main objective of the Computer Misuse Act 1990 (CMA)²⁰ was primarily to combat the offence of gaining unauthorised access to computer data and programs. Very soon it became obvious that it needed to be amended, it was emphasised, above all, the powerlessness of the law enforcement authorities in their fight against the perpetrators of DoS attacks, which could not be brought to justice on the basis of the CMA. Given these opinions and the fact that the United Kingdom signed the Convention on Cybercrime²¹ and the necessity to implement the provisions of Framework Decision 2005/222, which has been made by means of adopting the Police and Justice Act 2006,²² a number of substantial changes were introduced. For instance, the provision of Section 3 criminalising the disruption of computer operations was thoroughly modified (inter alia, enabling the prosecution of perpetrators of DoS attacks on its basis), and the provision of Section 3A, criminalising the development and distribution of hacking tools, was introduced. Furthermore, sanctions have been reinforced.²³ Under the most recent amendment (Serious Crime Act 2015²⁴) the offence of causing, or threatening to cause, considerable damage has been added.

Currently, the Computer Misuse Act contains provisions criminalising four categories of infringement:

- (1) acts related to obtaining unauthorised access (unauthorised access to a computer program or data in electronic form—Section 1; unauthorised access with intent to commit further offences—Section 2);

¹⁸For aggravated types of the offence, the penalty can be even up to ten years' imprisonment (see section 269(3) of StGB).

¹⁹Cf. Hoeren (2012), pp. 492–493.

²⁰An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes (c. 18); the discussed legal acts are available on the official website <http://www.legislation.gov.uk>, accessed on 15.05.2020. CMA applies throughout the UK.

²¹The United Kingdom signed the Convention on Cybercrime on 23 November 2001, but ratified it until 25 May 2011, followed by its entry into force on 1 September 2011.

²²Police and Justice Act 2006 (c. 48).

²³Smith (2007), pp. 1019–1020; Murray (2010), pp. 338–340, 346–348; Walden (2007), pp. 174–175.

²⁴Serious Crime Act 2015 (c. 9).

- (2) unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, network etc.—Section 3;
- (3) unauthorised acts causing, or creating risk of, serious damage—section 3ZA;
- (4) making, supplying or obtaining “hacking tools”—Section 3A.

The offence of unauthorised access, as defined in Section 1 (1), consists of causing a computer to perform any activity with the intent to secure access to any program or to data stored in any computer. This offence may be committed only intentionally. Section 1(1) (c) indicates that the offender must be aware, at the time of the action, that he is not entitled to access the data or the program. Simultaneously, it is stipulated that the intent of the perpetrator does not need to be to secure unauthorised access to a specific program or data (or even to a specific type of program or data), or to data or software held in any particular computer [Section 1 (2)]. In other words, it is not necessary to prove that the perpetrator of the act in question intended to obtain specific information or acted for specific reasons in order to bring charges against him or her. The intent of the offence is not a decisive factor in determining whether an offence has been committed or not, it could be, for example, to break the safeguards to test one's skills or simply to make a “joke”. Moreover, it is also not necessary to prove that the perpetrator has actually gained access in order to attribute criminal liability to a given act. It is sufficient for him or her to initiate the appropriate measures resulting in operations that may enable him or her to do so.

The amount of the penalty that may be imposed depends on the type of proceedings under which this is to take place. In the case of summary proceedings (this is a procedure without a jury, currently conducted by a single professional judge), the offence is punishable by imprisonment of not more than twelve months or a fine, or both. In general, these are the highest penalties that may be imposed under this procedure. However, if the judge considers it necessary to impose a more severe sanction, the case may be referred to the Crown Court, which may impose a sentence of up to two years' imprisonment or a fine (without limiting its amount), or both at the same time.

Section 2 of the Computer Misuse Act criminalises the practice of obtaining unauthorised access with the intent to commit or facilitate the commission of further offences. It is committed by the offender whose conduct has the attributes of an offence referred to in Section 1, which constitutes a kind of activity preceding the commission of another offence, as referred to in that Section, or activity facilitating the commission of such an offence (whether by himself or herself or a third party).

It is irrelevant to the existence of the offence in question whether a “further offence” was committed at the time of unauthorised access or whether it happened later. The perpetrator of this offence is also liable if this further offence has not been committed, or even if it was impossible.²⁵ The perpetrator is liable to a more severe penalty than the one provided for unauthorised access only. It is punishable by

²⁵Cf. Clough (2013), p. 51.

imprisonment of up to five years or a fine (or both). However, where summary procedure is applied, the situation is analogous to that of the case of an unlawful act referred to in Section 1.

The second group of offences provided for in the Computer Misuse Act includes conduct consisting of the perpetrator's intentional or reckless unauthorised act in relation to a computer, which is intended or likely to disrupt the operation of a computer, network, etc. This category includes two types of offences, which differ in the *mens rea* component. The first one is committed with intentional fault, the perpetrator commits an unauthorised act with the intention of causing the consequences indicated in Section 3 (2), i.e., to impair the operation of any computer, to prevent or hinder access to any program or data held on any computer, to impair the operation of any such program or the reliability of any such data. The second type of crime in question may be committed out of recklessness. Under Section 3 (3), the perpetrator, when undertaking unauthorised acts as referred to in Section 3 (1) is reckless as to whether the consequences indicated in Section 3 (2) occur (i.e. program or data impairment etc.). For both categories of the criminal act in question, the offender's conduct must be accompanied by the awareness that the act is unauthorised. It is not mandatory to prove that such conduct has led to any impairment in the operation of a computer [(or to any other consequence laid down in Section 3 (2))].²⁶ Furthermore, as in the case of the offence of unauthorised access, it is irrelevant from the perspective of the offence in question whether the offender's action was directed against a particular computer, program or specific data, or a computer, program or data of any specific type (cf. comments to Section 1). Consequently, the impairment, prevention or hindering of access is also punishable if it is transitory in nature. Under proceedings held before the Crown Court, a prison sentence of up to ten years or a fine may be imposed. Under the summary proceedings—as in the case of the offences discussed earlier—it is possible to impose the highest penalties provided for by this type of procedure.

Section 3ZA defines the offence of unauthorised causing, or creating risk of, serious damage. This is an unauthorised act in relation to a computer (as defined in Section 3). The condition for liability is that the perpetrator, at the time of committing the act, is aware that he or she is not authorised to perform the actions that he or she is attempting. This offence may be committed both intentionally and with recklessness. The concept of serious damage of a material kind is understood broadly. According to Section 3ZA (2), it is damage to human welfare or to the environment, in any place it occurs (or may occur), or damage to the economy or national security of any country. Whereas, pursuant to Section 3 ZA (3), damage to human welfare is understood as:

- (1) loss to human life,
- (2) human illness or injury,
- (3) disruption of money, food, water, energy or fuel supplies,

²⁶Cf. Smith (2007), pp. 1020–1023.

- (4) disruption of the communication system (understood as the transmission of information),
- (5) disruption of facilities for transport,
- (6) disruption of the services related to health.

Section 3ZA (4) stipulates that it is immaterial whether the perpetrator's behaviour was the sole or principal cause of the damage, as well as whether it was a direct or indirect consequence of his or her act.

Due to the seriousness of the crime, the proceedings for the aforementioned offence are exclusively held before the Crown Court, which may impose a sentence of up to fourteen years' imprisonment, a fine, or both. However, where the act of the perpetrator has resulted in the death of a human being or damage to health or substantial harm to national security (or has brought about a threat thereof), the perpetrator shall be liable to imprisonment for life or to a fine, or to both.

Provisions criminalizing the conduct of producing, supplying or obtaining "hacking tools" are contained in Section 3A of the CMA. Three prohibited acts are defined. The first one includes making, adapting, supplying and offering to supply any "article" (this term should be understood as any programs and data held in electronic form)²⁷ with the intention that it should be used to commit (or to assist in the commission of) any of the offences referred to in Sections 1, 3 or 3ZA. It is immaterial to the liability of the offender whether the tool created (provided) was used to commit the offence, or even whether it was suitable for that purpose. The offender's intention to enable a third party to commit a crime is crucial. The act may therefore be committed only intentionally, in contrast to the second offence, which is described in Section 3A, which may also be committed out of recklessness. It consists in supplying or offering to supply any "article" believing that it is likely to be used to commit (or assist in the commission of) any of the offences specified in Sections 1, 3 or 3ZA of the CMA. The third offence identified in Section 3A is the obtaining of any "article" with the intention of using it to commit (or assist in the commission of) any of the offences under Sections 1, 3 or 3ZA or of its being supplied to a third party with the intention of using it to commit (or assist in the commission of) any of the offences under Sections 1, 3 or 3ZA.

In summary proceedings, as in the case of other offences, the maximum penalties provided for under such procedure may be imposed, while in the case of conviction on indictment before the Crown Court, the offender may be sentenced to imprisonment of up to two years, to a fine, or both.

²⁷In order to hold the perpetrator liable under this provision, it is sufficient that the object of his or her action is a single "article".

7 Spain

The applicable Penal Code of the Kingdom of Spain²⁸ (Código Penal) was adopted on the 23rd of November 1995, replacing the Code of 1870, which had been subject to multiple amendments.

Spain signed the Convention on CyberCrime on the 23rd of November 2001 and ratified it on the 3rd of June 2010. The offences in question are defined in Articles 197, 197 bis, 197 ter, 197 quater and 198 (Title X “Offences against privacy, the right to personal image and the inviolability of housing”, Chapter I “Discovery and disclosure of secrets”) and Articles 264, 264 bis, 264 ter (Title XIII “Offences against property and social and economic order”, Chapter VIII “Damage”) of Código Penal. The Spanish regulation in its present form is the result of a comprehensive amendment introduced under the Act of the 31st of March 2015²⁹ (which became valid on the 1st of July 2015), harmonising the Code regulations with EU laws.

According to Article 197(1), an imprisonment sentence of one to four years and a fine, or a sentence of twelve to twenty four months is imposed upon the perpetrator who, in order to discover (uncover) the secrets or to breach privacy of another person, without his or her consent, acquires any letters, e-mails or any other personal documents or belongings, intercepts telecommunications of that nature or uses technical means to eavesdrop on the transmission, recording or reproduction of sound or image or other manifestations of interpersonal communication. Pursuant to Paragraph 2, the same penalty may be imposed on an offender who, without being authorised to do so, intercepts, uses or alters proprietary³⁰ data of a personal or family nature stored as files on a computer, on information or electronic media, or in any similar data filing system, whether public or private, to the detriment of a third party (i.e. both the person directly harmed by the actions of the perpetrator, the data holder, i.e. usually the data subject, and any other third party who is affected by the act for any reason). The same penalty shall be imposed on anyone who, without being authorised to do so, accesses such data by any means, and alters or uses such data to the detriment of the owner or third party.

Furthermore, a sentence of between two and five years’ imprisonment is provided for a person who disseminates, discloses or transfers to third parties data or facts coming to his or her knowledge as a result of committing the acts referred to in Article 197(1) and (2) or images obtained in this way (Subparagraph 1 of Article 197 (3)). A person who is aware of the illegal origin of the data or images (i.e. the fact

²⁸Organic Law No. 10/1995 of 23 November 1995 (BOE No. 281 of 24 November 1995). The text is available on the Iberlex website (<http://www.boe.es>, accessed on 15.12.2020).

²⁹Organic Law No. 1/2015 of 30 March 2015 (BOE No. 77 of 31 March 2015).

³⁰According to the views of legal commentators and the views expressed in the case law of the Spanish Supreme Court, this concept is broader than sensitive data. It contains all the private data that is usually not disclosed to a wide circle of people, meaning persons other than closest relatives and friends. Cf. Letai, p. 246.

that they were obtained by means of one of the offences referred to in Article 197(1)-(2)), if he or she did not participate in obtaining the data or images, but performs the aforementioned activities, shall be liable to a fine and a sentence of between twelve and twenty four months or to imprisonment of between one and three years (Article 197(3), Subpara. 2).

Further Código Penal provisions in Art. 197 provide for a number of types of aggravated crimes under Article 197(1-2). Pursuant to Paragraph 4, the perpetrator of these offences shall be subject to more severe sanctions (imprisonment of three to five years) if he or she was the person responsible for the files, storage medium, electronic archive or register in which the data were processed or which were under his or her custody, or if the data, which were the subject of the offence were personal data and the perpetrator was not authorised to use them. Whereas, where private data classified as proprietary data (as referred to in Para. 2) are disseminated, transmitted or disclosed to a third party, the offender shall be subject to a penalty within the upper half of the range provided by law (Article 197(4), Subpara. 2). The nature of data being the object of offence constitutes a factor aggravating criminal liability pursuant to Article 197(5), in which it is stipulated that where the object of the offences referred to in the previous provisions includes data concerning religion, religious denomination, health, ethnic origin, race, sexual orientation (i.e. sensitive data), or where the victim is a minor or a person with disability in need of special care, the penalty imposed should fall within the upper half of the range provided by law.

In accordance with Article 197(6), if the offence referred to in the preceding paragraphs is committed for the purpose of making a profit, the offender shall be sentenced to a penalty, which falls within the upper half of the penalty range provided by law. However, if the offence affected data referred to in Para. 6 (sensitive data), the offender is liable to even more severe sentences, ranging from to seven years' imprisonment.

The first Subparagraph of Para. 7 of the discussed Article provides for a type of criminal act, which does not constitute a typical computer crime, but which may be committed using information technology. According to this provision, a person who, without the consent of the person concerned, distributes, discloses or transmits to third parties photographs or audio-visual recordings, which he or she has obtained with his or her consent in his or her place of residence or in other circumstances, which demonstrate their private nature and the intention not to disclose them to others shall be liable to imprisonment for a term of between three months and one year, or a fine and a sentence of between six and twelve months ("domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros") if disclosure is likely to infringe the privacy of that person.

The perpetrator can face a more severe penalty (imposed at the upper half of the penalty range) if he or she is or has been the spouse of the victim or has been in a similar relationship with him or her (but not necessarily cohabitation), or if the victim was a minor or a person with disability in need of special care, or if the offence was committed for the purpose of financial gain (Article 197(7) Subpara. 2).

The subsequent articles (197 bis, 197 ter, 197 quater), added under the amendment of the 31st of March 2015, are intended to implement the provisions of Directive 2013/40. Article 197 bis (1) provides for a penalty of six months to two years' imprisonment for obtaining or facilitating unauthorised access to the whole or any part of an information system by any means or method and after infringing security measures, or for remaining in the information system despite the opposition of the person, who has the right to prohibit it, (thus exceeding the limits of the powers conferred on the user). The second Subparagraph of that provision criminalises the unauthorised interception, by technical means, of non-public transmissions of computer data from, or within, an information system, including electromagnetic emissions. The said act is punishable by imprisonment for a period of three months to two years or a fine and a sentence of between three and twelve months.

The issue of the interrelation between the provisions of Art. 197 bis (1) and (2), and those of Art. 197 are particularly interesting. Unfortunately, the framework of this study does not allow this issue to be analysed.

The criminalisation of acts relating to hacking tools is provided for in Art. 197 ter. It prohibits, on pain of imprisonment for a term of between six months and two years or a fine of between three and eighteen months, unauthorised production, procurement for use, import or making available in any way to third parties, with the intention of facilitating the commission of any of the offences referred to in Article 197 (1) and (2) or Article 197 bis: a computer program designed or adapted primarily to commit such offences, or a computer password, access code or similar data enabling access to all or part of an information system.

Art. 197 quater provides for the aggravation of criminal liability where the acts referred to in this Chapter of the Code have been committed within the framework of a criminal organisation or group, a higher level of punishment than is provided in the Code may be imposed.

Article 198 defines the aggravated type for all offences referred to in Article 197. The aggravating feature is related to the *mens rea* component of the offence. This provision refers to persons who, acting as public officers and taking advantage of their function, commit an offence, which fulfils the characteristics of any of the prohibited acts specified in Article 197. Such offender shall be subject to a penalty appropriate to the offence in its upper half range. In addition, he or she is liable to an "absolute prohibition" (*la inhabilitación absoluta*) ordered for a period from six to twelve years.

The offences against the integrity of computer data and systems have been identified in Article 264 of the Código Penal, which has been thoroughly modified by the aforementioned amendment, and in the subsequent articles added as a result of the amendment. Under Article 264(1), a penalty of six months to three years' imprisonment shall be imposed on a person who, by any means whatsoever, without right, erases, damages, deteriorates, alters, deletes or renders inaccessible data, computer programs or electronic documents belonging to third parties, provided that the consequences of the act are serious. The aggravated type of this offence is

provided for in the next Paragraph. According to its contents, the perpetrator is subject to increased liability if the action:

- (1) has been committed within an organised criminal group, or
- (2) has caused serious disruption, or has been directed against a significant number of information systems, or
- (3) has jeopardised the provision of essential public services or the essential needs of the population, or
- (4) has affected a critical infrastructure information system or created a serious threat to the security of a Member State, the EU or an EU Member State, or
- (5) has been committed using the measures specified in Article 264 ter (i.e. “hacking tools”).

The penalty provided for includes imprisonment for a term of between two and five years and a fine, which may be imposed of up to ten times the equivalent of the damage caused. However, if the offence has had particularly serious consequences, an imprisonment sentence higher by one level may be imposed (Article 264(3)). Nevertheless, pursuant to Article 264 (4), penalties for the acts referred to in that Article are imposed applying the upper half range if, in committing them, the offender concerned has used the identity of a third party in order to gain access to an information system or to win the trust of a third party.

The next Article (Article 264 bis) criminalises attacks involving the unauthorised, substantial disruption or interruption of the operation of an information system belonging to a third party through the performance of acts described in the preceding provisions, the input or transmission of data, destruction, damage, deactivation, removal or replacement of an information system or mass storage. This offence is punishable by imprisonment for a term of six months to three years. Nonetheless, if it has had a significant impact on the activities of the enterprise or on the functioning of the public administration, the penalty shall be applied within upper half range, and may be increased by one level.

Article 264 bis (2) stipulates that where the act referred to in Para. 1 has been committed in the circumstances described in Article 264(2), the perpetrators are liable to a term of imprisonment of between three and eight years, and to a fine of between three and ten times the value of the damage caused. Similarly to the offences under Article 264, penalties for the acts, referred to in the said Article, are imposed in their upper half range if, in committing them, the offender has used the identity of a third party in order to gain access to an information system or to win the trust of a third party (Article 264 bis (3)).

Article 264 ter criminalises acts relating to hacking tools used to commit the offences referred to in the aforementioned provisions. It has the same wording as Article 197 ter, as discussed above, so it is not necessary to cite it again.

References

- Clough J (2013) Principles of cybercrime. New York
- Féral-Schuhl Ch (2010) Cyberdroit: le droit à l'épreuve de l'Internet. Paris
- Hoeren T (2012) Internet- und Kommunikationsrecht: Praxis-Lehrbuch. Cologne
- Letai P, Spain Part VII. Computer related crime. In: Blanpain R (ed) International encyclopaedia of laws. Vol 3. Cyber law (ed. J. Dumortier). Kluwer Law International
- Murray A (2010) Information technology law. The Law and Society, Oxford–New York
- Radoniewicz F (2016) Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym. Warsaw
- Rogacka-Rzewnicka M (2004) In: Machowska A, Wojtyczek K (eds) Prawo Francuskie, vol I. Cracow
- Smith GJH (ed) (2007) Internet law and regulation. London
- Walden I (2007) Computer crimes and digital investigations. Oxford

Filip Radoniewicz PhD; legal advisor; adjunct in the Department of Cybersecurity Law and New Technologies at the Institute of Law, War Studies University, Warsaw; expert at the Academic Centre for Cybersecurity Policy (War Studies University) and in the Ministry of Justice; he worked as an assistant judge (in the Fourth Criminal and Sixth Penitentiary Department of the Regional Court in Lublin); graduate of post-graduate studies: “European Union Law” at the Jagiellonian University, “Human Rights and Freedoms”, co-organized by the Institute of Legal Sciences of the Polish Academy of Sciences and the Helsinki Foundation for Human Rights, and “Computer Network Administration” at the Lublin University of Technology; author or co-author of approximately fifty publications, mainly in the field of broadly understood criminal law, new technology law and human rights. Selected publications: F. Radoniewicz (2016) *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym / Criminal liability for hacking and other offences against computer data and information systems/*, Wolters Kluwer, Warszawa; *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz /Act on the National Cybersecurity System. Commentary/* (2019) ed. W. Kitler, J. Taczowska-Olszewska, F. Radoniewicz, CH. Beck, Warszawa.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.