International Association of Penal Law (AIDP)
XIX[th] International Congress of Penal Law

Information Society and Penal Law

Report on Information Society, Section 4
Country Report Switzerland

Sabine GLESS (Section D), Anna PETRIG (Sections B and E), Dario STAGNO and Jeannine MARTIN (Sections A and C)

A. Definition of cybercrime and relevant provisions

1. Definition of cybercrime for the present report

The term "cybercrime" is understood in this report to cover "criminal conduct that affects the interests associated with the use of information and communication technology (ICT), such as the proper functioning of computer systems and the internet, the privacy and integrity of data stored or transferred in or through ICT, or the virtual identity of internet users."[1] Hence, in the present report, the concept of cybercrime primarily denotes offences protecting the confidentiality, integrity and availability of computer data and systems.[2] The following offences of Swiss criminal law qualify as so-called "CIA offences": Article 143 Swiss Criminal Code[3] (unauthorised obtaining of data), Article 143[bis] Swiss Criminal Code (unauthorised access to a data processing system) and Article 144[bis] Swiss Criminal Code (damage to data). For the sake of completeness, Article 147 Swiss Criminal Code (computer fraud) is included in the analysis at hand, which belongs to the category of so-called computer-related offences. In sum, when using the notion of "cybercrime" in the following, this must be understood as a reference to these four offences under Swiss criminal law, unless explicitly stated that other offences are meant as well (e.g. "ordinary" offences committed by means of computers and networks).

2. The four cybercrimes under Swiss criminal law

The four cybercrimes analysed in this report – unauthorised obtaining of data, unauthorised access to a data processing system, damage to data and computer fraud – were included in the Swiss Criminal Code in 1995.[4] The provision dealing with unauthorised access to a data processing system has

---

1 International Association of Penal Law, Newsletter 1/2012, ‹www.penal.org/IMG/Newsletter 2012-2EN(1).pdf› (accessed 5 May 2013), p. 42.

2 These offences are referred to as "CIA offences": Ulrich Sieber, Straftaten und Strafverfolgung im Internet, Gutachten C zum 69. Deutschen Juristentag, München 2012, p. C41; Arts. 143, 143[bis] and 144[bis] Swiss Criminal Code by and large correspond to Arts. 2–6 Convention on Cybercrime, adopted in Budapest on 23 November 2001, CETS No. 185 (hereinafter "Convention on Cybercrime"), which are grouped together under the title "Offences against the confidentiality, integrity and availability of computer data and systems". Art. 147 Swiss Criminal Code largely reflects Arts. 7–8 Convention on Cybercrime, which are comprised in the section on "Computer-related offences".

3 Code pénal suisse du 21 décembre 1937, etat le 1er janvier 2013, RS 311.0: (the abbreviation RS stands for *Receuil systématique du droit fédéral*, where federal legal acts in force in Switzerland are collected in a systematic order, and the number indicates the thematic area to which an act belongs) hereinafter "Swiss Criminal Code"; a translation of the Swiss Criminal Code by the Federal Authorities of the Swiss Confederation is available at ‹www.admin.ch/ch/e/rs/c311_0.html› (accessed 5 May 2013); since English is not an official language of the Swiss Confederation, the translation has no legal force.

4 RO 1994 2290 (the abbreviation RO stands for *Recueil officiel des lois fédérales*, where federal acts in force in Switzerland are published in a chronological order).

recently been amended[5] in order to meet the requirements flowing from the Convention on Cybercrime of the Council of Europe,[6] which was ratified by Switzerland on 21 September 2011 and which entered into force on 1 January 2012.[7]

Article 143 Swiss Criminal Code prohibits the unauthorised obtaining of data and thus protects persons from interferences with their power of disposition over data. According to this provision, any person who obtains for himself or another data that is stored or transmitted electronically or in some similar manner and which is not intended for him and has been specially secured to prevent his access may be held criminally liable. This provision is the implementation of Article 3 Convention on Cybercrime. However, unlike the provision of the Convention on Cybercrime, the offence defined in Article 143 Swiss Criminal Code is only fulfilled if the data is obtained for the offender's own or another's unlawful gain. Switzerland issued a declaration in that respect when ratifying the Convention on Cybercrime.[8]

Article 143bis(1) Swiss Criminal Code pertains to the unauthorised access to a data processing system and encompasses conduct commonly referred to as "hacking". It by and large reflects Article 2 Convention on Cybercrime. However, the provision of the Swiss Criminal Code requires that the alleged offender has hacked a system by surmounting special safety measures aimed at securing the system. Since this requirement is not contained in the relevant offence description of the Convention on Cybercrime, Switzerland issued a declaration in that respect.[9] Meanwhile, Article 143bis(2) Swiss Criminal Code prohibits the marketing or making accessible of passwords, programs or other data that one knows or must believe will be used for hacking purposes; the provision implements Article 6(1) Convention on Cybercrime.[10]

Article 144bis(1) Swiss Criminal Code prohibits causing damage to data. This cybercrime, which is the cyberspace equivalent of the prohibition of causing criminal damage to physical property, implements the content of Article 4 Convention on Cybercrime. Meanwhile, Article 144bis(2) Swiss Criminal Code criminalizes the manufacturing, importing, marketing, advertising, offering or otherwise making accessible programs that one knows or must believe will be used to cause damage to data as prohibited by the first paragraph of Article 144bis(1) Swiss Criminal Code. Since this provision only partly implements Article 6 Convention on Cybercrime, Switzerland issued a respective declaration when ratifying the treaty.[11].

Article 147 Swiss Criminal Code criminalizes computer fraud and is the cyberspace equivalent of the fraud provision of Article 146 Swiss Criminal Code. It by and large reflects the content of Article 8 Convention on Cybercrime.[12]

---

5 RO 2011 6293.

6 Convention on Cybercrime (see FN 2).

7 Convention du 23 novembre 2001 sur la cybercriminalité, etat le 1er janvier 2012, RS 0.311.43.

8 Convention sur la cybercriminalité (see FN 7), réserves et déclarations Suisse, b.

9 Message relatif à l'approbation et à la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité du 18 juin 2010, FF 2010 4275, p. 4281; Convention sur la cybercriminalité (see FN 7), réserves et déclarations Suisse, a.

10 Message relatif cybercriminalité (see FN 9), p. 4286.

11 Convention sur la cybercriminalité (see FN 7), réserves et déclarations Suisse, c.

12 Message relatif cybercriminalité (see FN 9), p. 4288.

B. Jurisdictional issues

1. Location of the place of commission

a) The principle

(aa) Cybercrimes are subject to general jurisdictional rules

The four offence descriptions referred to as cybercrimes under Swiss criminal law[13] do not contain any jurisdictional elements. Rather, these offences are subject to the *general* jurisdictional rules laid down in Articles 3 to 8 Swiss Criminal Code.[14] The primary jurisdictional basis under Swiss criminal law is the territoriality principle, which is set forth in Article 3 Swiss Criminal Code and which is given priority over other jurisdictional bases, notably those contained in Articles 4 to 7 Swiss Criminal Code.[15]

(bb) Place of commission under general jurisdictional rules

According to the principle of territoriality, Swiss criminal law is applicable to every person who commits an offence in Switzerland.[16] The principle is thus intrinsically linked with the rather clear notion of Swiss territory[17] and the concept of "place of commission", which is more intricate – especially in the realm of cybercrime.

The "place of commission" is defined in Article 8 Swiss Criminal Code: For an offence to fall within the geographical scope of application of Swiss criminal law it suffices that either the place where the criminal *conduct* was carried out (act or omission) *or* the place where the criminal *result* occurred is located in Switzerland. The provision thus encapsulates the so-called ubiquity theory,[18] which combines the theory of acting[19] and the theory of result.[20] Hence, the Swiss legislature opted for a very broad test to locate the place of commission in Switzerland with the result that the reach of the territoriality principle extends to extraterritorial conduct.

As a second step, the meaning of Article 8 Swiss Criminal Code, which defines the place of commission, is discussed specifically with regard to cybercrimes.

---

13 See Section A of this report.

14 See Section B.3 of this report discussing which of the jurisdictional bases contained in Arts. 3–8 Swiss Criminal Code are in fact applicable to the four cybercrimes of Swiss criminal law. For an overview on the general jurisdictional rules under Swiss criminal law, see Anna Petrig, Extraterritorial jurisdiction – the applicability of domestic criminal law to activities committed abroad in Switzerland, in: Ulrich Sieber/Susanne Forster/Konstanze Jarvers (eds.), National Criminal Law in a Comparative Perspective, Vol. 2.1: General limitations on the application of criminal law, Berlin 2011, pp. 118–136.

15 Andreas Donatsch/Brigitte Tag, Strafrecht I, Verbrechenslehre, 8th edition, Zürich 2006, p. 61; José Hurtado Pozo, Droit pénal, Partie générale, 3rd edition, Zürich 2008, p. 67 N 192; Stefan Trechsel/Hans Vest, Art. 3 Swiss Criminal Code, in: Stefan Trechsel/Mark Pieth (eds.), Schweizerisches Strafgesetzbuch, Praxiskommentar, 2nd edition, Zürich/St. Gallen 2013, p. 20 N 1.

16 José Hurtado Pozo (see FN 15), p. 67 N 193.

17 José Hurtado Pozo (see FN 15), pp. 67–68 N 194–195 and pp. 126–128 N 376–381; Stefan Trechsel/Hans Vest, Art. 3 Swiss Criminal Code (see FN 15), p. 20 N 3: the notion of "Switzerland" refers to the territory of the Swiss State as defined by domestic and international public law; it encompasses not only the land surface within state borders but also the airspace above it and the subsoil beneath it.

18 José Hurtado Pozo (see FN 15), p. 60 N 199 and p. 70 N 201.

19 The theory of acting is also referred to as the objective territoriality principle: see, e.g., Report of the International Law Commission: 58th Session (1 May–9 June and 3 July–11 August 2006), Annex E – Extraterritorial Jurisdiction, 2006, UN Doc. A/61/10, para. 11.

20 The theory of result is also referred to as the effects doctrine, see, e.g., Report of the International Law Commission (see FN 19), para. 12.

b) The concrete solutions

(aa) Theory of acting: where offender acted

According to the theory of acting, the offence is considered to be committed in Switzerland if the place where the offender was physically present when engaging in the prohibited conduct is located in Switzerland. If this is the case, the specific conduct falls within the geographical scope of application of Swiss criminal law. Thereby, it suffices that the person fulfilled one of the objective definitional elements of the offence[21] (partially) in Switzerland. However, mere preparatory acts carried out in Switzerland are generally not enough to give rise to a place of commission; rather, at least an attempt is necessary.[22]

In the realm of cybercrime, various places theoretically qualify as the place of acting, notably the place where the offender was physically present when entering the respective computer command, i.e. the place of the information input, the place where the server is located, which hosts the data uploaded by the alleged offender, or even the place where the data is made available, e.g. downloadable.[23] The majority of scholars argue that regarding the four cybercrimes of the Swiss Criminal Code, the place of acting must be located at the place where the offender was physically present when entering the respective computer commands.[24] This view finds support in cantonal case law.[25] The Swiss Federal Supreme Court has yet to decide this question specifically. However, in a case involving the determination of the competent forum *within Switzerland*, the Court opined that the place of the data input gives rise to a place of commission; meanwhile, the Court explicitly left the question open whether the place where the server is located could have the same effect.[26] Yet, the idea that the place where

---

21 Under Swiss criminal law, every offence is composed of objective and subjective definitional elements. While the subjective elements relate to the offender's inner world, the objective elements are those aspects of an offence that display or manifest themselves externally, that is, discernible conditions, factors and changes in the outside world, such as the description of who can commit the offence, the conduct, the object on which the criminal act or omission is performed, the result of the criminal conduct and the causality between conduct and result; on the objective definitional elements of an offence, see Anna Petrig, Objective Aspects of the Offense in Switzerland, in Ulrich Sieber/Susanne Forster/Konstanze Jarvers (eds.), National Criminal Law in a Comparative Perspective, Vol. 3.1: Defining criminal conduct, Berlin 2011, p. 255.

22 José Hurtado Pozo (see FN 15), p. 70 N 202–204; Stefan Trechsel/Hans Vest, Art. 8 Swiss Criminal Code (see FN 15), p. 33 N 2; see also Section B.1.b.cc of this report.

23 Christa Pfister, Hacking in der Schweiz im Spiegel des europäischen, des deutschen und des österreichischen Computerstrafrechts, Dissertation der Universität Zürich, Berlin 2008, p. 67; Marcel A. Niggli, Nationales Strafrecht vs. globales Internet, in: Rolf H. Weber/Reto M. Hilty/Rolf Auf der Maur (eds.), Geschäftsplattform im Internet II, Rechtliche und praktische Aspekte, Zürich 2001, pp. 143; Stephanie Müller, Die strafrechtliche Verantwortlichkeit für Verweisungen durch Hyperlinks nach deutschem und Schweizer Recht, Dissertation Zürich, Berlin 2011, p. 298.

24 Christa Pfister (see FN 23), p. 68; Stefan Heimgartner, Die internationale Dimension von Internetstraffällen – Strafhoheit und internationale Rechtshilfe in Strafsachen, in: Christian Schwarzenegger/Oliver Arter/Florian S. Jörg (eds.), Internet-Recht und Strafrecht, 4. Tagungsband, Bern 2005, p. 122; Christian Schwarzenegger, Der räumliche Geltungsbereich des Strafrechts im Internet. Die Verfolgung von grenzüberschreitender Internetkriminalität in der Schweiz im Vergleich mit Deutschland und Österreich, ZStrR 2010, pp. 117–119; Marcel A. Niggli (see FN 23), pp. 143–144; Daniel Koller, Cybersex, Die strafrechtliche Beurteilung von weicher und harter Pornographie im Internet unter Berücksichtigung der Gewaltdarstellungen, Dissertation Zürich, Bern 2007, p. 385.

25 Daniel Koller (see FN 24), p. 387.

26 BGE 8G.43/1999 (11 August 1999; unpublished; the abbreviation BGE stands for Bundesgerichtsentscheid, i.e. decisions of the Swiss Federal Supreme Court); the case is discussed in Philippe Weissenberger, Zum Begehungsort bei Internet-Delikten, ZBJV 11/1999, pp. 703–706; see also Franz Riklin, Der Gerichtsstand bei Internetdelikten, medialex, 4/1999, pp. 235–236.

the server is located qualifies as a place of commission has been rejected by a vast majority of scholars.[27]

To conclude, the place of acting is considered to be located in Switzerland if the alleged offender was physically present in Switzerland when entering the respective computer commands. Hence, the place of the data input is decisive for determining the place of acting, which, in turn, gives rise to a place of commission in Switzerland according to Article 8 Swiss Criminal Code.

(bb) Theory of result: where the result occurs

According to the theory of result, which is laid down in Article 8 Swiss Criminal Code in addition to the theory of acting, a crime is considered to have been committed in Switzerland if its result occurs in Switzerland. The notion of "result" is controversial in this context and the jurisprudence of the Swiss Federal Supreme Court regarding the concept of "result" lacks consistency.[28]

Initially adopting a very broad definition of the notion of "result", the Swiss Federal Supreme Court later restricted it and argued that the notion should be understood as synonymous with its definition in the context of result offences:[29] only those changes in the outside world, which correspond to an objective definitional element of the offence, are considered to be a result in the sense of Article 8 Swiss Criminal Code.[30] Hence, to construe a place of commission in Switzerland based on the theory of result is only possible for result offences – but not for conduct offences, which do not feature a result as previously defined and for which, as a consequence, a place of commission can only be located in Switzerland based on the theory of acting.[31] However, from the more recent case law of the Swiss Federal Supreme Court[32] it accrues that the Court broadened the notion of result in the field of offences against personal honour, especially when committed through the use of media. The Court held that an offence committed by the use of media can be prosecuted in Switzerland if a publication realized and edited abroad is distributed in Switzerland. It specified that for offences against personal honour, the communication of the defamatory statement as such constitutes the result and notably considered it sufficient to construe a place of commission in Switzerland if letters with defamatory content sent from abroad were read in Switzerland.[33] Hence, even though offences against personal honour are conduct offences,[34] the Court deems it possible that they feature a result in the sense of Article 8 Swiss Criminal Code. This development may be of significance with regard to the dissemination of illegal content through the use of the internet, i.e. for content-related offences committed in cyberspace. For

---

27 Christa Pfister (see FN 23), p. 68; Christian Schwarzenegger (see FN 24), pp. 117–119; Marcel A. Niggli (see FN 23), pp. 143–144; Daniel Koller (see FN 24), p. 386.

28 See, e.g., Valentine Delaloye, La poursuite pénale du délit formel et les problèmes de territorialité liés à internet, Jusletter du 27 février 2012, N 10–24.

29 Under Swiss criminal law, a distinction is drawn between conduct and result offences. Conduct offences are characterized by the fact that specific conduct is threatened with punishment; the offence is completed by the mere carrying out of the conduct threatened with punishment and no further or specific consequences must ensue from the conduct in question. As regards result offences, the offence description is only fulfilled if the conduct yields a certain result, which must be different from the conduct of the offender in terms of location or time or at least notionally; on this distinction, see Anna Petrig (see FN 21), pp. 266–267.

30 Peter Popp/Patrizia Levante, Art. 8 Swiss Criminal Code, in: Marcel A. Niggli/Hans Wiprächtiger (eds.), Strafrecht I, Art. 1–110 StGB/Jugendstrafgesetz, Basler Kommentar, 2nd edition, Basel 2007, p. 231 N 7; BGE 105 IV 326, p. 330, N 3.g; On the notion of "objective definitional element of the offense", see also Section B.1.b.aa of this report.

31 Valentine Delaloye (see FN 28), N 13–14; on the theory of acting see Section B.1.b.aa of this report.

32 See, e.g., BGE 125 IV 177 and BGE 128 IV 145, p. 153.

33 Valentine Delaloye (see FN 28), N 20; Christa Pfister (see FN 23), p. 69.

34 A minority of authors argue that they qualify as result offences: Valentine Delaloye (see FN 28), N 16–18.

the four cybercrimes under consideration in this report, however, this case law seems important only *if* it constituted the starting point for broadening the definition of "result" in the context of Article 8 Swiss Criminal Code in general.

Since currently only result offences – but not conduct offences – feature a result in the sense of Article 8 Swiss Criminal Code, i.e. can give rise to a place of commission in Switzerland, it is important to determine the nature of the four cybercrimes.

Article 144bis(1) Swiss Criminal Code prohibiting the causing of damage to data[35] and Article 147 Swiss Criminal Code criminalizing computer fraud[36] are both result offences. For these two cybercrimes, the location of a place of commission in Switzerland based on the theory of result is possible; hence, it is not necessary that the alleged offender acted in Switzerland so long as the result occurs in Switzerland.

Meanwhile, Article 143 Swiss Criminal Code, which criminalizes the unauthorised obtaining of data,[37] Article 143bis Swiss Criminal Code penalizing what is referred to as "hacking"[38] and Article 144bis(2) Swiss Criminal Code dealing with the manufacture and dissemination of computer viruses[39] are conduct offences. For these offences a place of commission in Switzerland can only be construed if the alleged offender acted in Switzerland, i.e. based on the theory of acting. Since these cybercrimes do *not* display a result as defined by the Swiss Federal Supreme Court in the context of Article 8 Swiss Criminal Code, it is not possible to construe a place of commission in Switzerland based on the theory of result (and these offences do not seem to fall within the exception of offences against personal honour committed through the use of media, which the Swiss Federal Supreme Court has held as yielding a result despite being conduct offences). Hence, in many situations where the negative effects of cybercrimes – which qualify as conduct rather than result offences – are felt in Switzerland, but where the conduct took place abroad rather than in Switzerland, the current interpretation of Article 8 Swiss Criminal Code does not allow a place of commission to be construed in Switzerland. Put differently, these cybercrimes cannot be subjected to Swiss criminal law based on the territoriality principle – however, they can potentially be brought within the ambit of Swiss criminal law by virtue of any other jurisdictional basis available under Swiss criminal law.[40]

We can thus conclude that for cybercrimes qualifying as result offences (Articles 144bis(1) and 147 Swiss Criminal Code), a place of commission can be located in Switzerland if either the result occurs in Switzerland or the conduct, i.e. entering the computer command, was (partially) carried out in Switzerland. For those cybercrimes qualifying as conduct offences (Articles 143, 143bis and 144bis(2) Swiss Criminal Code), it is currently only possible to locate a place of commission in Switzerland if they were (partially) committed in Switzerland. In other words, it does not suffice that their negative effects occur in Switzerland because these effects are not considered to be a result in the sense of Article 8 Swiss Criminal Code, i.e. the provision determining the place of commission. Overall, in many instances, cybercrimes cannot be subjected to Swiss criminal law based on the territoriality principle. It is against this background that various authors suggest that this dichotomy between result offences and

---

35 Stefan Trechsel/Dean Crameri, Art. 144bis Swiss Criminal Code, in: Stefan Trechsel/Mark Pieth (eds.), Schweizerisches Strafgesetzbuch, Praxiskommentar, 2nd edition, Zürich/St. Gallen 2013, p. 732 N 1 ff.; Christian Schwarzenegger (see FN 24), p. 122.

36 BGE 6S.597/2001, consid. 4.3.2; Christian Schwarzenegger (see FN 24), p. 122.

37 Stefan Trechsel/Dean Crameri, Art. 143 Swiss Criminal Code (see FN 35), pp. 721 ff. N 3 and 7; Philippe Weissenberger, Art. 143 Swiss Criminal Code, in: Marcel A. Niggli/Hans Wiprächtiger (eds.), Strafrecht II, Art. 111–392 StGB, Basler Kommentar, 2nd edition, 2007, p. 456 N 6 ff.

38 Christa Pfister (see FN 23), p. 70.

39 Christian Schwarzenegger (see FN 24), p. 122.

40 See Section B.3 of this report.

conduct offences must be overcome with regard to cybercrimes (or even generally).[41] As we will see later in more detail,[42] some authors go as far as to suggest that any cybercrime should be subjected to Swiss criminal law as soon as unlawful conduct carried out abroad "can be made visible on a screen" in Switzerland.[43]

(cc) Attempts

According to Article 8(2) Swiss Criminal Code, an attempt to commit an offence gives rise to a place of commission in Switzerland if the person acted in Switzerland or if the result should have occurred in Switzerland according to the offender's perception.[44] Thus, similar to completed crimes, it is the ubiquity theory – embracing the theory of acting and the theory of result – that guides the location of the place of commission for inchoate crimes. Hence, the analysis above regarding the application of the theory of acting and theory of result to completed cybercrimes[45] can be applied *mutatis mutandis* to attempted cybercrimes.

While mere preparatory acts generally do not give rise to a place of commission in Switzerland, the so-called "punishable preparatory acts" pertaining to specific crimes exhaustively listed in Article 260bis(1) Swiss Criminal Code do so.[46] The four cybercrimes of the Swiss Criminal Code are, however, not included in this list. Hence, only attempted cybercrimes, but not preparatory acts relating to their future commission, can give rise of a place of commission in Switzerland.

(dd) Participation

A black letter legal norm determining whether and when participation in an offence gives rise to a place of commission in Switzerland is missing from Swiss criminal law. However, jurisprudence has developed conditions under which participation in an offence establishes a place of commission in Switzerland.

According to this case law, the criminal conduct of one co-perpetrator in Switzerland establishes a place of commission in Switzerland for all co-perpetrators. We concluded earlier that in the realm of cybercrime, the place of commission can be determined according to the theory of acting or the theory of result, which together form the ubiquity theory laid down in Article 8 Swiss Criminal Code.[47] The place of acting is considered to be located in Switzerland if the alleged offender was physically present in Switzerland when entering the respective computer commands. Hence, if one co-perpetrator acted in Switzerland, Swiss criminal law is applicable to other co-perpetrators involved in the commission of the respective cybercrime. Furthermore, according to the theory of result, the criminal result obtained in Switzerland by one co-perpetrator gives rise to a place of commission in Switzerland for all other co-perpetrators.[48] Hence, as soon as a cybercrime qualifying as a result offence displays its result in the

---

41 For a discussion whether the dichotomy should be maintained in the realm of cybercrime and various positions held by scholars, see Christa Pfister (see FN 23), p. 71; Valentine Delaloye (see FN 28), N 10–24; Daniel Koller (see FN 24), pp. 393–395.

42 See Section B.5 of this report.

43 See, e.g., Daniel Koller (see FN 24), p. 394.

44 Maurice Harari/Miranda Liniger Gros, Art. 8 Swiss Criminal Code, in: Robert Roth/Laurent Moreillon (eds.), Code pénal, Commentaire romand, Basel 2009, p. 99 N 55–58.

45 See Section B.1 of this report.

46 Stefan Trechsel/Hans Vest, Art. 8 Swiss Criminal Code (see FN 15), p. 33 N 2.

47 See Section B.1.b.aa and bb of this report.

48 Peter Popp/Patrizia Levante, Art. 8 Swiss Criminal Code (see FN 30), p. 234 N 13; Maurice Harari/Miranda Liniger Gros, Art. 8 Swiss Criminal Code (see FN 44), p. 98 N 48–49.

sense of Article 8 Swiss Criminal Code in Switzerland,[49] all co-perpetrators involved in the commission of that offence are subject to Swiss criminal law.

An instigator is considered to have committed an offence in Switzerland even if he acted abroad if the result of the instigation occurred in Switzerland or, in the case of an attempt, the result should have occurred in Switzerland. The same holds true for an aider and abettor contributing to the offence from abroad, if the result of the crime occurs in Switzerland.[50] However, according to the case law of the Swiss Federal Supreme Court, persons instigating or aiding and abetting in Switzerland an offence committed abroad[51] are not subject to Swiss criminal law based on the territoriality principle (it might, however, be possible to apply Swiss criminal law based on jurisdictional bases other than the principle of territoriality).[52] This restrictive view is criticized in doctrine and it is argued that Swiss criminal law should be applicable under the condition that the principal offence is punishable at the place of commission.[53]

2. Necessity of determining place of commission

Absent any specific jurisdictional rules for cybercrimes,[54] the general jurisdictional rules of Articles 3 to 8 Swiss Criminal Law apply to these offences. As we have seen earlier, jurisdiction can only be based on the principle of territoriality[55] if a place of commission as defined in Article 8 Swiss Criminal Code can be construed in Switzerland.[56] Put differently, it is *a conditio sine qua non* that a place of commission can be construed in Switzerland so as to apply Swiss criminal law to a specific cybercrime based on the territoriality principle.

Unlike the territoriality principle, other jurisdictional bases of Swiss criminal law are not subject to the requirement that the place of commission is located in Switzerland. Rather, their very existence goes back to the idea of extending the application of Swiss criminal law to *extraterritorial* conduct. And yet, Article 8 Swiss Criminal Code defining the place of commission in Switzerland plays an indirect role in that the extraterritorial jurisdictional bases, which are of relevance for the four cybercrimes,[57] require that the offence was committed *abroad*, i.e. that no place of commission can be construed in Switzerland.[58]

To conclude, under Swiss criminal law as it stands today, there is an absolute necessity to identify the place of commission of a cybercrime in order to determine whether Swiss criminal law applies to it – either based on the territoriality principle (if there is a place of commission in Switzerland) or the active

---

49 See Section B.1.b.bb of this report.

50 Andreas Donatsch/Brigitte Tag (see FN 15), p. 51; Maurice Harari/Miranda Liniger Gros, Art. 8 Swiss Criminal Code (see FN 44), p. 98 N 54.

51 On the criminal liability of Swiss providers as aiders and abettors in the commission of a cybercrime, see Section C.5.a.bb of this report.

52 Andreas Donatsch/Brigitte Tag (see FN 15), p. 51; Maurice Harari/Miranda Liniger Gros, Art. 8 Swiss Criminal Code (see FN 44), p. 98 N 54; both citing BGE 104 IV 77, pp. 86–87 consid. 7b. On jurisdictional bases other than the territoriality principle, see Section B.3 of this report.

53 Maurice Harari/Miranda Liniger Gros, Art. 8 Swiss Criminal Code (see FN 44), p. 98 N 54.

54 See Sections B.1.a and C.2 of this report.

55 Art. 3 Swiss Criminal Code.

56 See Section B.1.a of this report.

57 See Section B.3 of this report.

58 Art. 6 and Art. 7 para. 1 and 2 lit. a Swiss Criminal Code.

or passive personality principle or the representation principle (if there is no place of commission in Switzerland, i.e. the offence was committed abroad and the other criteria have been met).

3. Jurisdictional rules applying to cybercrimes

a) Cybercrimes are subject to general jurisdictional rules

The four offences referred to as cybercrimes in this report[59] do not contain any jurisdictional elements. Rather, these offences are subject to the general jurisdictional rules of the Swiss Criminal Code, i.e. Articles 3 to 8 Swiss Criminal Code.[60] What follows is a discussion about which of these general jurisdictional rules are pertinent in the realm of cybercrime and the conditions under which they apply.

b) Territoriality principle

The first pertinent jurisdictional basis for applying Swiss criminal law to cybercrimes is the territoriality principle defined in Article 3 Swiss Criminal Code. We have already discussed the conditions under which it is triggered specifically with regard to the four cybercrimes. Also, we have seen that the broad localization theory laid down in Article 8 Swiss Criminal Code allows a place of commission to be construed in Switzerland even if the cybercrime (mainly) features extraterritorial moments.[61]

c) Active and passive personality principles

Among the so-called extraterritorial jurisdictional bases, which allow for the application of Swiss criminal law to the four cybercrimes of the Swiss Criminal Code, are the active and passive personality principles. These two principles are not only governed by the same provision, Article 7(1) Swiss Criminal Code, but their application is also subject to the same cumulative requirements. The only difference between the principles is that for the passive personality principle to apply, the victim has to be a Swiss national, while the offender has to possess Swiss nationality in order to base jurisdiction on the active personality principle. These nationality requirements are not explicitly stated in Article 7(1) Swiss Criminal Code, but can be inferred from the introductory sentence of Article 7(2) Swiss Criminal Code.[62] Whether the alleged offender or supposed victim possesses other nationalities in addition to Swiss nationality is irrelevant.[63]

As regards the cumulative conditions for triggering the application of the active and passive personality principles, it is first required that the extraterritorially-committed offence is also punishable at the place of commission or that the place of commission is not subject to any penal power.[64] The four cybercrimes of Swiss criminal law by and large reflect the offences defined in the Convention on Cybercrime.[65] If the extraterritorial conduct took place in another State party to this Convention, which also implemented its content into domestic law, the double criminality requirement is likely to be fulfilled.

---

59 Arts. 143, 143bis, 144bis and 147 Swiss Criminal Code; see Section A of this report.

60 See Sections B.1.a and C.2 of this report. The same holds true for hate speech via the internet, which is – according to the definition of cybercrime as used in this report – not a genuine cybercrime but an "ordinary" crime committed by means of the internet; this offence, which is likely to fulfil Art. 261bis Swiss Criminal Code criminalizing racial discrimination, is subject to the general jurisdictional rules of Arts. 3–8 Swiss Criminal Code.

61 See Section B.1 of this report.

62 Peter Popp/Patrizia Levante, Art. 7 Swiss Criminal Code (see FN 30), p. 222 N 2.

63 Stefan Trechsel/Hans Vest, Art. 7 Swiss Criminal Code (see FN 15), p. 29 N 3 and p. 31 N 9.

64 Art. 7 para. 1 lit. a Swiss Criminal Code; on the principle of double criminality, see Anna Petrig (see FN 14), pp. 319–320.

65 See Section A.2 of this report mentioning which cybercrimes of Swiss criminal law implement the offences defined in the Convention on Cybercrime and to what extent they deviate from these definitions.

Secondly, it is required that the offender who allegedly committed an offence abroad is voluntarily (or according to some authors even involuntarily)[66] present in Switzerland. Alternatively, presence of the offender can also be obtained through extradition, which must be based on a lawful procedure.[67]

The third requirement is that the crime under consideration must be an extraditable offence under Swiss law, yet the offender has not been extradited from Switzerland for any reason, notably because no third State requested his extradition or because such a request was rejected.[68] According to Article 35 Mutual Assistance Act,[69] an offence is an "extraditable offense" if it is "punishable not only under the law of Switzerland but also under the law of the requesting State by a sanction with deprivation of liberty for a maximum period of at least one year or with a more severe sanction"[70] and "is not subject to Swiss jurisdiction". This requirement aims to exclude the application of Swiss criminal law to minor offences committed abroad.[71] Due to the foreign law reference in the definition of "extraditable offense", whether a specific cybercrime qualifies as an extraditable offence can only be answered with regard to a specific fact pattern. Yet a general assertion can still be made that, under Swiss criminal law, all four cybercrimes fulfil the minimum penalty requirement of Article 35 Mutual Assistance Act.

d) Representation principle

The prosecution of persons who allegedly committed cybercrimes can potentially be based on two other jurisdictional grounds, both of which embody the representation principle.

(aa) Offences prosecuted in terms of an international obligation

According to Article 6 Swiss Criminal Code, any person who commits an offence abroad that Switzerland is obliged to prosecute in terms of an international convention is subject to Swiss criminal law. This jurisdictional basis was included in the Swiss Criminal Code in order to ensure that Switzerland always has jurisdiction over offences for which international law stipulates a duty to prosecute or extradite.[72] The application of Swiss criminal law based on Article 6 Swiss Criminal Code is subject to various conditions, to which we turn now.

The application of Swiss criminal law to extraterritorial conduct based on Article 6 Swiss Criminal Code is subject to various requirements, the first of which is that the offence was committed abroad. Hence, this criterion is fulfilled only if *no* place of commission can be construed in Switzerland according to

---

66 Marc Henzelin, Art. 6 Swiss Criminal Code, in: Robert Roth/Laurent Moreillon (eds.), Code pénal, Commentaire romand, Basel 2009, p. 72 N 24.

67 Achieving presence by unlawful means, notably by way of abduction, deception or circumvention of extradition proceedings does not fulfil the presence requirement stipulated in Art. 7 para. 1 lit. b Swiss Criminal Code; Peter Popp/Patrizia Levante, Art. 7 Swiss Criminal Code (see FN 30), p. 223 N 6; Stefan Trechsel/Hans Vest, Art. 7 Swiss Criminal Code (see FN 15), p. 30 N 7.

68 Message concernant la modification du code pénal suisse (dispositions générales, entrée en vigeur et application du code pénal) et du code pénal militaire ainsi qu'une loi fédérale régissant la condition pénale des mineurs du 21 september 1998, FF 1999 1787, pp. 1804–1805; Marc Henzelin, Art. 6 Swiss Criminal Code (see FN 66), p. 81 N 11.

69 Federal Act on International Mutual Assistance in Criminal Matters of 20 March 1981, status of 1 January 2013 (Loi fédérale du 20 mars 1981 sur l'entraide internationale en matière pénale, etat le 1er janvier 2013, RS 351.1), hereinafter "Mutual Assistance Act"; a translation of the Mutual Assistance Act by the Federal Authorities of the Swiss Confederation is available at ‹www.admin.ch/ch/e/rs/3/351.1.en.pdf› (accessed 5 May 2013); since English is not an official language of the Swiss Confederation, the translation has no legal force.

70 This requirement is thus in line with Art. 24 para. 1 lit. a Convention on Cybercrime relating to extradition: Message relatif cybercriminalité (see FN 9), p. 4302.

71 Message modification (see FN 68), p. 1804.

72 Stefan Trechsel/Hans Vest, Art. 6 Swiss Criminal Code (see FN 15), p. 26 N 1.

Article 8 Swiss Criminal Code.[73] The second requirement is that Switzerland is obliged to prosecute the offence by virtue of an international agreement. Various international treaties contain such a duty to prosecute. As regards cybercrimes, the Convention on Cybercrime, to which Switzerland is a party, stipulates a duty to extradite or prosecute in Article 24(6) for the offences defined in Articles 2 to 11. Since the four cybercrimes contained in the Swiss Criminal Code are by and large covered by the Convention on Cybercrime, they come under the duty to extradite or prosecute.[74] Hence, the requirement of Article 6 Swiss Criminal Code – that Switzerland is obliged to prosecute the respective offences by virtue of an international agreement – is generally fulfilled with regard to cybercrimes.

Since Switzerland is acting on behalf of a third State with a closer link to the offence, Article 6 Swiss Criminal Code further requires that the offence is also punishable at the place of commission (double criminality) or, alternatively, that the place of commission is not subject to any penal power.[75] Finally, the offender has to be (voluntarily)[76] present in Switzerland and has not been extradited.[77]

(bb) Rejected extradition request

Article 7(2)(a) Swiss Criminal Code provides for the application of Swiss criminal law to alleged offenders regarding whom Switzerland refused an extradition request for reasons unrelated to the nature of the offence. This provision aims at reconciling two competing interests: While Switzerland is obliged to respect certain bars to extradition,[78] it also has an interest in extraditing individuals suspected of having engaged in criminal conduct so as not to grant a safe haven and foster impunity. In the past, this tension has led to some disregard for the mandatory grounds for refusal of an extradition request.[79] Providing Swiss criminal jurisdiction for such cases is understood as a way out of this dilemma and a means of realizing both interests.

The application of Swiss criminal law based on this jurisdictional ground is only possible if neither the alleged offender nor the supposed victim is a Swiss national.[80] Furthermore, the offence must also be liable to prosecution at the place of commission or the place of commission is not subject to any State's criminal law jurisdiction. In addition, the alleged offender must be in Switzerland, and while extradition is permitted for the offence under Swiss law, the alleged offender is not extradited.[81] However, Swiss criminal law does not apply if an extradition request was refused because of the nature of the offence, notably its political, military or fiscal nature.[82]

---

73 On the determination of the place of commission according to Art. 8 Swiss Criminal Code in the realm of cybercrime, see Section B.1 of this report.

74 Council of Europe, Explanatory Report on the Convention on Cybercrime, ‹conventions.coe.int/Treaty/en/Reports/Html/185.htm› (accessed 5 May 2013), para. 251.

75 Peter Popp/Patrizia Levante, Art. 6 Swiss Criminal Code (see FN 30), pp. 216–218 N 2–7.

76 Not requiring voluntariness: Marc Henzelin, Art. 6 Swiss Criminal Code (see FN 66), p. 72 N 24.

77 Peter Popp/Patrizia Levante, Art. 6 Swiss Criminal Code (see FN 30), p. 218 N 8; Marc Henzelin, Art. 6 Swiss Criminal Code (see FN 66), p. 74 N 31–32.

78 An important bar to extradition flowing from human rights law and international refugee law is the principle of non-refoulement. Under Swiss law, the prohibition of refoulement is expressed in, *inter alia*, Art. 2 lit. a and b Mutual Assistance Act (see FN 69).

79 Peter Popp/Patrizia Levante, Art. 7 Swiss Criminal Code (see FN 30), p. 223 N 6.

80 Introductory words of Art. 7 para. 2 Swiss Criminal Code.

81 Art. 7 para. 1 lit. a–c read together with Art. 7 para. 2 Swiss Criminal Code.

82 Art. 7 para. 2 lit. a Swiss Criminal Code; see, e.g., Art. 3 Mutual Assistance Act (see FN 69); Marc Henzelin, Art. 6 Swiss Criminal Code (see FN 66), p. 82 N 17.

e) Impertinent jurisdictional bases

Among the jurisdictional bases that *cannot* serve as the basis for application of Swiss criminal law to the four cybercrimes analysed in this report is Article 4 Swiss Criminal Code, which embodies the protective principle. This jurisdictional basis is only amenable to the offences defined in Title 13 of the Swiss Criminal Code dealing with "felonies and misdemeanours against the State and national security". Since none of the cybercrimes considered in this report are contained in Title 13 of the Swiss Criminal Code, they are not amenable to the protective principle.

Article 5 Swiss Criminal Code subjecting specific offences committed against minors abroad to an absolute universality principle in not applicable to cybercrimes as defined in this report either. The exhaustive list of offences amenable to this jurisdictional rule does not contain any of the four cybercrimes.

Finally, the absolute universality principle stipulated in Article 7(2)(b) Swiss Criminal Code, which is reserved for offences qualifying as "a particularly serious felony that is proscribed by the international community", i.e. international core crimes, does not apply to the four cybercrimes.

f) Conclusion

We can conclude that the four cybercrimes under consideration here are subject to the general jurisdictional rules of the Swiss Criminal Code since these offence descriptions do not contain any jurisdictional elements. The application of Swiss criminal law to cybercrimes can potentially be based on the territoriality principle, which is equipped with a broad localization theory,[83] the active and passive personality principles[84] and the representation principle for offences committed abroad that Switzerland is obliged to prosecute in terms of an international agreement,[85] or the representation principle for offences where an extradition request was rejected.[86] The remaining jurisdictional bases of the Swiss Criminal Code do not seem amenable to the four cybercrimes under consideration here. Overall, Switzerland potentially has prescriptive and thus adjudicative jurisdiction over cybercrimes (partially) committed extraterritorially.

4. Prevention and settlement of jurisdictional conflicts

Substantive Swiss criminal law does not contain any rules on conflict of laws, which are intended to prevent or settle jurisdictional conflicts between two or more States both claiming jurisdiction. Some jurisdictional bases provided for in Articles 3 to 7 Swiss Criminal Code contain principles mitigating the *consequences* of jurisdictional conflicts by setting forth that foreign judgments are taken into account to some extent.[87] However, not all of these principles apply to all jurisdictional bases provided for in the Swiss Criminal Code, and – more importantly in the present context – they are not designed to prevent or solve jurisdictional conflicts but only to (partially) remedy consequences accruing from the multiple jurisdictional claims.

However, regarding the four cybercrimes of the Swiss Criminal Code, Switzerland is under an obligation to consult with other State parties equally claiming jurisdiction in a specific case "with a view to determining the most appropriate jurisdiction for prosecution" by virtue of Article 22(5) Convention on

83 Arts. 3 and 8 Swiss Criminal Code.

84 Art. 7 para. 1 Swiss Criminal Code.

85 Art. 6 Swiss Criminal Code.

86 Art. 7 para. 2 lit. a Swiss Criminal Code.

87 On the principles of imputation, extinction and enforcement, which allow foreign judgments to be taken into account to some extent, see Anna Petrig (see FN 14), pp. 321–324.

Cybercrime.[88] The application of this provision by Swiss prosecutorial authorities, i.e. to waive Swiss prosecution in a specific case, is made possible by Article 8 Swiss Criminal Procedure Code.[89] This provision stipulates some specific instances where, in deviation of the generally applicable principle of legality,[90] prosecution can be waived. One such instance is the waiving of prosecution "if the offence is already being prosecuted by a foreign authority or the prosecution has been assigned to such an authority".[91] Article 22(5) Convention on Cybercrime does *not* provide any indication on *how* to solve instances of positive jurisdictional conflicts – for instance, when to opt for a single venue for prosecution or when to prosecute some alleged offenders in one State and some in another State. According to the Explanatory Report to the Convention on Cybercrime, this decision is heavily dependent on the specificities of each case and therefore not amenable to a general rule pertaining to the solution of jurisdictional conflicts.[92] Furthermore, Article 22(5) Convention on Cybercrime has a major weakness in that the obligation to consult is not of an absolute nature.[93] Rather, an obligation to consult only exists "where appropriate", which opens the door for States to ultimately pursue their own interests without even making an effort to coordinate their course of action with other States also claiming jurisdiction.

5. Subjecting cybercrimes to universal jurisdiction?

The idea of subjecting cybercrimes to Swiss criminal law and jurisdiction regardless of where they have been committed as long as they display some negative effects in Switzerland has been put forth in scholarship pertaining to Swiss criminal law. Thus, it has been argued that the Swiss judge should be elevated to a position of a "judge of cyberspace" – a space to which the concept of (national) borders is foreign – with universal competence to try cybercrimes.[94]

Even though some scholars argue in favour of subjecting cybercrimes to universal jurisdiction, we do not consider it a likely scenario that the Swiss legislature actually does so in the near future. Admittedly, under Swiss criminal law, there is a clear trend of expanding extraterritorial jurisdiction. Over the last decades, the instances where Swiss law can be applied to extraterritorial conduct have multiplied. With the 2007 entry into force of the new General Part of the Swiss Criminal Code containing the general jurisdictional rules, the universality principle was introduced for specific (mainly sexual) offences committed against minors abroad and for particularly serious offences proscribed by the international community as a whole, namely international core crimes. In 2012, the Swiss legislature criminalized female genital mutilation, equipped with a jurisdictional rule subjecting the offence to an absolute universality principle.[95] This development reveals how the Swiss legislature is inclined to subject certain offences to an absolute universality principle, i.e. to make Swiss criminal law applicable to conduct that

---

88 See Section A.2 of this report.

89 Code de procédure pénale suisse du 5 octobre 2008, etat le 1er avril 2013, RS 312.0, hereinafter "Swiss Criminal Procedure Code"; a translation of the Swiss Criminal Procedure Code by the Federal Authorities of the Swiss Confederation is available at ‹www.admin.ch/ch/e/rs/c312_0.html› (accessed 5 May 2013); since English is not an official language of the Swiss Confederation, the translation has no legal force.

90 Art. 7 Swiss Criminal Procedure Code stipulates the principle of legality in criminal procedure.

91 Art. 8 para. 3 Swiss Criminal Procedure Code; on the principle of legality in criminal procedure and the moderate principle of opportunity under Swiss criminal law, see Anna Petrig, Principle of Legality (nullum crimen sine lege) in Switzerland, in: Ulrich Sieber/Susanne Forster/Konstanze Jarvers (eds.), National Criminal Law in a Comparative Legal Context, Vol. 2.1: General Limitations on the Application of Criminal Law, Berlin 2011, p. 120.

92 Explanatory Report (see FN 74), para. 239.

93 Explanatory Report (see FN 74), para. 239.

94 Daniel Koller (see FN 24), pp. 394–395, referring to a judge with universal competence ("Allzuständigkeit").

95 This development is described in Anna Petrig, The expansion of Swiss criminal jurisdiction in light of international law, Utrecht Law Review (accepted for publication; on file with author).

does *not* feature a (substantial) link to Switzerland, except for the offender's presence on Swiss soil. However, when looking at the offences subjected to universal jurisdiction, it also accrues that the legislatures used this most far-reaching jurisdictional basis to protect only specific fundamental interests – such as life and one's physical, psychological and sexual integrity. Since the four cybercrimes considered in this report are pure property offences,[96] it seems rather unlikely that the Swiss legislature would provide for absolute universal jurisdiction over these offences.

The more likely development is that certain restrictive criteria for application of specific jurisdictional rules, which allow Swiss criminal law to be applied to cybercrimes (partially) committed abroad, will be relaxed by courts, either in general or solely in relation to cybercrimes. Thus, for instance, it is possible that courts will broaden the notion of result in the context of cybercrimes in order to construe a place of commission based on the theory of result not only with regard to cybercrimes qualifying as result offences but also those that have the nature of conduct offences.[97] However, the pursuit of an even broader localization theory in the realm of cybercrime, i.e. to broaden the principle of territoriality, will reduce the scope of application of what is commonly referred to as "extraterritorial jurisdictional bases" contained in Articles 4 to 7 Swiss Criminal Code.[98] Put differently, it excludes the application of Swiss criminal law to extraterritorial cybercrimes based on the jurisdictional bases of Articles 6, 7(1) and (7)(2)(a) Swiss Criminal Code,[99] which require that the offence was committed "abroad". For an alleged offender subject to Swiss prescriptive and adjudicative jurisdiction it may, however, be more protective to have Swiss law applied to him based on extraterritorial jurisdiction rather than on the principle of territoriality. The most notable difference is that Articles 6, 7(1) and 7(2)(a) Swiss Criminal Code (unlike, obviously, the principle of territoriality) require double criminality, i.e. that the offence is not only criminalized under Swiss criminal law but also under the criminal law of the place of commission.

To conclude, when discussing the establishment of new jurisdictional bases or to amend or adapt the criteria of existing jurisdictional bases with regard to cybercrimes, the difficulty lies in defining the appropriate scope of domestic prescriptive and adjudicative jurisdiction, i.e. to strike a reasonable balance between unlimited liberty in cyberspace and unlimited liability for cybercrimes.[100] Thereby, the jurisdictional rules of the Swiss Criminal Code must be understood as forming a whole, i.e. equilibrium must be found between what is generally referred to as territorial and extraterritorial jurisdiction. In doing so, it must be borne in mind what the ratio behind the respective jurisdictional bases is, how they are interrelated and the consequences of applying one jurisdictional rule or the other. This is true not only in terms of allowing prosecutions, i.e. from the perspective of the prosecutorial authorities and the supposed victim, but also for the alleged offender's interests and rights.

---

96 They are all contained in title two of the Swiss Criminal Code, which contains offences against property.

97 Christa Pfister (see FN 23), pp. 73–74 on how Art. 8 Swiss Criminal Code and the ubiquity principle it embodies could be interpreted *de lege ferenda*; see also Section B.1.b.aa and bb.

98 The distinction drawn between the principle of territoriality (Art. 3 Swiss Criminal Code) and extraterritorial jurisdictional bases (Arts. 4–7 Swiss Criminal Code) does not reflect the fact that through the broad localization theory of Art. 8 Swiss Criminal Code it is possible to make Swiss criminal law applicable based on the territoriality principle to conduct physically taking place abroad.

99 See Section B.3.c and d of this report.

100 For a discussion on how to strike such a balance, see, for example, Thomas Weigend, Unbegrenzte Freiheit oder grenzenlose Strafbarkeit im Internet?, in: Gerhard Hohloch (ed.), Recht und Internet, Baden-Baden 2001, pp. 85–92; Albin Eser, Internet und internationales Strafrecht, in: Dieter Leipold (ed.), Rechtsfragen des Internet und der Informationsgesellschaft: Symposium der rechtswissenschaftlichen Fakultäten der Albert-Ludwigs-Universität Freiburg und der Städtischen Universität Osaka, Heidelberg 2002, pp. 303–326, available at ‹www.freidok.uni-freiburg.de/volltexte/3784/pdf/Eser_Internet_und_internationales_Strafrecht.pdf› (accessed 5 May 2013).

C. Substantive criminal law and sanctions

1. Cybercrimes with a transnational dimension

Conduct fulfilling one of the four cybercrimes under consideration in this report – unauthorised obtaining of data, unauthorised access to a data processing system, damage to data and computer fraud[101] – is likely to have a transnational dimension.[102]

2. No jurisdictional elements in cybercrime offences

As a general rule, Switzerland defines the geographical scope of its criminal law in *general* jurisdictional provisions, most importantly in Articles 3 to 8 Swiss Criminal Code. Only exceptionally does the Swiss legislature equip specific offences with a jurisdictional rule, which prevails over the general jurisdictional rules.[103] However, none of the cybercrimes considered in this report[104] contains such a specific jurisdictional rule, which implies that these offences are subject to the general jurisdictional rules.[105]

3. No jurisdictional elements in rules on participation

The rules of Swiss criminal law governing participation in a criminal offence are Articles 24 to 27 Swiss Criminal Code, none of which contain a jurisdictional element. As regards the territoriality principle and the determination of the place of commission, we already concluded that participation can give rise to a place of commission in Switzerland. However, this issue is not governed by black letter law norms, but rather it has been developed by jurisprudence.[106]

4. Cybercrime: a matter for domestic regulation?

According to the Swiss understanding, conduct amounting to cybercrime often features a transnational element. It is against this background that the Swiss legislature considers the prevention and repression of cybercrime to be a matter that cannot be regulated by each State separately. Rather – as evidenced by the (rather late)[107] ratification of the Convention on Cybercrime – the Swiss legislature deems it a necessity to adopt international rules in the realm of cybercrime.[108] Yet, the simple adoption and ratification of relevant international treaties is not sufficient. Generally, instruments pertaining to transnational crimes, such as the Convention on Cybercrime, do not stipulate criminal offences as such nor do they establish domestic jurisdiction. Rather, States are obliged to enact relevant rules under domestic law. Hence, while the adoption of harmonized international rules in the realm of cybercrime is essential, it is equally important to implement them domestically.

In addition to harmonized rules on the level of substantive criminal law, which are then implemented by domestic law, it is necessary to have adequate tools for international cooperation in the prevention, detection, investigation and prosecution of cybercrimes. Thus, for instance, the Swiss legislature has

---

101 See Section A of this report.

102 Département federal de justice et police (DFJP), Rapport de la commission d'experts "Cybercriminalité", Berne, juin 2003, p. 73; Stefan Heimgartner (see FN 24), p. 65.

103 See, e.g., Art. 124 para. 2 Swiss Criminal Code.

104 See Section A of this report.

105 See Sections B.1.a and B.3.a of this report.

106 See Section B.1.b.dd of this report.

107 Switzerland signed the Convention on Cybercrime on 23 November 2001; however, it did not ratify the instrument until 21 September 2011, which entered into force in Switzerland on 1 January 2012.

108 See, for example, the report concerning the ratification and implementation of the Convention on Cybercrime of the Swiss Government to the Swiss Parliament: *Message relatif cybercriminalité* (see FN 9), p. 4279; also the results from the public consultation regarding the ratification and implementation of the Convention on Cybercrime demonstrated that the majority of Cantons and political parties deemed it a necessity that Switzerland becomes a party to this international treaty: Message relatif cybercriminalité (see FN 9), p. 4280.

modified – to some extent – the rules governing mutual legal assistance in order to meet the specificities of cybercrimes as defined in the Convention on Cybercrime, namely to allow the exchange of electronic data with foreign authorities.[109] Switzerland also cooperates outside the formal framework of procedures of mutual legal assistance with foreign State authorities, notably based on police cooperation agreements, and with European or international organizations or bodies, such as Interpol and Europol.[110] Such international cooperation has intensified over the last several years[111] and will be enhanced in the future, as demonstrated by the current joint efforts to combat child pornography on the internet.[112] Also, it bears mentioning that the Swiss legislature designated the Federal Office of Police as the point of contact required under Article 35 Convention on Cybercrime,[113] which is supported by the Cybercrime Coordination Unit Switzerland (CYCO).[114]

Taken together, these legislative and institutional developments demonstrate that the Swiss legislature considers cybercrime as a matter that can only be effectively combated by means of international cooperation based on harmonized international rules.[115] This holds all the more true in light of the proliferation of cybercrimes.[116] In addition to intensified cooperation between the competent authorities of different States, the CYCO stresses the need for cooperation between State authorities and private institutions and actors (private-public partnerships), notably those providing internet-related services.[117]

5. No specific and genuine rules on provider liability

a) No genuine and specific rules on provider liability

Swiss law does not contain a genuine and specific set of rules governing the criminal liability of providers. Yet, the idea of enacting rules specifically governing the criminal liability of providers is not foreign to the criminal policy discussion in Switzerland, the discussion of provider liability was first launched roughly 15 years ago.[118] The most concrete outcome of this discussion was a preliminary draft law issued by the Swiss Government in 2004, which contained changes to the Swiss Criminal Code and the Swiss Military Criminal Code concerning the criminal liability of service providers and the powers of the Swiss Confederation to prosecute offences committed via electronic media

---

109 For instance, Art. 18b Mutual Assistance Act (see FN 69) was adopted, which implemented Art. 30 Convention on Cybercrime: AS 2011 6293 ff. = RO 2011 6293 ff.; Département federal de justice et police (DFJP), Communiqué du 18 juin 2010, Renforcement de la lutte internationale contre la cybercriminalité – Le Conseil fédéral propose de ratifier une convention du Conseil de l'Europe; on this, see also Sections D.1 and D.2.c of this report.

110 Message relatif cybercriminalité (see FN 9), p. 4301 ; also see FN 138.

111 Département fédéral de justice et police (DFJP), Rapport annuel 2011, juin 2012, pp. 62 f.; Cybercrime Coordination Unit Switzerland (CYCO), Annual Report 2011, published 4 April 2012, p. 1.

112 Département fédéral de justice et police (DFJP), Communiqué du 5 décembre 2012, Alliance contre la pédocriminalité sur internet: Simonetta Sommaruga [conseillière fédérale, annotation par l'auteur] à Bruxelles pour une conférence des ministres; CYCO, Report (see FN 111), p. 18.

113 Message relatif cybercriminalité (see FN 9), p. 4315.

114 CYCO, Report (see FN 111), p. 23.

115 This also includes Internet Service Provider and domain- or IP-administrators, see DFJP, Rapport annuel 2011 (see FN 111), p. 30.

116 CYCO, Report (see FN 111), p. 28.

117 CYCO, Report (see FN 111), p. 28.

118 See Rapport à l'appui d'avant-projets de modification du code pénal suisse et du code pénal militaire concernant la responsabilité pénale des prestataires et les compétences de la Confédération relatives à la poursuite des infractions commises par le canal des médias électroniques (cybercriminalité), Berne, octobre 2004, ‹www.ejpd.admin.ch/content/dam/data/kriminalitaet/gesetzgebung/netzwerkkriminalitaet/vn-ber-f.pdf› (accessed 5 May 2013).

(cybercrime).[119] Essentially, the preliminary draft law aimed at regulating provider liability along the following lines: While it excluded the liability of access providers *per se*,[120] it set forth the liability of hosting providers (regardless of the criminal liability of the content provider) in cases where the provider has knowledge of illegal content on its servers but does not undertake any steps to remove such data or to prevent access to it.[121] In addition, it obliged hosting providers to notify prosecutorial authorities about illegal content on its servers.[122] The reaction to this draft during the consultation procedure, where the Cantons, political parties and interested groups are invited to express their views on preliminary draft legislation,[123] was important in terms of the number of views collected[124] and extremely divergent in terms of substance. In light of these diverging views, it was deemed an impossible feat to reach a consensus on future regulation of providers. It was mainly for this reason that the Swiss Government decided not to take any further steps regarding the enactment of specific rules governing the criminal liability of providers. Rather, it considered that the issue was already sufficiently regulated by general norms of Swiss criminal law, to which we turn next.[125]

In doctrine, there is a general consensus that a specific criminal law aimed at providers would not solve problems but rather create new ones, and thus the preferred solution is to apply general rules of criminal law to construe provider liability.[126] It is also argued that excessively strict provider liability could result in providers acting as *de facto* judges if the law requires them to assess content and to remove or refrain from transmitting content that they perceive to be illegal. Providers would lack the competence and legitimacy to do so.[127]

Absent specific and genuine provider liability provisions, providers are subject to the general rules on criminal liability of Swiss criminal law. Primarily, provider liability is construed by having recourse to Articles 24 to 27 Swiss Criminal Code, which regulates participation in a criminal offence.[128] In cases

---

119 Rapport modification (see FN 118), pp. 21 ff.; this preliminary draft law finds its origin in a parliamentary motion requesting clarification of the issue of criminal liability of providers, similar to Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ L 178, 17 June 2000, pp. 1–16): Thomas Pfisterer, Cybercriminalité – Modification des dispositions légales, Conseil des États, motion 00.3714, see ‹http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20003714› (accessed 5 May 2013).

120 Art. 27 para. 4 preliminary draft Swiss Criminal Code.

121 Art. 322bis no. 1 para. 1 preliminary draft Swiss Criminal Code.

122 Art. 322bis no. 1 para. 2 preliminary draft Swiss Criminal Code.

123 Art. 147 Constitution fédérale de la Confédération suisse du 18 avril 1999, RS 101.

124 More than 100 consultation procedure responses were collected, which is an exceptionally high number. See David Rosenthal, Internet-Provider-Haftung – ein Sonderfall?, in: Peter Jung (ed.), Aktuelle Entwicklungen im Haftungsrecht, Bern/Zürich/Basel/Genf 2007, p. 175.

125 Among other reasons mentioned for not pursuing the idea of adopting specific rules governing criminal liability of providers were that such new regulations would elicit new interpretational challenges and difficulties. Another argument for not pursuing the draft legislation on provider liability was that the law as it stood did not have any negative consequences for providers and therefore no need for action existed: see Conseil federal, Rapport Cybercriminalité, Responsabilité pénale des prestataires et compétences de la Confédération en matière de poursuite des cyberinfractions, février 2008, pp. 7 f.; David Rosenthal (see FN 124), p. 163 ff.; Rapport modification (see FN 118), pp. 21 ff.; Christian Schwarzenegger, Strafbare Handlungen im Internet – wer ist verantwortlich? Fehlende gesetzliche Regelung in der Schweiz schafft Rechtsunsicherheit, Neue Zürcher Zeitung, 28 January 2008.

126 David Rosenthal (see FN 124), pp. 153 and 158.

127 David Rosenthal, Urheberrecht im Umbruch: Kapitulation vor dem Internet?, Gazzetta 52/2012, p. 91.

128 Christian Schwarzenegger, Weiche Pornographie im Internet und in der Mobiltelefonie (Art. 197 Ziff. 1 StGB) – Prävention, Jugendschutz durch altersbegrenzten Zugang (adult verification systems) und die Verantwortlichkeit der

where providers are legal persons, Article 102 Swiss Criminal Code, which embodies the principle of corporate criminal liability, can be relevant. Finally, some authors suggest applying Article 28 Swiss Criminal Code, which governs the criminal liability of the media, to providers.[129]

Before turning to these various ways of construing provider liability, we have to point to the fact that the case law on criminal liability of providers is rather scarce. The limited number of criminal prosecutions against providers is, first and foremost, due to the fact that cooperation between providers and prosecutorial authorities is quite strong.[130]

(aa) Preliminary remark: criminal liability of natural and legal persons and terminology

Until rather recently, the principle of *societas delinquere non potest* prevailed under Swiss criminal law, i.e. legal persons could not be held criminally liable. However, this concept was abandoned when the corporate criminal law entered into force in 2003. Since then, both natural and legal persons can be held criminally liable under Swiss criminal law.[131] The core norm governing corporate criminal liability under Swiss law is Article 102 Swiss Criminal Code, which will be discussed later in more detail.[132]

Providers can be either natural or legal persons, depending on their nature and characteristics. "Content providers" are persons who upload data from a computer onto a website and thus onto a server; in most cases, content providers are natural persons.[133] "Access providers" are generally legal persons incorporated in Switzerland who have a contractual relationship with a content provider. The main service to be provided by virtue of such contract is access to the internet, including making available the necessary infrastructure, such as a modem, telephone or television line or a wireless connection or mobile communication devices with internet access.[134] As a general rule, "host providers" are also legal persons. Their services consist of providing data storage space on their own servers connected with the internet where the (potentially illegal) content of websites can be automatically uploaded by content providers.[135]

(bb) Rules on participation

As previously mentioned, efforts to create a specific criminal law aimed at providers in Switzerland have failed. Therefore, the general rules of criminal law governing the attribution of criminal liability are applied in cases where providers are suspected of being involved in the commission of a cybercrime. The most obvious way to construe provider liability is by applying the rules on participation in a criminal offence, which are contained in Articles 24 to 27 Swiss Criminal Code.[136]

Under Swiss criminal law, the perpetrator of an offence may perpetrate an offence alone or together with a co-perpetrator; furthermore, he may be supported by an aider and abettor in the commission of the offence and/or he may be incited to commit the offence by an instigator. The perpetrator of an

---

Provider, in: Christian Schwarzenegger/Rolf Nägeli (eds.), 4. Zürcher Präventionsforum – Illegale und schädliche Inhalte im Internet und in den neuen Medien – Prävention und Jugendschutz, Zürich 2012, p. 55; David Rosenthal (see FN 124), p. 161; CYCO, Report (see FN 111), pp. 19 and 26.

129 David Rosenthal (see FN 124), pp. 155 ff.; Christian Schwarzenegger (see FN 128), pp. 54 ff. with further references.

130 David Rosenthal (see FN 124), p. 158.

131 Anna Petrig, Concept and Systematization of the Criminal Offense in Switzerland, in: Ulrich Sieber/Susanne Forster/Konstanze Jarvers (eds.), National Criminal Law in a Comparative Legal Context, Vol. 3.1: Defining Criminal Conduct, Berlin 2011, p. 108.

132 See Section C.5.a.dd of this report.

133 Christian Schwarzenegger (see FN 128), p. 44.

134 DFJP, Rapport "Cybercriminalité" (see FN 102), p. 31.

135 DFJP, Rapport "Cybercriminalité" (see FN 102), pp. 30 f.

136 Christian Schwarzenegger (see FN 128), p. 55; Stephanie Müller (see FN 23), p. 249.

offence fulfils all subjective and objective definitional elements of an offence[137] and he is the one exercising control over the conduct, i.e. it is in his hands whether an offence is committed or not.[138] In the realm of cybercrime, the content provider may qualify as a perpetrator according to this definition since it is in the hands of the provider whether illegal content is published on the internet.[139]

A co-perpetrator is a person who possesses control over the allegedly criminal conduct and who took, together with the perpetrator, a collective decision regarding the commission of the criminal act as such and the sharing of work for the commission of it.[140] As a general rule, host or access providers do not have a common plan with the content provider to commit a cybercrime and therefore do not qualify as co-perpetrators.[141] Meanwhile, a participant is a person who either incites another person to commit an offence (instigator)[142] or who supports the perpetrator in the commission of an offence (aider and abettor).[143]

For criminal liability of host and access providers, the most important form of participation is aiding and abetting. As regards the contribution of aiders and abettors, the support of the perpetrator can be either in the form of psychological or physical support.[144] It is important to note that the will of the aider and abettor must be such as to want the offence to be committed. Put differently, a person who does not want a specific offence to be committed, or has no knowledge of its commission, cannot be held liable for aiding and abetting the offence.[145] Before turning to the question whether access and hosting providers can be held liable as aiders and abettors, it must be mentioned that under Swiss criminal law, various means exist to limit criminal liability, namely the theory of objective attribution, which allows a specific result to not be imputed to a person despite the person's causal contribution to it. One such reason justifying the non-attribution of a specific result to a person is the term "social adequacy": If an offence is fulfilled by conduct that is socially accepted and tolerated, no criminal liability shall arise. Put differently, if a person offers products or services that he knows can be used for the commission of an offence, but that the offering of such services or products is socially accepted and tolerated, he cannot be held liable as an aider and abettor if his services or products are actually used for the commission of an offence. Similarly, according to the doctrine of admissible risk, situations where the offender's conduct created a risk, but the risk is not legally relevant because it constitutes either a socially normal, minimal risk or, if not minimal, a generally accepted risk within a society, he is not held criminally liable.

---

137 On the notion of subjective and objective definitional elements of an offence under Swiss criminal law, see Section B.1.a.bb of this report.

138 Kurt Seelmann, Strafrecht Allgemeiner Teil, 5th edition, Basel 2012, pp. 141 f.; Günter Stratenwerth, Schweizerisches Strafrecht, Allgemeiner Teil I: Die Straftat, 4th edition, Bern 2011, pp. 374 f.

139 DFJP, Rapport "Cybercriminalité" (see FN 102), p. 68; Christian Schwarzenegger (see FN 128), p. 66.

140 Günter Stratenwerth (see FN 138), p. 390.

141 At this point, it is important to distinguish cybercrimes from computer-related crimes such as pornography as, in cases of the latter, a host or access provider might qualify as a co-perpetrator if the criminal act is already committed by simply making illegal content accessible. For more details, see Marcel A. Niggli/Franz Riklin/Günter Stratenwerth, Die strafrechtliche Verantwortung von Internetprovidern – ein Gutachten, ‹www.ejpd.admin.ch/content/dam/data/kriminalitaet/gesetzgebung/netzwerkkriminalitaet/gutachten-niggli-d.pdf› (accessed 5 May 2013), p. 5.

142 See Art. 24 Swiss Criminal Code on incitement.

143 See Art. 25 Swiss Criminal Code on aiding and abetting.

144 Günter Stratenwerth (see FN 138), pp. 418 f.

145 Kurt Seelmann (see FN 138), p. 421.

Danger or harm resulting from such risks is not imputable to the offender despite the existing link between his conduct and the criminal result.[146]

By making hardware and software available and by offering various services, access providers afford the perpetrator of a cybercrime with access to the internet. Hence, the access provider makes it possible for the content provider to upload data or illegal content, which can be understood as supporting the commission of a cybercrime. It is against this background that providers may qualify as aiders and abettors and thus be held liable – especially in cases where the perpetrator cannot be held liable due to, for instance, the anonymity of cyberspace or the transnational elements of a specific fact pattern. The reasoning is that the conduct of access providers, i.e. to provide the content provider with access to the internet, is causal for the commission of a cybercrime since without such access the offence could not be committed.[147] However, providing access to the internet is generally seen as the type of conduct that is socially accepted and tolerated in an information society, and the conduct thus constitutes a generally accepted risk within modern society.[148] Hence, in application of the theory of social adequacy and the doctrine of admissible risk, the criminal liability of access providers is heavily limited. Accordingly, it is rather uncontested in doctrine that access providers generally cannot be held criminally liable as aiders and abettors.[149]

As regards host providers, the question of their criminal liability is less clear. The crucial element concerning their criminal liability is intent as a requirement of aiding and abetting, and thus liability centres on whether the host provider has knowledge of the illegal content on websites hosted by it.[150] As a general rule, when the contract is first concluded, the host provider does not know of the content with which a website is filled. Criminal liability can therefore only arise once illegal content is uploaded and is subject to the requirement that the host provider has knowledge or could have obtained knowledge about the illegal content. However, it is unclear whether host providers are under an obligation to regularly check the legality of the content on websites hosted by them on their own initiative or whether they can wait until they receive indicia of illegal content. It is also unclear whether, in cases where the host provider is in possession of indicia pointing towards illegal content, it has to check the content itself or whether it suffices that the host provider informs competent authorities about such indicia. What can be said, however, is that illegal content must be deleted as soon as the host provider has knowledge of the existence of such content.[151] Nonetheless, legal uncertainty governs, especially

---

146 On the theory of objective attribution, the notion of social adequacy and the doctrine of admissible risk, see Anna Petrig (see FN 21), pp. 272–273; Günter Stratenwerth (see FN 138), pp. 171 and 420; *ATF 134 IV 193*, p. 204 with further references (the abbreviation ATF stands for *arrêt du Tribunal Fédéral Suisse*, decisions of the Swiss Federal Supreme Court).

147 Christian Schwarzenegger (see FN 125).

148 David Rosenthal (see FN 124), pp. 159 f.; Thomas Kohli, Lyrics Server, sic! 12/2003, pp. 960 ff.

149 David Rosenthal (see FN 124), pp. 159 ff.; with reference to different opinions and referring to a judgment of 31 January 2003, where the Basel Criminal Court held that the providing for internet access is comparable to making a telephone line available and that no one would deem the latter to constitute a dangerous act; further see DFJP, Rapport "Cybercriminalité" (see FN 102), pp. 68–71.

150 This knowledge was, for example, the decisive element in *ATF 121 IV 109* concerning the manager of a telecommunication service providing the line for telephone sex services. The Swiss Supreme Court found that because the manager knew of the illegal behaviour of the telephone sex service, but did not stop it, he was liable for aiding and abetting his client. Although this case cannot be transferred offhandedly to cybercrimes, it shows how decisive the knowledge of the provider is for its criminal liability.

151 See David Rosenthal (see FN 127), p. 91; Marcel A. Niggli/Franz Riklin/Günter Stratenwerth (see FN 141), p. 22 with references to *ATF 121 IV 109*. In this judgment, the main critisism was that the responsible manager did not eliminate the access to the illegal service despite his knowledge of it.

given the lack of relevant case law from the Swiss Federal Supreme Court. To conclude, whether host providers can be held liable as aiders and abettors or whether they are free from criminal liability cannot be answered with certainty at the current juncture.[152]

In sum, it can be said that under Swiss criminal law, content providers qualify as perpetrators, while access providers are not held criminally liable because their conduct is understood to be socially accepted and tolerated. Meanwhile, host providers can potentially be seen as aiders and abettors or as free from criminal liability altogether.

(cc) Criminal liability of the media

In addition to the rules on participation in a criminal offence, Article 28 Swiss Criminal Code governing criminal liability of the media is somewhat relevant to provider liability. However, the application of this provision to criminal acts committed by providers is limited by various factors.

Firstly, the provision only applies to offences committed and completed through publication in a medium.[153] The four cybercrimes under consideration in this report do not feature this characteristic – except for a specific part of Article 144bis(2) Swiss Criminal Code:[154] When the alleged offender "provides instructions on the manufacture of … programs" as prohibited under the provision.[155] This is the only cybercrime that can be committed through a medium and where provider liability can potentially be construed based on Article 28(1) Swiss Criminal Code.

As regards Article 144bis(2) Swiss Criminal Code, uncertainty exists regarding the term "medium"; concretely, whether websites where the instructions for manufacturing prohibited programs as criminalized by Article 144bis(2) Swiss Criminal Code are published qualify as a medium in the sense of Article 28(1) Swiss Criminal Code. The term "medium" is not defined by the provision itself or elsewhere in criminal law.[156] According to doctrine, the term encompasses all means by which ideas can be published[157] and it is notably unnecessary that an organizational structure exist behind the medium, which is typical for classical media such as press and television.[158] In light of this rather broad definition of the term "medium" and that it encompasses non-periodical publications, websites are said to fall under Article 28(1) Swiss Criminal Code.[159]

According to Article 28(1) Swiss Criminal Code, if an offence is committed and completed through publication in a medium, only the author, i.e. content provider, is liable to prosecution. However, in cases where the author cannot be identified or be brought before a court in Switzerland, then the editor

---

152 See DFJP, Rapport "Cybercriminalité" (see FN 102), pp. 156–169.

153 Among the offences committed and completed through publication in a medium are the offences against personal honour contained in Art. 173 ff. Swiss Criminal Code and the breach of official secrecy or professional confidentiality of Arts. 320–321 Swiss Criminal Code.

154 Among the offences committed and completed through publication in a medium are the offences against personal honour contained in Art. 173 ff. Swiss Criminal Code and the breach of official secrecy or professional confidentiality of Arts. 320–321 Swiss Criminal Code, see DFJP, Rapport "Cybercriminalité" (see FN 102), pp. 62 f.

155 Stefan Trechsel/Dean Crameri, Art. 144bis Swiss Criminal Code (see FN 35), p. 734 N 12.

156 Franz Zeller, Art. 28 Swiss Criminal Code, in: Marcel A. Niggli/Hans Wiprächtiger (eds.), Strafrecht I, Art. 1–110 StGB/Jugendstrafgesetz, Basler Kommentar, 2nd edition, Basel 2007, p. 537 N 31.

157 Stefan Trechsel/Marc Jean-Richard-dit-Bressel, Art. 28 Swiss Criminal Code, in: Stefan Trechsel/Mark Pieth (eds.), Schweizerisches Strafgesetzbuch, Praxiskommentar, 2nd edition, Zürich/St. Gallen 2013, p. 174 N 3.

158 Franz Zeller, Art. 28 Swiss Criminal Code (see FN 156), p. 538 N 35.

159 Franz Zeller, Art. 28 Swiss Criminal Code (see FN 156), p. 539 N 36; Marcel A. Niggli/Franz Riklin/Günter Stratenwerth (see FN 141), p. 19; Stephanie Müller (see FN 23), pp. 245 f.; Günter Stratenwerth (see FN 138), pp. 441 N 167 with further references.

is liable to prosecution for the offence of failure to prevent an illegal publication.[160] If, in turn, there is no responsible editor, then the person responsible for the publication is liable to prosecution for the said offence. Hence, the provision embodies a system of subsidiary liabilities.[161] If, due to the inadequate organization of a corporation, no natural person responsible for the publication can be identified, the corporation as such can be held liable in a subsidiary way provided that all the requirements of Article 102 Swiss Criminal Code are fulfilled.[162]

Since the publication of content on the internet is generally automatic and the content is not subject to a preliminary content review by technical personnel, it is unclear whether host providers can be said to be responsible for publication in the sense of Article 28 Swiss Criminal Code.[163] What can be said with certainty is that host providers who edit contributions of its users can be held criminally liable for illegal content.[164] Thereby, liability can be construed by applying the rules of participation since the editing of content by the host provider can be seen as aiding and abetting the cybercrime committed by the content provider.[165] On the other hand, a host provider editing content of a website is comparable to an editor of a newspaper and could thus be held liable based on Article 28 Swiss Criminal Code. However, if providers, which only permit publishing content on a technical level without reviewing the content as such, were held liable in cases where no responsible person for the publication can be identified, a system of quasi unlimited liability would thereby be created.[166] It is for that reason that there is no unanimity in doctrine and case law as to whether provider liability can be construed based on Article 28 Swiss Criminal Code,[167] which was drafted with a view to create liability on the part of media publication in the classical sense, such as newspapers and magazines, and does not address the unique problems in the realm of cybercrime.[168] As regards access providers, the prevailing view is that they should not be held liable for providing access to the internet under Article 28 Swiss Criminal Code on criminal liability of the media.

Overall, the rules on criminal liability of the media do not quite fit cybercrime offences committed by means of the internet and are – with the exception of one aspect of Article 144bis(2) Swiss Criminal Code – not applicable to cybercrimes.[169]

---

160 Art. 322bis Swiss Criminal Code.

161 Stefan Trechsel/Marc Jean-Richard-dit-Bressel, Art. 28 Swiss Criminal Code (see FN 157), p. 173 N 1.

162 Art. 102 Swiss Criminal Code only applies to misdemeanours, which are defined in Art. 10 para. 3 Swiss Criminal Code as "offences that carry a custodial sentence not exceeding three years or a monetary penalty". Art. 144bis para. 2 and Art. 322bis Swiss Criminal Code are both misdemeanours according to that definition.

163 DFJP, Rapport "Cybercriminalité" (see FN 102), p. 68; Christian Schwarzenegger (see FN 128), p. 55.

164 DFJP, Rapport "Cybercriminalité" (see FN 102), pp. 68 f.

165 Christian Schwarzenegger (see FN 128), p. 46.

166 Marcel A. Niggli/Franz Riklin/Günter Stratenwerth (see FN 141), p. 19; also see decision 6B_645 2007 and 6B_650/2007, 2 May 2008, consid. 7.3.4.4.2, where the Swiss Federal Supreme Court denied the obligation to control all uploaded material on the providers server; also see Alexander Kernen, Volle Verantwortlichkeit des Host Providers für persönlichkeitsverletzende Handlungen seines Kunden – Gemäss Bundesgericht steht einer Blogbetreiberin bei Beseitigungs- und Feststellungsansprüchen kein Haftungsprivileg zu, Jusletter du 4 mars 2013, N 9 and 25.

167 See for a more detailed discussion Marcel A. Niggli/Franz Riklin/Günter Stratenwerth (see FN 141), pp. 8 ff. with further references; also see Franz Zeller, Art. 28 Swiss Criminal Code (see FN 156), p. 557 N 79.

168 Art. 28 Swiss Criminal Code read together with Art. 322bis Swiss Criminal Code ("Failure to prevent an illegal publication").

169 Rapport modification (see FN 118), pp. 7 f.; DFJP, Rapport "Cybercriminalité" (see FN 102), pp. 68 and 156–169; Marcel A. Niggli/Franz Riklin/Günter Stratenwerth (see FN 141), pp. 18 ff.

(dd) Corporate criminal liability

Criminal liability of corporations is regulated by Article 102 Swiss Criminal Code. Article 102(2) Swiss Criminal Code sets forth that a corporation can be held criminally liable for specific offences irrespective of the criminal liability of any natural person. However, none of the four cybercrimes under consideration in this report is among the offences that give rise to such primary corporate liability.[170]

Article 102(1) Swiss Criminal Code foresees general and subsidiary liability of corporations in cases where the offence was committed in the exercise of commercial activities in accordance with the objects of the corporation and if it is impossible to attribute the conduct to a specific natural person due to the inadequate organization of the corporation. Unlike primary corporate liability, this form of general and subsidiary liability is not limited to specific offences. Hence, the four cybercrimes are clearly covered by it.[171]

The first question concerning corporate liability under Article 102(1) Swiss Criminal Code is whether a host provider, which is a corporation, can be held liable for the illegal content uploaded by a content provider. This question can clearly be answered in the negative. Corporate liability only arises if a criminal act is committed by a person within the organizational structure of a corporation.[172] It does not extend to entities lying outside the corporation's sphere of influence, such as clients.[173] In cases of cybercrimes, neither access nor content providers are within the organizational structure of a host provider, they merely have a contractual relationship as clients. Thus, no liability arises under Article 102(1) Swiss Criminal Code.

However, corporate liability plays an important role *if* one could attribute responsibility to a host provider through the rules on participation. If a host provider is not a natural but a legal person, it is still only criminally liable in cases where Article 102(1) Swiss Criminal Code is applicable. This first requires that the responsibility for the criminal act cannot be attributed to a natural person, e.g. an employee, due to organizational deficiencies.[174] Second, the provision requires that the offence is committed "in the exercise of commercial activities in accordance with the objects of the undertaking". This requirement ensures that there is a link between the underlying offence for which the corporation shall be held liable and the activity of the corporation.[175] Only if these requirements are met can a host provider that is a legal person be held criminally liable under Swiss law.

In sum, absent any specific provisions governing provider liability, criminal conduct must be attributed to providers by applying general rules on attribution, while the provisions on criminal liability of the media and on corporate criminal liability are not quite tailored to the specificities of providers. However, which

170 Message relatif cybercriminalité (see FN 9), pp. 4291–4293.

171 Message relatif cybercriminalité (see FN 9), pp. 4291–4293.

172 This can, for example, be organs, partners or employees and, arguably, in the case of outsourcing, persons mandated and persons acting for the benefit of a corporation and with its acquiescence; on this, see Marcel A. Niggli/Diego Gfeller, Art. 102 Swiss Criminal Code, in: Marcel A. Niggli/Hans Wiprächtiger (eds.), Basler Kommentar, Strafrecht I, 2nd edition, Basel 2007, p. 1710 N 69.

173 Marcel A. Niggli/Diego Gfeller, Art. 102 Swiss Criminal Code (see FN 172), p. 1709 N 66.

174 Günter Heine, Organisationsverschulden aus strafrechtlicher Sicht: Zum Spannungsfeld von zivilrechtlicher Haftung, strafrechtlicher Geschäftsherrenhaftung und der Strafbarkeit von Unternehmen, in: Marcel A. Niggli/Marc Amstutz (eds.), Verantwortlichkeit im Unternehmen aus zivil- und strafrechtlicher Sicht, Basel 2007, pp. 93–124 and pp. 100 ff.; Mark Pieth, Die strafrechtliche Verantwortung des Unternehmens, ZStrR 2003, pp. 353 ff. and p. 365.

175 Günter Stratenwerth (see FN 138), pp. 450 N 186.

avenue is chosen in a specific case heavily depends on the view of a specific judge and is thus unpredictable to a certain degree.[176]

b) Jurisdictional implications of attribution of responsibility

The different ways by which to attribute responsibility to providers may have jurisdictional implications, notably as regards the establishment of a place of commission in Switzerland.

For instance, if criminal liability is attributed based on the rules on participation, one has to keep in mind the peculiarities of the Swiss regulations regarding participation, which were discussed earlier.[177] Essentially, the conduct of a co-perpetrator in Switzerland suffices to establish jurisdiction for all co-perpetrators. However, if a person is aiding and abetting in Switzerland an offence committed abroad, this conduct does not give rise to a place of commission in Switzerland. Hence, the conduct of a host provider in Switzerland does not establish a place of commission in Switzerland if all the other events took place abroad.[178]

Furthermore, if responsibility of providers were attributed based on the provisions on criminal liability of the media, it is sufficient that the illegal content is accessible in Switzerland to create a place of commission and thus jurisdiction.[179]

Moreover, given the possible transnational nature of cybercrimes, corporate liability according to Article 102(1) Swiss Criminal Code not only applies to entities incorporated under Swiss law but also extends to foreign entities, i.e. corporations and other undertakings of foreign law.[180] However, it is necessary that either the place of commission of the offence (i.e. the place where the organizational measures allowing for attribution of illegal conduct to a natural person should have taken place) or the place where the result occurs is located in Switzerland. This seems to exclude liability under Article 102 Swiss Criminal Code if a provider is not incorporated in Switzerland and if neither the conduct nor the result as defined earlier can be located there.[181]

In conclusion, there are no specific rules on provider liability under Swiss law. The provider's responsibility for cybercrimes, however, can be established based on either the general rules on participation or the rules of the responsibility of the media. If a provider is a legal person, responsibility can only be attributed if the requirements for corporate liability according to Article 102(1) Swiss Criminal Code are met. For either means of attribution of responsibility, the general jurisdictional rules as set out earlier[182] are applicable. However, given the lack of relevant case law regarding cybercrimes, many questions remain controversial.

---

176 Ordonnance du 24 février 1982 sur l'entraide internationale en matière pénale, etat le 5 décembre 2006, RS 351.11 [hereinafter "Mutual Assistance Ordinance"].

177 See Section B.1.b.dd of this report.

178 See Section B.1.b.dd of this report; as well as Marcel A. Niggli/Franz Riklin/Günter Stratenwerth (see FN 141), p. 6.

179 See section B.1.b.bb of this report.

180 See Art. 102 para. 4 Swiss Criminal Code; Stefan Trechsel/Marc Jean-Richard-dit-Bressel, Art. 102 Swiss Criminal Code (see FN 157), p. 552 N 6.

181 Marcel A. Niggli/Diego Gfeller, Art. 102 Swiss Criminal Code (see FN 172), p. 1764 N 412.

182 See Section B of this report.

D. Cooperation in criminal matters

1. Impact of specificities of information technology on mutual assistance

Under Swiss law, mutual legal assistance is primarily governed by the Mutual Assistance Act and the Mutual Assistance Ordinance.[183] In addition, other legal acts contain provisions relevant for mutual legal assistance,[184] such as the Swiss Criminal Procedure Code.[185]

Thus far, the specificities of information technology have not caused a paradigm shift in Swiss law on mutual legal assistance in criminal matters. Rather, the legal framework still abides by the classical principles of international cooperation in criminal matters, most notably the submission of a request for assistance from one State to another. However, this is not to say that the specificities of information technology are absent from relevant legal acts. To the contrary, the legal acts governing mutual legal assistance contain various (to some extent rather new) norms explicitly taking into account the developments in the realm of information technology. For instance, the recent ratification of the Convention on Cybercrime – which equally follows the classical principles of international cooperation in criminal matters[186] – triggered the adoption of a new provision in the Mutual Assistance Act on the transmission of electronic communications traffic data to another State before the conclusion of the respective mutual assistance proceedings.[187] When analysing the impact of information technology on the nature and characteristics of mutual legal assistance in criminal matters, one must, however, bear in mind that the exchange of information does not only take place on a formalized level, i.e. following the respective procedures laid down in the rules on mutual legal assistance. Rather, in many instances, an informal exchange of information takes place, which bypasses the formal proceedings on mutual assistance.[188]

As regards the collection of evidence in cyberspace for criminal proceedings, the Swiss Criminal Procedure Code does not contain any explicit and specific provisions. However, various norms refer to hardware and techniques (e.g. computers, data storage devices, telecommunications) used for collecting evidence from the internet and thus apply to this new form of evidence collection, which has steadily grown in importance. What is more, many provisions of the Swiss Criminal Code are of a general nature and are thus also applicable to this type of evidence gathering.[189] However, given the rather fast pace of developments in the realm of information technology, the interpretation and meaning

---

183 See FN 176.

184 For a rather complete list of Swiss legislation governing mutual legal assistance, see: Bases légales nationales sur l'entraide internationale en matière pénale, ‹www.rhf.admin.ch/rhf/fr/home/straf/recht/national.html› (accessed 5 May 2013); Accords multilatéraux d'entraide judiciaire internationale en matière pénale ‹www.rhf.admin.ch/rhf/fr/home/straf/recht/multilateral.html› (accessed 5 May 2013); and Accords bilatéraux d'entraide judiciaire internationale en matière pénale, ‹www.rhf.admin.ch/rhf/fr/home/straf/recht/bilateral.html› (accessed 5 May 2013).

185 Art. 54 Swiss Criminal Procedure Code.

186 International Association of Penal Law, Newsletter 1/2012, p. 48 FN 17; see also ‹www.penal.org/IMG/Newsletter 2012-2EN(1).pdf› (accessed 5 May 2013).

187 Art. 18b Mutual Assistance Act (see FN 69); on this provision, see below Section D.2.c. if this report.

188 See, for example, ATF 132 II 1, summary of the decision (*regeste*), where the Swiss Federal Supreme Court discussed the problem of informal information exchange by allowing the activity of foreign undercover agents in Switzerland: "L'intervention d'agents infiltrés par la voie de l'entraide judiciaire est particulièrement problématique parce que le flux d'informations entre l'agent et son supérieur n'est pas contrôlable et qu'elle remet en question le principe fondamental du droit de l'entraide judiciaire d'après lequel aucun renseignement utilisable par l'autorité requérante ne doit lui parvenir avant l'entrée en force de la décision de clôture.".

189 Sabine Gless, Strafverfolgung im Internet, ZStrR 2012, p. 6.

of these norms in the context of a specific means or technique of evidence collection in cyberspace is often a controversial topic of discussion.[190]

2. Interception of (wireless) telecommunications

a) Requirements for interception of (wireless) telecommunications

Under Swiss law, the interception of (wireless) telecommunications in the context of criminal proceedings and mutual legal assistance in criminal matters is governed by different legal bases, namely the Swiss Criminal Procedure Code,[191] the Communication Surveillance Act[192] and the Mutual Assistance Act.[193]

The Mutual Assistance Act governs surveillance of telecommunications in the context of mutual assistance cases in general and specifically to establish the whereabouts of the defendant in extradition cases. However, it only contains sparse regulation of these issues and mainly refers to the relevant provisions of the Swiss Criminal Procedure Code referred to above and to the Communications Surveillance Act.[194]

The relationship between the provisions on surveillance of post and telecommunications of the Swiss Criminal Procedure Code and the Communications Surveillance Act – notably the issue of which act prevails in cases of conflicting prescripts – is not entirely clear. Thus, for example, in a recent (criticized)[195] case involving the issue of how far back in time traffic and invoice data and subscriber information can be requested, the Swiss Federal Supreme Court decided that the more permissive provision of the Communications Surveillance Act is *lex specialis* and prevails over the six months deadline stipulated in the relevant provision of the Swiss Criminal Procedure Code.[196]

Switzerland is not a party to any agreement specifically pertaining to cross-border interception of telecommunications. However, it is a party to the Convention on Cybercrime containing, *inter alia*, provisions on the interception of communications, notably Articles 30 and 33, which have been incorporated into Swiss law by Article 18(b) Mutual Assistance Act. It bears mentioning that the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, which was ratified by Switzerland,[197] provides for cross-border observation and covert investigations,[198] but does not contain any rules on transnational interceptions of telecommunications.

---

190 See, for example, Section D.2.a.bb of this report on the controversy surrounding whether the use of GovWare is allowed under Swiss law.

191 Among the most pertinent rules of the Swiss Criminal Procedure Code are Art. 246 ff. on the search of records and recordings, Art. 263 ff. on seizure, Art. 269 ff. on the surveillance of post and telecommunications, Art. 282 ff. on observation and Art. 286 ff. on undercover investigations.

192 Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication, état le 16 juillet 2012, RS 780.1 [hereinafter "Communication Surveillance Act"].

193 Among the most pertinent provisions of the Mutual Assistance Act (see FN 69) are Art. 18a and 18b.

194 Art. 18a para. 4 Mutual Assistance Act (see FN 69).

195 Andreas Heiniger, Das Bundesgericht geht in der Fernmeldeüberwachung weiter, als es das Gesetz erlaubt, Anmerkungen zu BGE 1B_481/2012 vom 22. Januar 2013, Jusletter du 22 janvier 2013.

196 Juan Vasella, BGE 1B_481/2012: Rückwirkende Internet-Teilnehmeridentifikation für längeren Zeitraum als sechs Monate zulässig, swissblawg, 18 February 2013, ‹www.swissblawg.ch/2013/02/1b4812012-ruckwirkende-internet.html› (accessed 5 May 2013).

197 Ordonnance du 16 décembre 2009 sur le système de gestion de personnes, de dossiers et d'affaires (PAGIRUS) de l'Office fédéral de la justice, RS 0.351.12.

198 Arts. 17 and 19 Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters.

Communications in cyberspace take many different forms and, as a consequence, the rules and requirements governing the interception of such communications for the purpose of evidence collection vary. In the following, four important situations are discussed: The control of e-mail communications, the surveillance of voice over internet telephony, the interception of traffic data and covert investigations on the internet.

(aa) E-mail communications

The use of e-mail is among the most popular forms of internet-based communication. Law enforcement officials can obtain information contained in e-mails either by surveilling the flow of information in real-time or after the correspondence has already taken place. The form chosen notably depends on whether a specific case requires covert surveillance or whether it suffices to store messages after they have been sent and received. The decision to use one or the other type of evidence gathering may also be influenced by pragmatic considerations, such as which form allows the easiest access to e-mail correspondence.[199]

The *search* for stored e-mails for purposes of evidence gathering is subject to the rules on the search of records and recordings of the Swiss Criminal Procedure Code.[200] Among the recordings and data carriers mentioned in Article 246 Swiss Criminal Procedure Code are CDs, USB sticks, hard discs or servers.[201] A *seizure* of e-mail correspondence is subject to the general rules on seizure of the Swiss Criminal Procedure Code.[202] The use of the internet to collect e-mails as evidence is generally only necessary if the messages or correspondence is only accessible via the internet, most notably where cloud computing is used to store the relevant data. But even in this case, the cloud containing the data is stored at a physically localized server, which can be searched by the competent law enforcement body. Hence, the generally applicable rules on the search and seizure of recordings laid down in the Swiss Criminal Code are applicable to e-mail communications.[203]

The applicable legal framework is different if an e-mail correspondence is surveilled in real-time and in a covert manner. According to the prevailing view in doctrine, this measure, which is the interference with an ongoing communication without the knowledge of the participants to it, can only take place pursuant to the rather stringent rules on the surveillance of post and telecommunications, which are primarily laid down in Articles 269 *et seq.* Swiss Criminal Procedure Code and the Communications Surveillance Act. Unlike telephone conversations, where as a general rule the content can only be captured by wiretapping, an e-mail correspondence leaves a trace since the messages are stored. Nevertheless, it is illegal to *secretly* seize such stored correspondence. Rather, gaining access to the content of an e-mail correspondence is only possible either as a measure of surveillance of telecommunications if conducted without the knowledge of the participants or by means of an "open" seizure, which the respective person(s) are informed of.[204]

---

199 Sabine Gless (see FN 189), p. 6.

200 Art. 246 ff. Swiss Criminal Procedure Code.

201 Michael Aepli, Die strafprozessuale Sicherstellung von elektronisch gespeicherten Daten, Zürich 2004, pp. 89 ff. and 118 ff.; Olivier Thormann/Beat Brechbühler, Article 246 Swiss Criminal Procedure Code, in: Marcel A. Niggli/ Marianne Heer/ Hans Wiprächtiger (eds.), Schweizerische Strafprozessordnung/Jugendstrafprozessordnung, Basler Kommentar, Basel 2011, p. 1652 f. N 3.

202 Art. 263 ff. Swiss Criminal Procedure Code.

203 Sabine Gless (see FN 189), pp. 8–9.

204 Sabine Gless (see FN 189), p. 10; on when the control of content of an e-mail correspondence must take the form of a surveillance measure and when such data can be subject to an "open" seizure, see Andreas Donatsch/Albert Schmid, Der Zugriff auf E-Mails im Strafverfahren – Überwachung (BÜPF) oder Beschlagnahme?, in: Christian Schwarzenegger/Oliver Arter/Florian S. Jörg (eds.), Internet-Recht und Strafrecht, 4. Tagungsband, Bern 2005, p. 151 ff.

(bb) Voice over IP

The rules governing surveillance of post and telecommunications[205] not only apply to traditional conversations over the telephone, but also to new forms of communication, such as mobile phones and voice over internet telephony. The technical features of voice over IP telephony, however, differ considerably from traditional telephone communications and, as a consequence, special challenges arise for internet providers in making such conversations accessible to law enforcement agencies. This holds especially true for internet telephony services, which are based on peer-to-peer and client-server systems, such as Skype. This type of internet telephony is not computer-based and the conversation is encrypted and sent in data parcels through the internet. Since the content of the communication is only decrypted and "re-assembled" at the recipient's computer, the conversation cannot be intercepted in the line, i.e. when transmitted – as is possible for landline phone calls.[206] Such voice over IP conversations can only be intercepted either by obtaining the cooperation of a provider or by using spyware (also known as GovWare), which can decrypt the data or manipulate the microphone.

It is a controversial issue whether the use of GovWare is allowed for evidence collection purposes under Swiss law. One side argues that the use of spyware is imperative for telephone tapping and covered by Articles 269 to 279 Swiss Criminal Procedure Code (provisions on the surveillance of post and telecommunications) read together with Article 280 Swiss Criminal Procedure Code (provisions on the permitted use of technical surveillance devices).[207] This view is considered problematic by others who argue that, according to experts, spyware currently available can generally not be limited to registering a voice over IP conversation. Rather, GovWare also allows for, *inter alia*, the search of computers and activation of microphones, which allows for other conversations taking place in the room to be registered. Hence, they argue that for this type of surveillance, a legal basis is missing from Swiss law and that the use of GovWare is notably not covered by Articles 280 *et seq.* Swiss Criminal Procedure Code (on surveillance using technical surveillance devices) and Articles 282 *et seq.* Swiss Criminal Procedure Code (on observation).[208]

From this short overview of the different stances on the permissibility of the use of GovWare accrues that the current legal basis is not sufficiently clear. Against this background, the Swiss Government submitted a draft law to the Parliament in February 2013, which aims at introducing a legal basis specifically regulating the use of spyware for law enforcement purposes. According to this draft, the use of GovWare shall, subject to certain criteria, be permitted to intercept the content of a conversation and traffic data for the investigation and prosecution of certain particularly grave offences listed in the law, but not for purely preventive purposes. At the same time, online searches and the surveillance of rooms with microphones or cameras is prohibited by the draft law.[209] Since the draft law is still in the early

---

205 Art. 269 ff. Swiss Criminal Procedure Code and Communications Surveillance Act (see FN 192).

206 Marco Gercke/ Philipp W. Brunst, Praxishandbuch Internetstrafrecht, Stuttgart 2009, pp. 335 ff., N 844 ff.

207 See Sylvain Métille, Les mesures de surveillance prévues par le CPP, Jusletter du 19 décembre 2011, N 33; Olivier Jotterand/Jérémie Müller/Jean Treccani, L'utilisation du cheval de Troie comme mesure de surveillance secrète, Jusletter du 21 mai 2012, N 20.

208 Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter du 5 décembre 2011, N 18; Stefan Heimgartner, Strafprozessuale Beschlagnahme, Zürich/Basel/Genf 2011, p. 41; Niklaus Ruckstuhl/Volker Dittmann/Jörg Arnold, Strafprozessrecht, Zürich 2011, N 858; Dominic Ryser: «Computer Forensics», eine neue Herausforderung für das Strafprozessrecht, in: Christian Schwarzenegger/Oliver Arter/Florian S. Jörg (eds.), Internet-Recht und Strafrecht, 4. Tagungsband, Bern 2005, pp. 553 ff. and p. 576; Martin Steiger, Bundestrojaner ohne Rechtsgrundlage in der Schweiz, available at ‹www.steigerlegal.ch/2011/10/13/bundestrojaner-ohne-rechtsgrundlage-in-der-schweiz› (accessed 5 May 2013).

209 Confédération Suisse, Surveillance des communications: des bases légales claires et modernes, 27 février 2013, ‹www.news.admin.ch/message/index.html?lang=fr&msg-id=47920› (accessed 5 May 2013).

stages of the legislative process, it is difficult to predict whether this draft law will ultimately pass and whether the main features described will be retained.

(cc) Traffic data

According to Article 273 Swiss Criminal Procedure Code, the collection of traffic and invoice data and subscriber information is allowed. Currently, this data can be requested for the previous six months. The draft law mentioned above[210] proposes an extension of this period to twelve months.[211]

As stated earlier, the Communications Surveillance Act also stipulates that traffic data can be requested. Unlike Article 273 Swiss Criminal Procedure Code, Article 14(4) Communications Surveillance Act does not contain a deadline for how long back traffic data can be obtained. We have already referred to a recent case in which the Swiss Federal Supreme Court considered the (more permissive) provision of the Communications Surveillance Act to be foregoing *lex specialis*.[212]

(dd) Covert observations on the internet

Debate also surrounds the question whether and in which form law enforcement officials are allowed to collect information for criminal proceedings from publicly accessible chat rooms, websites and blogs, i.e. "public cyberspace" without being specifically authorized to do so. The answer mainly depends on the intensity and length of such observations and the interaction of law enforcement officials with other persons. It is argued that law enforcement officials can visit the public cyberspace and store data so long as they do not actively intervene in a conversation. This type of observation in the public cyberspace is comparable to a police patrol in the real world, where law enforcement officials can observe persons on public property without further ado. However, the situation must be qualified differently if targeted surveillance of a person or a group of persons takes place around the clock and over a longer period. This type of observation, it is argued, cannot be compared to a police patrol in the real world, but must rather abide by the criteria set forth in Article 282 Swiss Criminal Procedure Code governing observation. In cases where law enforcement officials start entering into contact with a specific person, this amounts to an undercover investigation, which must abide by the requirements set forth in Articles 286 *et seq.* Swiss Criminal Procedure Code.[213]

b) Providers or satellites located outside Switzerland

All three Swiss companies offering mobile phone services have concluded roaming contracts with foreign companies. According to these contracts, the clients of foreign companies can use their foreign SIM cards in Switzerland by using the networks of the Swiss companies. In such cases, the Communication Surveillance Act also applies to these foreign companies. Theoretically, foreign internet providers are also subject to the Communication Surveillance Act. However, technical difficulties arise in surveilling the e-mail correspondence of a client using the services of a foreign provider in Switzerland.[214]

c) Mutual legal assistance concerning interception of telecommunications

As stated earlier in this report, the surveillance of telecommunications in mutual legal assistance cases is governed by Article 18a Mutual Assistance Act. According to this provision, surveillance of telecommunications traffic may be ordered by Swiss authorities at the request of another State in order to establish the whereabouts of a person sought for extradition and in other mutual assistance

210 See Section D.2.a.bb of this report.

211 Confédération Suisse, Surveillance (see FN 209).

212 See Section D.1 of this report.

213 Sabine Gless (see FN 189), p. 15.

214 August Biedermann, Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 6. Oktober 2000, ZStrR 2002, p. 80.

cases.[215] While Article 18a Mutual Assistance Act designates the competent authorities for the issuance of a surveillance order, it stipulates that the requirements and procedure for surveillance in the context of mutual assistance are governed by Articles 269 to 279 Swiss Criminal Procedure Act on surveillance of post and telecommunications and the Communications Surveillance Act.[216]

A considerable amount of time may elapse between a request for mutual assistance and the issuance of a final and binding surveillance order in mutual legal assistance proceedings. This long duration stands in stark contrast to the fast-paced nature and fluidity of electronic data, which can be moved across borders within seconds and is often not stored over a longer period. Hence, such data may no longer be available at the conclusion of mutual assistance proceedings. Hence, electronic data differs from "traditional" pieces of evidence, which generally persist in time and are not as easy to move from one location to another. In light of this and in order to bring Swiss procedural law in line with Article 30 Convention on Cybercrime on the expedited disclosure of preserved traffic data and Article 33 Convention on Cybercrime governing mutual assistance in real-time collection of traffic data, Article 18b Mutual Assistance Act on electronic communications traffic data was adopted.[217]

Essentially, Article 18b(1) Mutual Assistance Act allows Swiss authorities dealing with a request for mutual assistance to transmit electronic communications traffic data to another State before the conclusion of the mutual assistance proceedings in two situations: First, if provisional measures indicate that the communication, which is the subject of the request, originated abroad and, second, if the data was acquired by the executing authority based on an order for authorised real-time surveillance according to Articles 269 to 281 Swiss Criminal Procedure Code. An important *caveat* is stipulated in Article 18b(2) Mutual Assistance Act: The data transmitted before the conclusion of the mutual assistance proceedings must not be used as evidence. Such use only becomes possible once the request for mutual assistance has been granted by way of a legally binding decision and the extent of it determined by such a decision. However, the means Switzerland has at its disposal to enforce an order addressed to a third State not to use such data as evidence – unless granted by way of a decision resulting from mutual assistance proceedings – may be limited.

For the individual subject to surveillance, an important difference accrues regarding whether surveillance takes place based on an order adopted in full-fledged mutual assistance proceedings of Article 18a Mutual Assistance Act or as a provisional measure foreseen in Article 18b Mutual Assistance Act, most notably as regards the right to be heard on the transmission of data. In cases of the former, the individual has a right to participate in the proceedings and to access the files if this is necessary to safeguard his interests.[218] In cases of the latter, transmission take place without the person subject to surveillance being informed beforehand and granted an opportunity to put forward his or her arguments against the handover of the information collected.[219] Hence, the willingness on the part of the Swiss legislature to share data with third States already in the early stages of investigations and proceedings

---

215 Art. 18a para. 1 and 2 Mutual Assistance Act (see FN 69).

216 Art. 18a para. 3 Mutual Assistance Act (see FN 69).

217 Message relatif cybercriminalité (see FN 9), pp. 4276 and 4309–4314.

218 Art. 80b Mutual Assistance Act (see FN 69); on this provision, see Laurent Moreillon, Entraide internationale en matière pénale, Basel 2004, pp. 371–375; the right to be heard specifically is guaranteed by Art. 29 para. 2 Swiss Constitution (see FN 123) and Art. 26–30 of the Federal Act of 20 December 1968 on Administrative Procedure to which Art. 12 Mutual Assistance Act (see FN 69) refers: *idem*, p. 372.

219 Message relatif cybercriminalité (see FN 9), pp. 4310–4311.

does not come without drawbacks on the level of individual rights – which are, however, according to one view, sufficiently safeguarded under the new Article 18b Mutual Assistance Act.[220]

Lastly, it bears mentioning that some requests of third States for telephone interception are accompanied with little factual information. This renders it difficult for Swiss authorities to decide whether the requirements for surveillance of telecommunications are met, which are set rather high in order to protect privacy.[221] This holds notably true for the requirement that a strong suspicion must exist that a specific offence has been committed. In practice, a way around this rather stringent test has been found: Switzerland requires an assurance from the foreign authorities when providing them with data by means of a provisional measure that they only use the data for investigation purposes and not as formal evidence in criminal proceedings. Whether such assurances actually safeguard the rights and interests of persons subject to surveillance is debatable.[222]

3. Grounds for refusing a request regarding searches of the internet, computer and networks

Under Swiss law, a request for mutual legal assistance can be refused on a number of grounds, notably if the granting of assistance violates certain human rights of the person concerned.[223] A request for mutual assistance concerning the search in cyberspace is, in principle, subject to these same rules. However, there is little doctrine available on the fundamental rights potentially violated by such measures. Among the constitutional rights that may be at stake in cases of internet, computer and network searches are notably the right to privacy in persons' private and family life, their home, mail and telecommunications, the right to be protected against the issuance of their personal data, and the freedom of expression and information.[224]

A special concern regarding requests for assistance regarding searches of the internet, computers and networks is the right of the individual to participate and to be heard in the relevant proceedings and to subject respective decisions to judicial control. As a general rule, each person who has been subject to a covert investigation must be informed afterwards about the specific measure and be provided a possibility for judicial control. If a surveillance measure is taken in a domestic case, the person must be notified at latest after the investigation is closed according to Article 10 Communication Surveillance Act. If this rule were applied when executing a letter rogatory, the requesting authority could only obtain the information after a final decision based on Article 80b Mutual Assistance Act. This would defeat the purpose of many requests of foreign authorities for surveillance. In doctrine, two courses of action have been proposed. The first is that Swiss authorities open an investigation of their own, one which meets all the requirements of national law for the respective surveillance measure. Data obtained in that procedure is provisionally handed over to foreign authorities under the condition that the receiving State issues assurances that the data will only be used for investigation but not for evidence purposes.[225] A second way to proceed is that Swiss authorities require foreign authorities to inform the person

---

220 On how the interests of the person whose electronic communications traffic data is transmitted by virtue of Art. 18b Mutual Assistance Act (see FN 69), see Message relatif cybercriminalité (see FN 9), pp. 4310–4311.

221 See, for example, ATF 132 II 1, N 2.3.

222 Stefan Wehrenberg/Irene Bernhard, Auslieferung trotz kritischer Menschenrechtslage – Einhaltung von Menschenrechten durch diplomatische Garantien?, Jusletter du 28 avril 2008.

223 Sabine Gless, Internationales Strafrecht, Basel 2011, pp. 108 ff.

224 Arts. 13 and 16 Swiss Constitution (see FN 123); on the specific content of these rights, see Jörg Paul Müller/Markus Schefer, Grundrechte in der Schweiz, 4th edition, Bern 2008; on human rights and cooperation, see also Sections E.1 and 2 of this report.

225 August Biedermann (see FN 214), p. 82.

concerned about the surveillance measure.[226] Both courses of action are based on trust since Switzerland cannot enforce assurances issued by a third State.[227]

4. Double criminality requirement

Under Swiss law on mutual assistance, there is no specific provision requiring double criminality for cases where the conduct under consideration is legal at the place of commission but illegal in the jurisdiction where it displays its effects. However, the general rule stated in Article 30(1) Mutual Assistance Act – according to which Swiss authorities may not address requests to another State if they themselves could not grant such requests under the Mutual Assistance Act – could be a fall-back rule for this situation.[228] What is more, according to Article 64 Mutual Assistance Act, measures requiring the use of procedural compulsion can only be ordered "if the description of the circumstances of the case indicates that the offence being prosecuted abroad contains the objective elements of an offence under Swiss law. The measures must be carried out in accordance with Swiss law."

When assessing the double criminality requirement, the competent Swiss authorities merely examine whether the facts provided by a foreign authority requesting mutual legal assistance fulfil the definitional elements of an offence under Swiss criminal law.[229] Thus, if Swiss authorities order surveillance measures in the execution of a letter rogatory, these measures must satisfy all requirements stipulated in Swiss law.[230] Therefore, a request for interception where the underlying conduct triggering the request for this measure is not an offence under Swiss criminal law will be rejected.[231]

5. Extraterritorial investigations

As regards extraterritorial investigations, two situations must be distinguished: Firstly, extraterritorial investigations conducted by Swiss authorities abroad and, secondly, extraterritorial investigations carried out by foreign authorities on Swiss territory.

As regards the first constellation, i.e. investigations carried out by Swiss authorities abroad, there is broad consensus among Swiss scholars that they require the consent – either by way of general agreement or on an *ad hoc* basis – of the State on the territory of which these measures are carried out. However, under which circumstances a Swiss official is acting extraterritorially is a controversial issue. For instance, some scholars argue that a Swiss official sitting in Switzerland and downloading data from a computer located abroad is not acting extraterritorially.[232] Meanwhile, other scholars maintain that downloading data stored on a computer located abroad amounts to extraterritorial conduct and thus requires the consent of the State concerned.[233] It must be noted that Article 32 Convention on Cybercrime, to which Switzerland is a party, trans-border access to stored computer data is allowed

---

226 Thomas Hansjakob, BÜPF / VÜPF, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, St. Gallen 2006, p. 282.

227 Stefan Wehrenberg/Irene Bernhard (see FN 222).

228 Stefan Heimgartner (see FN 24), p. 138.

229 Art. 1 Mutual Assistance Ordinance (see FN 176); BGE 1C_138/2007, judgment of 17 July 2007, consid. 2.3.1; ATF 116 Ib 89, p. 94; ATF 132 II 81, consid. 2; Nadja Capus, Strafrecht und Souveränität: Das Erfordernis der beidseitigen Strafbarkeit in der internationalen Rechtshilfe in Strafsachen, Bern 2010, pp. 424 ff.; Peter Popp, Die Rechtsprechung des Bundesgerichts zur Internationalen Strafrechtshilfe in den Jahren 2006/2007, ZBJV 2009, p. 303.

230 See Art. 18a para. 3 Mutual Assistance Act (see FN 69).

231 Art. 64 para. 1 Mutual Assistance Act (see FN 69).

232 See, for example, Niklaus Schmid, Strafprozessuale Fragen im Zusammenhang mit Computerdelikten und neuen Informationstechnologien im allgemeinen, ZStrR 1993, p. 109.

233 See, for example, Michael Aepli (see FN 201), p. 130 f.; Stefan Heimgartner (see FN 208), pp. 90 f.; Omar Abo Youssef, Smartphone-User zwischen unbegrenzten Möglichkeiten und Überwachung, ZStrR 2012, p. 105.

without the consent of another State Party in two situations: For open source data and in cases of lawful and voluntary consent of the person who has lawful authority to disclose the data.[234]

Regarding the second constellation, i.e. foreign officials carrying out investigations in Switzerland, they must be authorised by Swiss authorities. Otherwise, such investigations may amount to criminal conduct, notably violating Article 271 Swiss Criminal Code criminalizing unlawful activities on behalf of a foreign State. According to Swiss law, it is possible that foreign authorities are present when a letter rogatory is executed in Switzerland.[235] What is more, after receiving approval by the competent authority, foreign officials can carry out investigations in Switzerland independently.[236]

6. Prohibition of self service

As stated earlier in this report,[237] unauthorised collection of information for foreign authorities is a criminal act in Switzerland.[238] Put differently, so-called "self service" is not permitted unless, as will be discussed later, it occurs in "public cyberspace" – for example, by downloading data from publicly accessible websites.[239] Self-service not only violates the individual rights of persons in third States but also constitutes a serious interference with the sovereignty of that third State.[240]

7. Searching "public cyberspace" and computers located abroad

As regards the permissibility of collecting information for criminal proceedings in "public cyberspace", such as publicly accessible chat rooms, websites, blogs and chat rooms without specific authorization to do so, we refer to our earlier findings.[241]

As to the permissibility of searching computers abroad, we refer to the previously discussed findings on the permissibility of extraterritorial investigations[242] and the applicability of human rights law to such investigative measures.[243]

8. Data exchange based on international agreements

Switzerland is party to various agreements, which foresee an automatic cross-border exchange of data for the prevention, investigation and prosecution of crime.

On the bilateral level, Switzerland concluded, for example, various Passenger Name Record agreements, notably with the United States[244] and Canada.[245] Also, in order to remain within the

---

234 On the meaning of this provision in the context of Swiss law, see Message relatif cybercriminalité (see FN 9), p. 4313.

235 Art. 65a para. 1 and 2 Mutual Assistance Act (see FN 69); on the content of these provisions, see Laurent Moreillon (FN 218), pp. 319–323; see judgments of the Swiss Federal Criminal Court (Cour pénale fédérale) of 15 April 2010, RR.2010.9, consid. 2 ff. and of 26 July 2007, RR.2007.59, consid. 2.2; on the possibility of an appeal against an incidental decision that causes immediate and irreparable prejudice through the presence of persons involved in the foreign proceedings, see Art. 80e para. 2 lit. b Mutual Assistance Act (see FN 69); see Laurent Moreillon (FN 218), pp. 379–382.

236 Office fédéral de la justice, Wegleitung zur internationalen Rechtshifle in Strafsachen, 9th edition, Bern 2009, p. 62, see ‹http://www.rhf.admin.ch/etc/medialib/data/rhf.Par.0085.File.tmp/wegl-str-d-2009.pdf› (accessed 5 May 2013); also see Andreas Donatsch/Stefan Heimgartner/Madeleine Simonek, Internationale Rechtshilfe unter Einbezug der Amtshilfe im Steuerrecht, Zürich/Basel/Genf 2011, p. 4.

237 See Section C.5 of this report.

238 Art. 271 Swiss Criminal Code.

239 See Section C.7 of this report.

240 Michael Aepli (FN 201), p. 130 f.; Susan Brenner/Joseph Schwerha, Transnational Evidence Gathering and Local Prosecution of International Cybercrime, John Marshall Journal of Computer and Information Law 2002, pp. 347–395, p. 374.

241 See Section D.2.a.dd of this report.

242 See Section D.5 of this report.

243 See Section E.2 of this report.

United States Visa Waiver Program, Switzerland signed a PCSC (Preventing and Combating Serious Crime) agreement with the United States and a Memorandum of Understanding for the exchange of data on alleged and known terrorists (HSPD-6) in December 2013. The PSCS agreement notably provides for an automatic exchange of fingerprints and DNA data as a means of preventing and combating serious crime.[246]

On a multinational level, Switzerland is a party to the SIS (Schengen Information System), which is an important tool for data exchange in the realm of cross-border police cooperation.[247] Switzerland established the SIRENE (Supplementary Information Request at the National Entry) Bureau, which is staffed on a 24/7 basis and is part of the Federal Office of Police (Fedpol).

Switzerland is not a party to any agreement similar to the SWIFT agreement between the EU and the US.[248]

9. The exchange, use and protection of data

As a general rule, personal data can only be transferred outside Switzerland under the condition that an adequate level of protection is ensured in the State to where the data is exported. The Federal Data Protection Act[249] contains an exhaustive list of acceptable methods that ensure adequate data protection abroad. For example, the Federal Data Protection and Information Commissioner maintains and publishes a list of States that are considered to provide for an adequate level of data protection. Furthermore, the issuance of "sufficient warranties" that a certain level of data protection will be ensured, notably the inclusion of specific clauses in data transfer agreements, is considered sufficient to ensure data protection in situations of cross-border data transfer.[250] Indeed, many cooperation agreements concluded by Switzerland contain specific provisions on the processing of data that has

---

[244] Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC), Communiqué du 14 janvier 2009, La Suisse et les Etats-Unis concluent un nouvel accord sur les données des passagers aériens, see ‹www.uvek.admin.ch/dokumentation/00474/00492/index.html?lang=fr&msg-id=23258› (accessed 5 May 2013).

[245] Memorandum of Understanding Between the Canada Border Services Agency and the Swiss Federal Office for Civil Aviation Concerning Advance Passenger Information/Passenger Name Record of 17 March 2006, concerning RS 0.748; the agreement has not been published in the RS but can be found at ‹www.news.admin.ch/NSBSubscriber/message/attachments/2242.pdf› (accessed 5 May 2013); information on the conclusion, entry into force, etc. is available at ‹www.eda.admin.ch/eda/fr/home/topics/intla/intrea/dbstv/data04/e_99993604.html› (accessed 5 May 2013).

[246] Département fédéral de justice et police (DFJP), Communiqué du 21 septembre 2012, Maintien dans le Visa Waiver Program des Etats-Unis: le Conseil fédéral approuve deux instruments de coopération, see ‹www.ejpd.admin.ch/content/ejpd/fr/home/dokumentation/mi/2012/2012-09-211.html› (accessed 5 May 2013). The HSPD-6 memorandum of understanding is already in force and is about to be implemented. In order to enter into force, the PCSC agreement must be approved by the Swiss parliament; at this writing, it is not yet clear when the agreement will be submitted to the parliament.

[247] Art. 2 Accord du 26 octobre 2004 entre la Confédération suisse, l'Union européenne et la Communauté européenne sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen (avec annexes et acte final), RS 0.362.31; referring to the adoption of the SIS foreseen by Art. 92 ff. Convention d'application de l'Accord de Schengen du 14 juin 1985 entre les gouvernement des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes; Journal officiel de l'UE n° L 239 du 22/09/2000 p.19–62.

[248] Financial Messaging Data Agreement EU-US, Official Journal of the EU, n° L 195 of 27 July 2010, p. 5.

[249] Federal Act of 19 June 1992 on Data Protection, RS 235.1, see ‹www.admin.ch/ch/e/rs/c235_1.html› (accessed 5 May 2013).

[250] David Rosenthal, Data Protection – Switzerland Q&A- Chapter, in: Practical Law Company (ed.), PLC Cross-border Information Technology 2007/2008 Handbook, p. 82 ‹www.homburger.ch/fileadmin/publications/DAPSWQAC_01.pdf› (accessed 5 May 2013).

been transmitted by Switzerland to the third State or international organization with whom the cooperation agreement has been concluded.[251]

In addition to specific legislation regarding data protection, various other Swiss legal acts, namely the Swiss Criminal Code, contain provisions on the protection of data obtained from abroad or transmitted to a third State or international organization. To illustrate this, we use the example of exchanges of police information with Interpol. Article 352 Swiss Criminal Code stipulates that data protection is governed by the principles of the Mutual Assistance Act as well as the Constitution and General Regulations of Interpol declared applicable by the Swiss Government. Furthermore, the Federal Act on Data Protection has been declared applicable as regards the exchange of information in connection with searches for missing persons and the identification of unknown persons and for administrative purposes.[252] Article 355f Swiss Criminal Code, in turn, governs data exchanges and protection within the framework of judicial cooperation under the Schengen Association Agreements.

Overall, the rules governing data protection in cases of cross-border data transfers are dispersed throughout the Swiss legal framework and the relationship between the different applicable rules is not always entirely clear.

10. Establishing an international enforcement system

In our view, such an international enforcement system can only be implemented among States sharing the same basic values as regards, *inter alia*, privacy, freedom of speech and political rights. However, the UN-ITU summit has once more demonstrated that it is currently impossible to find common ground regarding these questions.[253]

12. Switzerland's participation in Interpol, Europol, Eurojust or other supranational offices

Although Switzerland is not an EU Member State, it has cooperated with Europol since 2006 based on an agreement, which enables both sides to combat certain cross-border crimes.[254] The Swiss Federal Office of Police (Fedpol) acts as the national point of contact between Europol and other competent authorities of Switzerland.[255] Other competent authorities, such as the law enforcement agencies and immigration authorities of the Swiss Confederation and the Cantons are listed in Annex II of the cooperation agreement.[256] Article 355a Swiss Criminal Code allows these authorities to cooperate with Europol, notably to exchange personal data, including sensitive personal data and personality profiles.

Switzerland also cooperates with Interpol. The Swiss Federal Office of Police (Fedpol) carries out the duties of the National Central Bureau, notably by coordinating the exchange of information between the federal and cantonal prosecution services on the one hand, and the National Central Bureaus of other states and the General Secretariat of Interpol on the other.[257]

---

[251] See, for example, Art. 13 Accord entre la Suisse et Eurojust, conclu le 27 novembre 2008, entré en vigeuer par échange de note le 22 juillet 2011, RS 0.351.6; see also Arts. 3 and 5 of the PNR agreement between Canada and the US (FN 245); or Art. 94 Convention of 19 June 1990 implementing the Schengen Agreement (CISA), Official Journal of the EU n° L 239 of 22 September 2000, pp. 19–62.

[252] Art. 352 Swiss Criminal Code.

[253] See ‹http://wcitleaks.org› (accessed 5 May 2013).

[254] Accord entre la Confédération suisse et l'Office européen de police conclu le 24 septembre 2004, RS 0.362.2; also see Markus Mohler, Schengen, Eine Einführung, in: Stephan Breitenmoser/Sabine Gless/Otto Lagodny (eds.), Schengen in der Praxis, Zürich/St. Gallen 2009, pp. 3–24, 6.

[255] Art. 5 Accord entre la Confédération suisse et l'Office européen de police conclu le 24 septembre 2004.

[256] The competent authorities are the police, law enforcement and prosecutorial authorities and immigration authorities.

[257] Art. 350 Swiss Criminal Code.

Switzerland also concluded a cooperation agreement with Eurojust, which has the objective of enhancing cooperation so as to combat serious transnational crimes.[258]

E. Human Rights Concerns

Switzerland is a party to the core human rights treaties, most notably the ECHR and the ICCPR. Furthermore, the Swiss Constitution contains a rather complete catalogue of fundamental rights, and the Swiss Supreme Court regularly interprets and specifies the scope and content of these rights. In addition, many cantonal Constitutions also contain a catalogue of fundamental rights. These individual rights granted on the cantonal level are relevant given that, as a general rule, the investigating and prosecuting authorities are of a cantonal nature.

Various human rights of the Swiss Constitution (which often find a counterpart in cantonal constitutions) are potentially jeopardized in the context of criminal investigations using information technology. Among them are the right to privacy in persons' private and family life, in their home and in relation to their mail and telecommunications, the right to be protected against the misuse of their personal data, and the freedom of expression and information.[259]

These rights, however, have no absolute validity. Rather, they can be restricted by respecting the requirements laid down in Article 36 Swiss Constitution. Firstly, any restriction of fundamental rights, for example through the exercise of investigative powers, must have a legal basis – in cases of significant restrictions, a federal act is necessary, i.e. democratically legitimized legislation. What is more, the restriction must be justified by the public interest or the protection of the fundamental rights of others. In addition, any restriction on fundamental rights must be proportionate and the essence of fundamental rights, i.e. their core, must always be respected.[260] Thus, uses of investigative measures in cyberspace for the purpose of criminal prosecution, which constitute an interference with fundamental rights of the persons subject to the respective measure, are allowed within these parameters.

We now turn to the extraterritorial application of human rights norms to investigative measures conducted by Swiss officials abroad. It must first be noted that there is no consensus in Swiss doctrine on where to draw the line between territorial and extraterritorial conduct in the context of investigative measures that use information technology. This was illustrated earlier by the example of a Swiss official sitting at his desk in Switzerland and downloading data from a computer located abroad. While some argue that this does not amount to an extraterritorial act, others take the opposite stance. Whether such conduct qualifies as extraterritorial conduct not only matters on an inter-state level, but it is also pertinent with regard to the applicability of human rights.[261]

Also, in the realm of mutual assistance, one must draw a distinction between extraterritorial and territorial conduct. Many of the decisions taken in Switzerland, i.e. territorially, may have human rights related consequences abroad, i.e. extraterritorially. A decision taken by Swiss officials in Switzerland (for example, the issuance of an extradition order) is indeed a territorial act – even though the decision may lead to human rights violations abroad. Hence, human rights law – specifically procedural norms influencing the relevant decision on mutual assistance as well as the substantive norms, such as the

---

258 Accord entre la Suisse et Eurojust, conclu le 27 novembre 2008, entré en vigeuer par échange de note le 22 juillet 2011, RS 0.351.6; the objective is described in Art. 2.

259 Arts. 13 and 16 Swiss Constitution (see FN 123); on the specific content of these rights, see Jörg Paul Müller/Markus Schefer (see FN 224).

260 Art. 36 Swiss Constitution (see FN 123); on this provision, see, for example, René Rhinow/Markus Schefer, Schweizerisches Verfassungsrecht, 2nd edition, Basel 2009, pp. 237–245.

261 On this controversy and the importance of the differentiation on an inter-state level, see Section C.5 of this report.

principle of non-refoulement – undeniably apply to such acts and conduct.[262] To the extent that investigations are conducted extraterritorially, it is briefly recalled here that the extraterritorial application of the rights and liberties stipulated in the ECHR and ICCPR is conditioned on the requirement that the State has "jurisdiction" in the sense of the respective jurisdictional clauses of these treaties.[263] Essentially, beyond its own borders, a State has jurisdiction either *de jure* based on an agreement with another State or based on the flag State principle or *de facto* because it exercises control over a person or territory.[264] The question whether a State acts extraterritorially and whether it has jurisdiction in the sense of human rights jurisdictional clauses, can ultimately only be answered with regard to a specific investigative measure that a given authority has taken.

The catalogue of fundamental rights stipulated in the Swiss Constitution is not explicitly limited to state action within the Swiss borders. Rather, Article 35(1) Swiss Constitution, which is included in the chapter on fundamental rights, stipulates, *inter alia*, that fundamental rights must be upheld throughout the legal system – and thus also in the realm of mutual legal assistance.[265] Furthermore, as per Article 35(2) Swiss Constitution, everyone who acts on behalf of the state is bound to respect the fundamental rights and must contribute to their implementation. The determining factor is thus whether an official acts on behalf of the State,[266] which he generally does when taking investigative measures (at home or abroad) in the context of criminal proceedings. The argument that Swiss officials carry the Swiss Constitution in their pockets when crossing the Swiss border seems also required by Article 5 Swiss Constitution on the rule of law, which namely stipulates that all activities of the state shall be based on and limited by law – without stating any exemption to that fundamental principle.

Under Swiss law, a general rule on the admissibility of evidence collected *abroad*, i.e. a rule providing criteria on when and under what conditions information collected abroad can be used in Swiss criminal investigations and proceedings in currently missing from Swiss law. Some prohibitions on the use of evidence obtained abroad in Swiss proceedings emanate directly from international human rights law, such as information obtained through torture. However, in many cases, international human rights law may not be violated by the use of a specific method or means of evidence collection, and the evidence was nevertheless collected in a manner incompatible with Swiss law. In the absence of a principled rule, whether the evidence is admissible in such cases is decided on a case-by-case basis.[267]

---

262 Anne Peters, Die Anwendbarkeit der EMRK in Zeiten komplexer Hoheitsgewalt und das Prinzip der Grundrechtstoleranz, Archiv des Völkerrechts 48/2010, pp. 1 and 7.

263 Art. 1 ECHR and Art. 2 para. 1 ICCPR.

264 For the ECHR, see, for example, Michael Duttwiler/Anna Petrig, Neue Aspekte der extraterritorialen Anwendbarkeit der EMRK, AJP 10/2009, pp. 1247–1260; on the ICCPR, see HRC, General Comment No. 31, para 10, UN Doc. CCPR/C/21/Rev.1/Add. 13 (26 May 2004).

265 Regina Kiener/Walter Kälin, Grundrechte, Bern 2007, p. 38.

266 Regina Kiener/Walter Kälin (see FN 265), pp. 40–41.

267 On cross-border evidence collection and the case-by-case approach, see Sabine Gless, Vortrag Strafrechtslehrertagung, Zürich 2013 (on file with authors).

G. Appendix: relevant rules of Swiss criminal law

1. The four cybercrimes

Art. 143 Swiss Criminal Code: Unauthorised obtaining of data

[1] Any person who for his own or for another's unlawful gain obtains for himself or another data that is stored or transmitted electronically or in some similar manner and which is not intended for him and has been specially secured to prevent his access is liable to a custodial sentence not exceeding five years or to a monetary penalty.

[2] The unauthorised obtaining of data to the detriment of a relative or family member is prosecuted only on complaint.

Art. 143bis Swiss Criminal Code: Unauthorised access to a data processing system

[1] Any person who obtains unauthorised access by means of data transmission equipment to a data processing system that has been specially secured to prevent his access is liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty.

[2] Any person who markets or makes accessible passwords, programs or other data that he knows or must assume are intended to be used to commit an offence under paragraph 1 is liable to a custodial sentence not exceeding three years or to a monetary penalty.

Art. 144bis Swiss Criminal Code: Damage to data

1. Any person who without authority alters, deletes or renders unusable data that is stored or transmitted electronically or in some other similar way is liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty.

If the offender has caused major damage, a custodial sentence of from one to five years may be imposed. The offence is prosecuted ex officio.

2. Any person who manufactures, imports, markets, advertises, offers or otherwise makes accessible programs that he knows or must assume will be used for the purposes described in paragraph 1 above, or provides instructions on the manufacture of such programs is liable to a custodial sentence not exceeding three years or to a monetary penalty.

If the offender acts for commercial gain, a custodial sentence of from one to five years may be imposed.

Art. 147 Swiss Criminal Code: Computer fraud

[1] Any person who with a view to his own or another's unlawful gain, by the incorrect, incomplete or unauthorised use of data, or in a similar way, influences the electronic or similar processing or transmission of data and as a result causes the transfer of financial assets, thus occasioning loss to another, or immediately thereafter conceals such a transfer is liable to a custodial sentence not exceeding five years or to a monetary penalty.

[2] If the offender acts for commercial gain, he is liable to a custodial sentence not exceeding ten years or to a monetary penalty of not less than 90 daily penalty units.

[3] Computer fraud to the detriment of a relative or family member is prosecuted only on complaint.

2. Rules on participation, criminal liability of media and corporations

a) Participation

Art. 24 Swiss Criminal Code: Incitement

[1] Any person who has wilfully incited another to commit a felony or a misdemeanour, provided the offence is committed, incurs the same penalty as applies to the person who has committed the offence.

[2] Any person who attempts to incite someone to commit a felony incurs the penalty applicable to an attempt to commit that felony.

Art. 25 Swiss Criminal Code: Complicity

Any person who wilfully assists another to commit a felony or a misdemeanour is liable to a reduced penalty.

b) Criminal liability of media

Art. 28 Swiss Criminal Code: Criminal liability of the media

[1] If an offence is committed and completed through publication in a medium, then, subject to the following provisions, only the author is liable to prosecution.

[2] If the author cannot be identified or if he cannot be brought to court in Switzerland, then the editor responsible in accordance with Article 322bis is liable to prosecution. If there is no responsible editor, then the person responsible for publication in accordance with Article 322bis is liable for prosecution.

[3] If the publication has taken place without the knowledge or against the will of the author, then the editor or, in his absence, the person responsible for publication is liable to prosecution as the offender.

[4] The accurate reporting of public talks and official communications from a public authority may not be made subject to prosecution.

Art. 322bis Swiss Criminal Code: Failure to prevent an illegal publication

Any person who, as the person responsible in terms of Article 28 paragraphs 2 and 3, wilfully fails to prevent the publication of material2, the publication of which constitutes an offence is liable to a custodial sentence not exceeding three years or to a monetary penalty. If the person concerned acts through negligence, the penalty is a fine.

c) Corporate criminal liability

Art. 102 Swiss Criminal Code: Liability under the criminal law

[1] If a felony or misdemeanour is committed in an undertaking in the exercise of commercial activities in accordance with the objects of the undertaking and if it is not possible to attribute this act to any specific natural person due to the inadequate organisation of the undertaking, then the felony or misdemeanour is attributed to the undertaking. In such cases, the undertaking is liable to a fine not exceeding 5 million francs.

[2] If the offence committed falls under Articles 260ter, 260^{quinquies}, 305bis, 322ter, 322^{quinquies} or 322^{septies} paragraph 1 or is an offence under Article 4a paragraph 1 letter a of the Federal Act of 19 Dec. 1986 on Unfair Competition, the undertaking is penalised irrespective of the criminal liability of any natural persons, provided the undertaking is responsible for failing to take all the reasonable organisational measures that were required in order to prevent such an offence.

[3] The court assesses the fine in particular in accordance with the seriousness of the offence, the seriousness of the organisational inadequacies and of the loss or damage caused, and based on the economic ability of the undertaking to pay the fine.

[4] Undertakings within the meaning of this title are:

a. any legal entity under private law;

b. any legal entity under public law with exception of local authorities;

c. companies;

d. sole proprietorships.

3. General jurisdictional rules of the Swiss Criminal Code

Art. 3 Swiss Criminal Code: Felonies or misdemeanours in Switzerland

[1] Any person who commits a felony or misdemeanour in Switzerland is subject to this Code.

[2] If the person concerned has served a sentence in full or in part for the offence in another country, the Swiss court must take the sentence served into account in determining the sentence to be imposed.

[3] If the person concerned has been prosecuted in a foreign country at the request of the Swiss authorities, then unless the offence involves a gross violation of the principles of the Federal Constitution or the Convention from 4 November 1950 for the protection of Human Rights and Fundamental Freedoms (ECHR), he is not prosecuted in Switzerland for the same offence if:

a. the foreign court has acquitted him and the judgment has taken full legal effect;

b. the penalty to which he had been sentenced in the foreign country has been served, suspended or has prescribed.

[4] If the person prosecuted abroad at the request of the Swiss authorities has not served the sentence or has only served it in part, the whole sentence or the remainder shall be served in Switzerland. The court decides whether a measure that has not been executed abroad or has only been served in part must be executed or continued in Switzerland.

Art. 4 Swiss Criminal Code: Felonies or misdemeanours against the state committed abroad

[1] This Code also applies to any person who commits a felony or misdemeanour against the state or its national security (Art. 265–278).

[2] If the person concerned has been convicted of the offence and has served the sentence in full or in part in another country, the court shall take the sentence served into account in determining the sentence to be imposed.

Art. 5 Swiss Criminal Code: Offences against minors abroad

[1] This Code also applies to any person who is in Switzerland, is not being extradited and has committed any of the following offences abroad:

a. trafficking in human beings (Art. 182), indecent assault (Art. 189), rape (Art. 190), sexual acts with a person incapable of proper judgment or resistance (Art. 191) or encouraging prostitution (Art. 195) if the victim was less than 18 years of age;

b. sexual acts with children (Art. 187) if the victim was less than 14 years of age;

c. aggravated pornography (Art. 197 no. 3) if the articles or representations depict sexual acts with children.

[2] Unless the offence involves a gross violation of the principles of the Federal Constitution and the ECHR, the person concerned is not liable to further prosecution in Switzerland for the offence if:

a. he has been acquitted of the offence abroad in a legally binding judgment;

b. the sentence that was imposed abroad has been served, waived, or has prescribed.

[3] If the person concerned has been convicted of the offence abroad and if the sentence imposed abroad has been partly served, the court shall take the part served into account in the sentence to be imposed. The court decides whether a measure ordered abroad but only partly executed there must be continued or taken into account in the sentence imposed in Switzerland.

Art. 6 Swiss Criminal Code: Offences committed abroad prosecuted in terms of an international obligation

[1] Any person who commits a felony or misdemeanour abroad that Switzerland is obliged to prosecute in terms of an international convention is subject to this Code provided:

a. the act is also liable to prosecution at the place of commission or no criminal law jurisdiction applies at the place of commission; and

b. the person concerned remains in Switzerland and is not extradited to the foreign country.

[2] The court determines the sentence so that overall the person concerned is not treated more severely than would have been the case under the law at the place of commission.

[3] Unless the offence involves a gross violation of the principles of the Federal Constitution and of the ECHR, the person concerned is not liable to further prosecution in Switzerland if:

a. he has been acquitted of the offence abroad in a legally binding judgment;

b. the sentence that was imposed abroad has been executed, waived, or has prescribed.

[4] If the person concerned has been convicted of the offence abroad and if the sentence imposed abroad has been partly served, the court shall take the part served into account in the sentence to be imposed. The court decides whether a measure ordered abroad but only partly executed there must be continued or taken into account in the sentence imposed in Switzerland.

Art. 7 Swiss Criminal Code: Other offences committed abroad

[1] Any person who commits a felony or misdemeanour abroad where the requirements of Articles 4, 5 or 6 are not fulfilled is subject to this Code if:

a. the offence is also liable to prosecution at the place of commission or the place of commission is not subject to criminal law jurisdiction;

b. the person concerned is in Switzerland or is extradited to Switzerland due to the offence; and

c. under Swiss law extradition is permitted for the offence, but the person concerned is not being extradited.

[2] If the person concerned is not Swiss and if the felony or misdemeanour was not committed against a Swiss person, paragraph 1 is applicable only if:

a. the request for extradition was refused for a reason unrelated to the nature of the offence; or

b. the offender has committed a particularly serious felony that is proscribed by the international community.

[3] The court shall determine the sentence so that overall the person concerned is not treated more severely than would have been the case under the law at the place of commission.

[4] Unless the offence involves a gross violation of the principles of the Federal Constitution and the ECHR, the person concerned is not liable to further prosecution in Switzerland for the offence if:

a. he has been acquitted of the offence abroad in a legally binding judgment;

b. the sentence that was imposed abroad has been served, waived, or has prescribed.

[5] If the person concerned has been convicted of the offence abroad and if the sentence imposed abroad has been partly served, the court shall take the part served into account in the sentence to be imposed. The court decides whether a measure ordered abroad but only partly executed there must be continued or taken into account in the sentence imposed in Switzerland.

Art. 8 Swiss Criminal Code: Place of commission

[1] A felony or misdemeanour is considered to be committed at the place where the person concerned commits it or unlawfully omits to act, and at the place where the offence has taken effect.

[2] An attempted offence is considered to be committed at the place where the person concerned attempted it and at the place where he intended the offence to take effect.

4. Relevant criminal procedural rules

a) Search of records and recordings

Art. 246 Criminal Procedure Code: Principle

Documents, audio, video and other recordings, data carriers and equipment for processing and storing information may be searched if it is suspected that they contain information that is liable to seizure.

Art. 247 Criminal Procedure Code: Conduct

[1] The proprietor may comment before a search on the content of records and recordings.

[2] Experts may be called in to examine the content of records and recordings, and in particular to identify records and recordings with protected content.

[3] The proprietor may provide the criminal justice authority with copies of records and recordings and printouts of stored information if this is sufficient for the purpose of the proceedings.

Art. 248 Criminal Procedure Code: Sealing of evidence

[1] Records and property that according to the proprietor may not be searched or seized due to the right to remain silent or to refuse to testify or for other reasons must be sealed and may neither be inspected nor used by the criminal justice authorities.

[2] Unless the criminal justice authority files a request for the removal of the seals within 20 days, the sealed records and property shall be returned to the proprietor.

[3] If it files a request for the removal of the seals, the following courts shall issue a final judgment thereon within a month:

a. in preliminary proceedings: the compulsory measures court;

b. in other cases: the court before which the case is pending.

[4] The court may call in an expert to examine the content of records and property.

b) Surveillance of post and telecommunications

Art. 269 Criminal Procedure Code: Requirements

[1] The public prosecutor may arrange for post and telecommunications to be monitored if:

a. there is a strong suspicion that an offence listed in paragraph 2 has been committed;

b. the seriousness of the offence justifies surveillance; and

c. investigative activities carried out so far have been unsuccessful or the enquiries would otherwise have no prospect of success or be made unreasonably complicated.

[2] Surveillance may be ordered in the investigation of the offences under the following Articles:

a. SCC: Articles 111–113, 115, 118 number 2, 122, 124, 127, 129, 135, 138–140, 143, 144 paragraph 3, 144bis number 1 paragraph 2 and number 2 paragraph 2, 146–148, 156, 157 number 2, 158 number 1 paragraph 3 and number 2, 160, 161, 163 number 1, 180–185, 187, 188 number 1, 189–191, 192 paragraph 1, 195, 197, 221 paragraphs 1 and 2, 223 number 1, 224 paragraph 1, 226, 227 number 1 paragraph 1, 228 number 1 paragraphs 1–4, 230bis, 231 number 1, 232 number 1, 233 number 1, 234 paragraph 1, 237 number 1, 238 paragraph 1, 240 paragraph 1, 242, 244, 251 number 1, 258, 259 paragraph 1, 260bis–260^{quinquies}, 261bis, 264–267, 271, 272 number 2, 273, 274 number 1 paragraph 2, 285, 301, 303 number 1, 305, 305bis number 2, 310, 312, 314, 317 number 1, 319, 322ter, 322^{quater} and 322^{septies};

b. Federal Act of 16 December 2005 on Foreign Nationals: Articles 116 paragraph 3 and 118 paragraph 3;

c. Federal Act of 22 June 2001 on the Hague Convention on Adoption and on Measures to Protect Children in International Adoption Cases: Article 24;

d. War Material Act of 13 December 1996: Articles 33 paragraph 2 and 34–35b;

e. Nuclear Energy Act of 21 March 2003: Articles 88 paragraphs 1 and 2, 89 paragraphs 1 and 2 and 90 paragraph 1;

f. Narcotics Act of 3 October 1951: Articles 19 number 1 second sentence and number 2, and 20 number 1 second sentence;

g. Environmental Protection Act of 7 October 1983: Article 60 paragraph 1 letters g–i as well as m and o;

h. Goods Control Act of 13 December 1996: Article 14 paragraph 2.

i. Sport Promotion Act of 17 June 2011: Article 22 paragraph 2.

[3] If the adjudication an offence subject to military jurisdiction is assigned to the jurisdiction of the civil courts, the surveillance of post and telecommunications may also be ordered in the investigation of the offences under Article 70 paragraph 2 of the Military Criminal Procedure Code of 23 March 1979.

Art. 270 Criminal Procedure Code: Subject matter of surveillance

The postal address and telecommunications connection of the following persons may be monitored:

a. the accused;

b. third parties if there is reason to believe based on specific information that:

1. the accused uses the postal address or the telecommunications connection of the third party, or

2. the third party receives certain communications on behalf of the accused or passes on communications from the accused to another person.

Art. 271 Criminal Procedure Code: Preservation of professional confidentiality

[1] When monitoring a person belonging to one of the professions mentioned in Articles 170– 173, the court must ensure that information that is relevant to the enquiries or the reason why this person is being monitored is separated from information that is relevant, in order to guarantee that no professional secrets come to the knowledge of the criminal justice authority.

[2] Direct interception of communications is permitted only if:

a. there is a strong suspicion that the person subject to professional confidentiality is guilty of an offence; and

b. there are specific reasons justifying the direct interception of communications.

[3] In the surveillance of other persons, information about which a person named in Articles 170–173 may refuse to testify must be removed from the case documents and destroyed immediately; it may not be used.

Art. 272 Criminal Procedure Code: Duty to obtain authorisation and general authorisation

[1] The surveillance of post and telecommunications requires the authorisation of the compulsory measures court.

[2] If enquiries reveal that the person under surveillance is changing his or her telecommunications connection regularly, the compulsory measures court may by way of exception authorise the surveillance of all identified connections used by the person under surveillance for telecommunications so that authorisation is not required in each individual case (general authorisation). The public prosecutor shall submit a report to the compulsory measures court for approval every month and on conclusion of the surveillance.

[3] If during the surveillance of a connection in terms of a general authorisation, measures are required to protect professional confidentiality and such measures are not mentioned in the general authorisation, an application for authorisation for the individual surveillance operation concerned must be submitted to the compulsory measures court.

Art. 273 Criminal Procedure Code: Traffic and invoice data, subscriber information

[1] If there is a strong suspicion that a felony or misdemeanour or a contravention in terms of Article 179septies SCC has been committed, and if the requirements of Article 269 paragraph 1 letters b and c are met, the public prosecutor may request information:

a. on when and with which persons or connections the person under surveillance is communicating or has communicated via post or telecommunications;

b. on traffic and invoice data.

[2] The order requires the approval of the compulsory measures court.

[3] The information mentioned in paragraph 1 may be requested irrespective of the duration of surveillance and for up to 6 months thereafter.

Art. 274 Criminal Procedure Code: Authorisation procedure

[1] The public prosecutor shall submit the following documents to the compulsory measures court within 24 hours of surveillance or the release of information being ordered:

a. the order;

b. a statement of the reasons and the case documents relevant for authorisation.

[2] The compulsory measures court shall decide and provide a brief statement of the reasons within 5 days of the surveillance or the release of information being ordered. It may grant authorisation subject to a time limit or other conditions, or request further information or investigations.

[3] The compulsory measures court shall give notice of the decision immediately to the public prosecutor and to the Post and Telecommunications Surveillance Bureau in terms of Article 2 of the Federal Act of 6 October 2000 on the Surveillance of Post and Telecommunications.

[4] The authorisation shall expressly state whether:

a. measures must be taken to protect professional confidentiality;

b. the direct interception of communications is permitted.

[5] The compulsory measures court shall grant authorisation for a maximum of 3 months. The authorisation may be extended on one or more occasions for a maximum of 3 months at a time. If an extension is required, the public prosecutor shall file an application for the extension, stating the reasons therefor, before expiry of the current authorisation.

Art. 275 Criminal Procedure Code: Conclusion of surveillance

[1] The public prosecutor shall stop surveillance immediately if:

a. the requirements are no longer fulfilled; or

b. the authorisation or its extension is refused.

[2] In cases under paragraph 1 letter a, the public prosecutor shall notify the compulsory measures court that surveillance has been concluded.

Art. 276 Criminal Procedure Code: Results not required

[1] Records of authorised surveillance operations that are not required for criminal proceedings shall be stored separately from the case documents and destroyed immediately on conclusion of the proceedings.

[2] Postal items may be retained for as long as this is necessary for the criminal proceedings; they must be released to the addressee as soon as the status of the proceedings permits.

Art. 277 Criminal Procedure Code: Use of the results of unauthorised surveillance operations

[1] Documents and data carriers obtained in unauthorised surveillance activities must be destroyed immediately. Postal items must be delivered to the addressee immediately.

[2] The results of unauthorised surveillance operations may not be used.

Art. 278 Criminal Procedure Code: Accidental finds

[1] If in the course of surveillance operations offences other than those specified in the surveillance order come to light, these findings may be used against the accused provided surveillance would have been permitted in the investigation of the offences concerned.

[1bis] If offences come to light during surveillance operations in terms of Article 3 of the Federal Act of 6 October 2000 on the Surveillance of Post and Telecommunications, the findings may be used subject to the requirements specified in paragraphs 2 and 3.

[2] Findings relating to offences committed by a person who is not named as a suspect in the surveillance order may be used if the requirements for the surveillance of this person are fulfilled.

[3] In cases under paragraphs 1, 1[bis] and 2, the public prosecutor shall order surveillance immediately and begin the authorisation procedure.

[4] Records that may not be used as accidental finds must be stored separately from the case documents and destroyed on conclusion of the proceedings.

[5] Any findings made in a surveillance operation may be used to trace wanted persons.

Art. 279 Criminal Procedure Code: Notice

[1] The public prosecutor shall notify the suspect under surveillance and third parties under surveillance in terms of Article 270 letter b of the reason for and form and duration of the surveillance operation on conclusion of the preliminary proceedings at the latest.

[2] With the consent of the compulsory measures court, notice may be deferred or dispensed with if:

a. the findings are not used as evidence in court proceedings; and

b. deferring or dispensing with notice is necessary to protect overriding public or private interests.

[3] Persons whose telecommunications connection or postal address has been under surveillance or who have used a connection or postal address that has been under surveillance may file an appeal under Articles 393–397. The period for filing the appeal begins on receipt of the notice.

c) Surveillance using technical surveillance devices

Art. 280 Criminal Procedure Code: Permitted use

The public prosecutor may use technical surveillance devices in order to:

a. listen to or record words spoken in private;

b. observe or record events in private or not generally accessible places;

c. establish the whereabouts of persons or property.

Art. 281 Criminal Procedure Code: Requirements and conduct

[1] Devices may only be used in relation to a suspect.

[2] Premises or vehicles of third parties may only be monitored if there is reason to believe on the basis of specific information that a suspect is present on those premises or using that vehicle.

[3] Use of devices may not be ordered in order to:

a. record as evidence in court proceedings events involving an accused who is in custody;

b. monitor premises or vehicles of a third party who belongs to one of the professions mentioned in Articles 170–173.

[4] The use of technical surveillance devices is otherwise governed by Articles 269–279.

d) Observation

Art. 282 Criminal Procedure Code: Requirements

[1] The public prosecutor and, in the enquiries, the police may covertly observe persons and property in generally accessible locations and make image or sound recordings while doing so if:

a. there is reason to believe on the basis of specific information that felonies or misdemeanours have been committed; and

b. the enquiries would otherwise have no prospect of success or be made unreasonably complicated.

[2] Where observation activities ordered by the police have been conducted for one month, their continuation requires authorisation by the public prosecutor.

Art. 283 Criminal Procedure Code: Notice

[1] The public prosecutor shall notify the persons directly concerned by observation activities of the reason for and form and duration of the observation activities on conclusion of the preliminary proceedings at the latest.

[2] Notice may be deferred or dispensed with if:

a. the findings are not used as evidence in court proceedings; and

b. deferring or dispensing with notice is necessary to protect overriding public or private interests.

5. Rules on mutual legal assistance

Art. 18a Mutual Assistance Act (IMAC): Surveillance of postal and telecommunications traffic

[1] In extradition cases, the Federal Office may, at the express request of another State order the surveillance of postal and telecommunications traffic in order to establish the whereabouts of the defendant.

[2] In other mutual assistance cases, the following authorities may order the surveillance of postal and telecommunications traffic:

a. the Office of the Attorney General of Switzerland or of the Cantonal Public Prosecutor;

b. the Federal Office, if it is executing the request for mutual assistance itself.

[3] The surveillance order must be submitted to the following authorities for approval:

a. by the federal authorities: the federal compulsory measures court;

b. by the cantonal authorities: the cantonal compulsory measures court.

[4] The requirements for surveillance and the procedure shall otherwise be governed by Articles 269–279 CrimPC and the Federal Act of 6 October 2000 on the Surveillance of Postal and Telecommunications Traffic.

Art. 18b Mutual Assistance Act: Electronic communications traffic data

[1] The federal or cantonal authority dealing with a request for mutual assistance may order the transmission of electronic communications traffic data to another State before conclusion of the mutual assistance proceedings if:

a. provisional measures indicate that the communication that is the subject of the request originated abroad; or

b. the data was acquired by the executing authority based on an order for authorised real-time surveillance (Art. 269–281 of the CrimPC).

[2] The data may not be used in evidence before the ruling on granting and the extent of mutual assistance is legally binding.

[3] Notice of the ruling under paragraph 1 and any order or authorisation for surveillance must be given to the Federal Office immediately.

Art. 64 Mutual Assistance Act: Compulsory measures

[1] Measures under Article 63 which require the use of procedural compulsion may be ordered only if the description of the circumstances of the case indicates that the offence being prosecuted abroad contains the objective elements of an offence under Swiss law. The measures must be carried out in accordance with Swiss law.

[2] If the offence prosecuted abroad is not an offence in Switzerland, measures under Article 63 which require the use of procedural compulsion shall be allowed for:

a. the exoneration of a defendant;

b. the prosecution of offences involving sexual acts with minors.