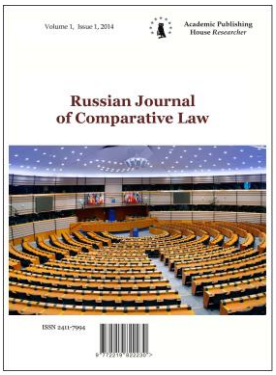

Published in the Russian Federation
Russian Journal of Comparative Law
Has been issued since 2014.
ISSN 2411-7994
E-ISSN 2413-7618
Vol. 9, Is. 3, pp. 74-83, 2016

DOI: 10.13187/rjcl.2016.9.74
http://ejournal41.com

UDC 343.241

Covert Post and Telecommunications Surveillance in Swiss Criminal Proceedings

Andreas Donatsch [a, *], Mischa Demarmels [a]

[a] University of Zurich, School of Law, Switzerland

Abstract

This article discusses the covert surveillance of post and telecommunications as a coercive measure in Swiss criminal proceedings. Since such surveillance interferes with a number of fundamental rights and freedoms, it should meet the requirements of human rights limitations. Firstly, the offence must constitute a so-called "catalogue offence" under Art. 269 para. 2 of the Swiss Code of Criminal Procedure. Further, there must be a strong evidence to suspect that such a catalogue offence has been committed in reality. In addition, the seriousness of the offence must justify the surveillance. Finally, previously undertaken investigative activities must have proven to be unsuccessful, or there are grounds to suspect that in absence of such surveillance the investigation will not succeed or will likely become disproportionately more complicated.

Against this background, the authors analyze the latest amendments to the Federal Statute on the Surveillance of Post and Telecommunications (the BÜPF) and their impact on the conduct of criminal proceedings.

Keywords: Switzerland, Code of Criminal Procedure, criminal proceedings, coercive measures, covert post and telecommunications surveillance, surveillance and production of metadata, IMSI-Catcher, revision of the Federal statute on the Surveillance of Post and Telecommunications (the BÜPF), Government-Software (the GovWare), requirements governing the use of the GovWare.

1. Introduction

Coercive measures are set out as an exhaustive inventory in Art. 196 ff. of the Swiss Code of Criminal Procedure (hereinafter - the CCP). Several types of such measures are stipulate by the CPP which can be used autonomously or can be combined. Coercive measures under the CCP should serve the goal of securing the evidence and ensuring the presence of a person during the proceedings. Such measures represent a set of procedural activities undertaken by criminal justice authorities which interfere with fundamental rights of the persons concerned. The term "fundamental rights" for the purposes of our present discussion includes not only rights set up by the Federal Constitution, but also those human rights which are protected by international human rights treaties [1, Art. 196, N 2]. Most often, coercive measures encroached on the right to personal liberty and security (Art. 5 of the European Convention on Human Rights), the right to respect for

* Corresponding author
E-mail addresses: lst.donatsch@rwi.uzh.ch (A. Donatsch); mischa.demarmels@rwi.uzh.ch (M. Demarmels)

private and family life (Art. 8 of the European Convention on Human Rights), and the right to property (Art. 1 of the Protocol No. 1 to the European Convention on Human Rights). The European convention on Human Rights entered into force for Switzerland on 28 November 1974. Yet Switzerland signed but not as yet ratified the Protocol No. 1 to the European Convention on Human Rights.

There is a considerable number of coercive measures, stipulated for by the CCP. These measures include: obligating a person to attend court or administrative hearing, detention on remand, search, and seizure. There are also provisions on covert surveillance which include: the surveillance of post and telecommunications, the surveillance of technical monitoring devices, observation, as well as the surveillance of banking transactions and undercover investigations. Post and telecommunications surveillance is among the most frequently employed coercive measures in Switzerland.

2. Materials and methods

This article explores the procedure and human rights compliance of covert surveillance of post and telecommunications as a coercive measure. The principal sources are academic writings, decisions of the Federal Court, and the official documents of the Swiss Government. The review is based on analytical legal assessment and utilizes general methodologies of legal research.

3. Discussion

I. The Surveillance of Post and Telecommunications

The covert surveillance of post and telecommunications was implemented in 2015 on a total of 9650 occasions. 3381 of the said cases constituted real time surveillance, and 6269 involved retrospective surveillance (retrospective production of traffic data and billing information – so-called metadata) [2]. Various requirements for the *corpus delicti* of a criminal offence under investigation and for the subject of surveillance must be met in order for the surveillance to be authorised by the court as a coercive measure. In addition, the procedure must be clearly set out in law regulating the surveillance process from the point at which the surveillance is authorised to the point of concluding the outcomes of surveillance accompanied by obligations to provide information about the surveillance.

A. Requirements concerning Communications

The authorities are permitted to monitor the contents of post and telecommunications only when four cumulative requirements are fulfilled. Firstly, a crime must constitute a so-called catalogue offence under Art. 269 para. 2 of the CCP. Further, there must be strong evidence to suspect that such an offence has been committed in reality. In addition, the seriousness of the offence must justify the surveillance. Finally, previously undertaken investigative activities must have proven to be unsuccessful, or there are grounds to suspect that in absence of such surveillance the investigation will not succeed or will likely become disproportionately more complicated.

1. Catalogue Offence under Art. 269 para. 2 of the CCP

Art. 269 para. 2 of the CCP stipulates an exhaustive inventory or catalogue of offences. Surveillance can only be imposed in respect of the prosecution of one of the criminal offences set out in the catalogue [3] (e.g. homicide, theft, robbery, fraud, rape etc.) and the judge is not entitled to expand this inventory [4, Art. 269 N 28]. This ensures clarity with regards to those cases where surveillance is permissible yet it allows certain problems [5]. On the one hand, the choice of offences in the said catalogue can be somewhat haphazard [6, N 1184]. On the other hand, situations are possible when surveillance would also be proportionate in respect of less serious offences. In addition, the existence of a catalogue of offences could lead to a tendency to authorize the surveillance in respect of all offences set out in the catalogue, irrespectively of the specific circumstances of a certain case [6, N 1184].

2. Strong Suspicion

When it comes to catalogue offences, the existence of a reasonable suspicion that a crime has been committed is not *per se* sufficient to allow surveillance, rather it is essential that there is strong suspicion in the sense of Art. 197 para. 1 b) CCP (Art. 269 para. 1 a) of the CCP).

There several degrees of suspicion which are difficult to differentiate from each other [7]. According to the Federal Court, strong suspicion that a criminal offence has been committed is established when concrete indications exist «according to which the incriminating behaviour is substantially likely to meet the definition of the criminal offence in question» [8].

3. Proportionality

In addition to the requirement that there should be a strong suspicion that a catalogue offence has been committed, it is necessary that the surveillance can be justified by the seriousness of the criminal offence in question. This requirement serves as a guarantee of proportionality of surveillance. Determining the proportionality of surveillance, the authorities should take several factors into consideration. It is essential to consider the seriousness of the offence, but it is also necessary to give due to the extent of suspicion, and the significance of interference with the rights of the persons concerned [4, Art. 269 N 23; 6, N 1186]. Finally, the likelihood of success of coercive measure should be taken into consideration in balancing the issue of proportionality of the surveillance [4, Art. 269 N 23].

4. Subsidiarity

It is significant to respect the principle of subsidiarity in the procedure of post and telecommunications surveillance. This implies that previously undertaken investigative activities should have been proven to be unsuccessful or that an investigation without surveillance would have no reasonable chance to succeed or would become disproportionately more complicated [9]. The subsidiarity test is usually easy to meet yet it can't undermine its significance for human rights protection [10; 6, N 1187].

B. Subject of Post and Telecommunications Surveillance

The subject of surveillance is defined in Art. 270 of the CCP. It is important to distinguish between the functional subject of surveillance and the group of people which can be put under surveillance.

From a functional perspective, postal addresses and telecommunication connections can be subject to surveillance. The surveillance of postal addresses includes information about the receipt as well as the dispatch of the post, the possibility to control the contents of post, and to copy or even substitute the contents of the post in certain cases [11]. In addition, post communications can be held back, providing that this is permissible under the provisions on temporary confiscation [4, Art. 270 N 2]. The surveillance of telecommunication connections includes all telecommunications falling under the scope of the Telecommunications Act (the TCA) [12]. It includes, in addition to telephone communications, also fax, pager, mobile telephone communications, as well as data and internet communications. The latter includes not merely e-mail communications but also all activities on the internet [13].

When it comes to concrete persons who can be put under surveillance, the post and communications connections of the accused person (Art. 270 a) of the CCP) and third parties (Art. 270 b) pf the CCP) can be subject to surveillance. The surveillance of the third parties can only be imposed in two categories of cases: either, there must be indications suggesting that the accused person is using the postal address or telecommunication connections of the third party [14]; or, there must be a suspicion that the third party remains in communication with the accused person. In such cases, it is necessary that there is a suspicion that somebody is receiving messages on behalf of the accused or conveys such messages from the accused person to others.

In decision of 6 November 2012 the Federal Court extended the scope of the term 'usage' of communication connections by proclaiming that the surveillance of telecommunication connections of a third party is permissible when it is very likely that this connection is being used to contact the accused person [15].

There are restrictions concerning surveillance of those persons who are bound by a duty of professional confidentiality under Art. 170-173 of the CCP (See Art. 271 of the CCP). In such cases a triage must be undertaken in order to set apart information which does not pertain to the investigation or which relates to the rules of confidentiality [16]. According to the revised version of Art. 270 of the CCP, such information must be destroyed and cannot be used in criminal

proceedings, unless there is a strong suspicion that the person bound by the duty of confidentiality has committed a crime, and that particular grounds exist which justify such an exception [17].

C. Imposing and Ending the Telecommunications Surveillance

The surveillance of post and telecommunications can only be imposed by the prosecution authorities. While the order imposing the surveillance must generally be made in written form, in exceptional cases it can be imposed orally [18]. The information will be handed over, however, only once there is a written confirmation of the order [19; 4, Art. 269 N 44]. The surveillance order is passed to the «office of post and telecommunications surveillance» at the IT service centre of the Federal Justice and Police Department (ÜPF ISC-EJPD). This department conveys the request to the relevant telecommunications provider.

Finally, the prosecution authorities must convey their requests to the court of law for authorisation of coercive measures. Within 24 hours since the imposition of the order, the authorities should submit their reasoning and any relevant files to the court for deciding on implementing the coercive measures (See Art. 274 para. 1 of the CCP). Dealing with these documents, the court can authorise the surveillance for a period of up to three months (See Art. 274 para. 5 CCP). On the request of the prosecution, this authorisation can be renewed in every individual case for a period of up to three months (See Art. 274 para. 5 of the CCP). The prosecution must stop the surveillance without delay when the requirements for it are no longer fulfilled or if the court refuses to authorise or renew the authorisation of this coercive measure. If the surveillance is concluded on the initiative of the prosecution, this must be communicated to the court deciding on coercive measures (See Art. 275 para. 2 of the CCP). The surveillance is concluded on the basis of the order from the prosecution which is subsequently confirmed by the relevant public authority [20].

The person subjected to surveillance should, as a general rule, be informed on the finalizing of pre-trial procedure at the latest regarding the fact that he or she had been a subject of surveillance. The person whose telecommunications or postal address was under surveillance has the right to appeal against it within a period of 10 days from the day when he or she received such information, under Art. 393 ff. of the CCP (See Art. 279 of the CCP).

D. Surveillance and the Production of Metadata

The surveillance and the production of traffic and billing data (so-called metadata), as well as user identification data is regulated in Art. 273 of the CCP. Not merely the contents of post or telecommunications can be subject to surveillance. More general information is also subject to surveillance, such as e.g., information about who had contacted whom, when, and where, etc. The requirements for the procedure of gathering such data are less strict. There is no requirement that the crime would be a catalogue offence under Art. 269 para. 2 of the CCP. It is sufficient that there is a strong suspicion that a crime or offence or a misdemeanour in the sense of Art. 179^{septies} CC has been committed. In addition, the principles of proportionality (See above II.A.3) and subsidiarity (See above II.A.4) must also be respected. Finally, the order that metadata should be produced must be authorised by the court deciding on coercive measures (Art. 273 para. 2 of the CCP). Metadata must be retained by post and telecommunication providers for a period of six months (Art. 12 para. 2, Art. 15 para. 3 of the BÜPF, Art. 273 para. 3 of the CCP).

II. Recent Legislative Amendments

The revision of the Federal Statute on the Surveillance of Post and Telecommunications (the BÜPF) resulted in amending the provisions regarding surveillance in the CCP [21]. These amendments provide for new types of surveillances measures to be employed, these provisions are extended *ratione personae,* and new changes regard the allocation of surveillance costs. Originally, it was proposed that the data retention period would be extended from six to 12 months [22 p. 2781]. This proposal was subject, however, to considerable criticism in the Parliament which led after consultations to the compromise of reducing this period to six months [23].

A. New Technical Measures

The said legal amendments led to the adoption of two new statutory provisions incorporated into the CCP. These provisions regulate the covert surveillance of telecommunications by means of special technical equipment (Art. 269bis of the ED-CCP) and IT programmes (Art. 269ter of the ED-CCP). This expansion is a reaction of the legislative authorities to the new means of communication which assist criminals in avoiding the situations of being subject to surveillance. New technical measures are designed to address such loopholes.

1. Use of Special Technical Equipment

The introduction of Art. 269bis in the ED-CCP allowed, in particular, to set up a legal basis for the extended use of the IMSI-Catchers [22 p. 2701, 2769; 4 Art. 269bis N 1]. This legal provision was intentionally broadly defined, in order to provide the authorities with opportunities to react on changes in telecommunication technologies and, if necessary, to use newly developed equipment for surveillance [4 Art. 269bis N 1]. The prosecution authorities are obligated, in accordance with Art. 269bis para. 2 of the CCP, to maintain statistical data on the use of surveillance. This obligation was introduced during consultations in the Parliament.

a) IMSI-Catcher

The IMSI-Catcher is a mobile device which simulates the functions of a mobile communications antenna [24, p. 281; 22, p. 2769]. Mobile devices in the vicinity of the IMSI-Catcher communicate with it and are then connected by the Catcher to the next available mobile communications antenna. This enables the IMSI-Catcher, without the user of a mobile device being aware of, to intercept the traffic data. This allows the telephone number, the IMEI (International Mobile Station Equipment Identity) of the device and the IMSI (International Mobile Subscriber Identity) of the device's SIM card to be logged [4, Art. 269bis N 2]. In addition, it allows to locate the position of the device within the network. The intention of the legislative authorities is to extend those measures, which are already employed, by means of Art. 269$^{bis\ of\ the}$ ED-CCP by creating a legal basis for using IMSI-Catchers for intercepting other data, and enabling monitoring telephone conversations and data which is sent and received [22, p. 2769]. The (restricted) use of IMSI-Catchers is currently based on Art. 280 of the CCP [22, p. 2769].

b) Requirements

In order that special technical equipment may be used for the purposes of the surveillance of telecommunications, the following cumulative requirements must be fulfilled: According to Art. 269bis a) of the ED-CCP, the requirements as set out in Art. 269 of the CCP regulating the surveillance of post and telecommunications must be met. Any measures concerning surveillance of telecommunications under Art. 269 of the CCP which had previously been undertaken must have been unsuccessful or surveillance conducted using such measures must have been deemed not to have a reasonable chance to succeed, or would likely to have become disproportionately more complicated (para. b). This type of surveillance is to be considered as subsidiary with respect to current surveillance possibilities [22, p. 2770]. An example of a case where such subsidiary measures can be employed is when, e.g., the IMEI or the IMSI is unknown and the telecommunication provider is unable for technical reasons to provide the requested data and, hence, surveillance by usual means is not possible [4, Art. 269bis N 9]. Finally, the equipment must be authorised for use by the Bundesamt für Kommunikation (the BAKOM) (para. c). The authorisation should be provided with respect of a specific user for a specific number of requisite pieces of equipment. This requirement is designed to prevent interference with normal telecommunications through the use of the equipment [22, p. 2771]. During the authorisation proceedings, the authority is also required to examine whether the equipment is sufficiently protected against the threat of manipulation [4, Art. 269bis N 10].

2. Use of Particular IT Programmes

In addition to the use of special technical equipment, the introduction Art. 269ter of the CCP is designed to enable the employment of special IT programmes. This is necessary in order to respond to technical developments in communications technology and to fill in the *lacunae* preventing the effective crime investigation [22, p. 2775]. In particular, the use of IT programmes is intended to deal with the problems resulting from the increased use of encrypted communications (Viber, Whatsapp) by the means of enabling surveillance through Government software

(the GovWare). In such cases, surveillance is not possible through the usual means. The reason for this is that the relevant programmes encrypt the data directly on the individual devices and send it in separate data packages to the receiving device. This means that the relevant provider is unable to intercept all the data or to decrypt the data which it has intercepted [25, Rz 2].

a) Government-Software (the GovWare)

The GovWare is an IT programme which is installed on the relevant electronic device (computer, laptop, smartphone, etc.) in order to carry out the programmed activities. These consist, in particular, of circumventing the encryption of data by ensuring that the encrypted communication is intercepted after it had been decrypted by the receiving device and forwarded to the investigating authority [25, Rz 5].

The IT programmes are also able to activate microphones or cameras on the infiltrated devices, and to pass on sounds or video recordings to the investigating authority, as well as to covertly search the devices for data. The use of the GovWare for such purposes is not permitted by Art. 269ter para. 1 of the ED-CCP [24, p. 280]. This means that any data collected must be immediately destroyed and cannot be used in criminal proceedings (See Art. 269ter para. 3 of the ED-CCP).

The installation of the GovWare on the device under investigation can take place by various means. Firstly, the IT programme can be installed online – for instance by way of the e-mail. Secondly, criminal prosecution authorities can secure physical access to the relevant device and directly install the software. Finally, the user of the device might be induced to connect the device to a system which is already infiltrated by the GovWare [26].

b) Requirements Regarding IT Programmes

The GovWare must meet a number of requirements, in order for it to be utilised by criminal prosecution authorities. From a practical perspective, it is necessary that such surveillance can't be discovered by a person under surveillance or by the anti-virus software installed on his or her device. Furthermore, it is necessary that the software can be quickly installed and deleted, if necessary, without the device being physically accessed. Finally, the software must be specially programmed for each deployment and adapted to meet the specific requirements in the case at issue [4, Art. 269ter N 5]. From a statutory perspective, Art. 269^{quater} of the ED-CCP requires that a complete and unalterable protocol of surveillance by way of the IT programme should be maintained; this protocol forms part of file data in criminal investigation (para. 1). In addition, the extraction from the data processing system under surveillance to the requisite criminal prosecution authority must take place in a secure manner (para. 2). Finally, the software designers are obligated to provide criminal prosecution authorities with the respective source codes in order to allow examination of the program function of the GovWare (para. 3).

c) Requirements Governing the Use of the GovWare

The GovWare can only be used if the requirements, set out in Art. 269 paras. 1 and 3 of the CCP are met (Art. 269ter para. 1 a) of the ED-CCP). This means that there must be a strong suspicion that a crime has been committed, and the principles of proportionality and subsidiarity must be respected (See above II.A.4).

The prosecution authorities must suspect one of the criminal offences set out in Art. 286 para. 2 of the CCP (para. b). The legislator, therefore, relies on a more restrictive catalogue of offences applicable in the context of undercover investigations rather than the catalogue, set out in the context of conventional surveillance in the sense of Art. 269 para. 2 of the CCP. This was intended to reflect the seriousness of the interference with the rights of the person concerned [22, p. 2777 ff.]. This aim is generally to be commenced. Nevertheless, it is questionable whether in the context of undercover investigations references to the catalogue offences is a correct means of achieving this goal. This catalogue of offences was expressly created to serve the purposes of undercover investigations. Surveillance by means of the GovWare dos not have much in common with undercover investigations. This software is used to monitor a variety of means of communication. This is, with the exception of encrypted communications delivered by way of, e.g., Viber, already possible by way of conventional means of surveillance under Art. 269 of the CCP. Consequently, it would have been preferable to refer to the catalogue of offences in Art. 269 para. 2 of the CCP, to afforded greater effort for examination of proportionality of the measure [4, Art. 269ter N 5; 25, Rz. 25; 22, p. 2777 ff.].

Furthermore, "double subsidiarity" is required so that to ensure that any telecommunication surveillance measures previously undertaken under Art. 269 of the CCP must have been proven unsuccessful, or must have been unlikely to succeed, or would have disproportionately complicated the investigation (para. c).

The surveillance is prescribed on the basis of the so-called surveillance order. In the context of the use of the GovWare such order should specify both, the usual elements relating to the subject of the order, and the types of data which is sought. Finally, the rules must be determined with regards to non-public places which can be infiltrated, in order for the GovWare to be installed.

B. Extension of the Law Ratione Personae

The amendments to the BÜPF have led to the law being specified more clearly and extended *ratione personae*. This is currently regulated in Art. 1 para. 2 of the BÜPF. This legal provision refers to state or licenced providers, or those providers subject to reporting obligations of post and telecommunication services, and internet providers. In the future the group of person's subject to the BÜPF (those under obligation to cooperate with authorities) is clearly defined and, depending on their respective activities, divided into six categories. Different obligations apply to various categories (See Art. 19 ff. of the BÜPF). For instance, a company can fall within several categories. Art. 2 of the BÜPF divides the groups of persons under obligation to cooperate into the following categories [27]:

- Providers of post services in the sense of the PG [28] (para. a);
- Providers of telecommunication services, in accordance with Art. 3 b) of the Telecommunications Act of 30 April 19975 (the TCA, SR 784.10) (para. b);
- Providers of services, which reply on telecommunications services and which enable one-way or multi-way communications (providers of derivative communications services) (para. c);
- Operators of internal communications networks (para. d);
- Persons which make their access to a public telecommunications network available to third parties (para. e);
- Professional resellers of cards and similar means of enabling access to a public telecommunications network (para. f).

These extensions of the law *ratione personae* enable filling in the existing lacunae in law. It means that all persons are covered by the recent legal amendments who are active in post and telecommunications, and who have access to data which could be of interest to criminal investigation [22, p. 2706; 24, p. 283].

C. Retention of Metadata

Initially the revision of the law intended also to the extend the data retention period from six months to 12 months, with the aim of optimizing the activities of criminal prosecution authorities. In some cases, the six-month deadline had expired before the criminal prosecution authorities were able to request the production of meta data [22, p. 2708; 24, p. 287]. Considerable opposition to this extension in the Parliament meant that ultimately the data retention period was not extended [29]. The criticism related, in particular, to the concerns about serious interferences with the rights of the person concerned and about the costs, associated with doubling the data retention period for post and telecommunication providers.

In addition to the data retention period, there was a considerable and surprisingly intense discussion during the parliamentary debates about the storage location of the retained metadata [30]. The National Assembly, in its capacity as the second chamber of the Parliament, introduced a new paragraph, para. 5^{bis} of Art. 26 into the BÜPF. This was designed to obligate the telecommunication providers to store the metadata on the Swiss territory. Art. 26 para. 5^{bis} of the BÜPF was ultimately deleted following the request of the conciliation committee [31]. This means that there is no requirement that metadata should be stored only in Switzerland.

D. Surveillance Costs

The surveillance of post and telecommunications gives rise to a variety of costs. The providers who are under a duty to cooperate with public authorities are required, on the one hand, to create and maintain the necessary facilities. On the other hand, they also incur costs in the context of specific surveillance activities, in particular through staff expenditure. Currently the providers are obligated to cover these costs themselves. They do however receive appropriate compensation, which serves to cover some of the costs. Initially, it was intended that this remuneration should be later abolished. Following the cost analysis reports, however, the decision was made to abolish this proposal and maintain the current system. Consequently, criminal prosecution authorities imposing the surveillance measures will still be obligated to pay a global fee, which encompasses a fee for the «office of post and communications surveillance» and appropriate compensation for the services of the provider under the duty to cooperate. The authorities are required to pass on the compensation to the individual providers [See Art. 38 of the ED-BÜPF; 22, p. 2758 ff.; 24, p. 290].

The decision to retain the granting of appropriate compensation appears justified. It represents an appropriate compromise between the state's obligation to pay for the surveillance as a result of its monopoly on prosecution for crimes, and the general obligation to cooperate in the context of the investigation. The fact that the compensation does not cover the provider's costs can be justified with references to the fact that experts and witnesses are also (only) entitled to appropriate compensation. Furthermore, the banks, the insurance companies, or the trustees, etc., are also required in the context of legal orders to produce information and to cover the costs associated with the production of the data [32]. Finally, the providers pursue their activities in a high risk field where they are able to make profits and are obligated to carry out business risks [33].

4. Results

If the prosecution authorities impose the surveillance of post and telecommunications it is essential that the fundamental rights of the person affected are respected, and the coercive measures can be justified by the seriousness of the crime in question in order to guarantee the proportionality requirement.

5. Conclusion

The amendments to the BÜPF succeeded to provide criminal prosecution authorities with the urgently required means to react to developments in technologies, and, consequently, in the means of communication. The outlined legal amendments have largely addressed the lacunae having existed in the area of effective criminal investigation. At the same time, the rights and freedoms of those persons concerned have been guaranteed to the largest extent possible. All the process of surveillance is regulated by statutory law and the persons are entitled with the right to appeal against the surveillance measures. The procedure for imposing the surveillance is clearly regulated and it sets out various protective measures in order to protect the persons involved in it from disproportionate interference with their rights.

References

1. Markus Hug, Alexandra Scheidegger in: Andreas Donatsch, Thomas Hansjakob, Viktor Lieber (Hrsg.), Kommentar zur Schweizerischen Strafprozessordnung (StPO), 2nd ed., Zürich/Basel/Genf 2013.

2. https://www.li.admin.ch/de/themen/statistik (last visited on October 3, 2016).

3. See Art. 269 para. 2 of the CCP // https://www.admin.ch/opc/de/classified-compilation/20052319/index.html#a269 (last visited on October 3, 2016).

4. Thomas Hansjakob, in: Andreas Donatsch/Thomas Hansjakob/Viktor Lieber (Hrsg.), Kommentar zur Schweizerischen Strafprozessordnung (StPO), 2nd ed., Zürich/Basel/Genf 2013.

5. See for detailed consideration of the dangers Hansjakob, [4], Art. 269 N 28 ff.; for criticism Marc Jean-Richard-dit-Bressel, in: Marcel Alexander Niggli/Marianne Heer/Hans Wiprächtiger (Hrsg.), Basler Kommentar, Schweizerische Strafprozessordnung, Jugendstrafprozessordnung, Art. 196-457 StPO, 2nd ed., Basel 2014, Art. 269 N 59 ff.

6. Niklaus Oberholzer, Grundzüge des Strafprozessrechts, 3rd ed., Bern 2012, N 1184.

7. See further Hug/Scheidegger, [1], Art. 197 N 12; Jean-Richard-dit-Bressel, [5], Art. 269 N 34 ff.

8. BGE 137 IV 126 Erw. 3.2; BGer vom 26. Juli 2013, 1B_230/2013, Erw. 5.1.1.

9. See in this regard Hansjakob, [4], Art. 269 N 24 ff.

10. BGer vom 22. Juni 2011, 1B_425/2010, Erw. 3.3; Jean-Richard-dit-Bressel, [5], Art. 269 N 41; Niklaus Schmid, Handbuch des schweizerischen Strafprozessrechts, 2nd ed., Zürich/St.Gallen, 2013, N 1141 FN 478.

11. See in this regard Hansjakob, [4], Art. 270 N 2, who argues that it is not permissible to alter the content.

12. SR 784.10, Telecommunications Act (TCA) of April 30, 1997.

13. See in detail on this point: Hansjakob, [4], Art. 270 N 3.

14. Following the revision of the BÜPF this was renamed the telecommunications service, see: Entwurf BÜPF, BBl 2016, 2013.

15. See in detail: BGE 138 IV 232 Erw. 2 ff.

16. Schmid, [10], N 1146.

17. See: Entwurf BÜPF, BBl 2016, 2013; Botschaft BÜPF, 2780.

18. It is not necessary to provide reasons as the telecommunications provider has no right or obligation to examine the issue, see: BGE 130 II 249; Hansjakob, [4], Art. 269 N 45.

19. Andreas Donatsch/Christian Schwarzenegger/Wolfgang Wohlers, Strafprozessrecht, 2nd ed., Zürich/Basel/Genf 2014, § 8.14.

20. Hansjakob, [4], Art. 275 N 10 ff. If the prosecution does not issue a request that the surveillance be extended, the relevant office may cease the surveillance of its own initiative (Art. 1 para. 1 letter d, Art. 13 para. 1 letter g BÜPF); Schmid, [10], N 1152.

21. The deadline for a referendum to be called expired on July 7, 2016.

22. Botschaft BÜPF.

23. See: the Schlussabstimmungstext des Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 18. März 2016, BBl 2016 1991, 2014.

24. Emanuel Jaggi, Die Revision des BÜPF // ZStrR, 133/2015.

25. Thomas Hansjakob, Der Einsatz von GovWare in der Schweiz // Jusletter IT vom 15. Mai 2014.

26. See in this regard: Hansjakob, [4], Art. 269ter N 18.

27. For further details concerning the individual categories see: Botschaft BÜPF, 2706 ff.

28. SR 783.0, Postgesetz (PG) of December 17, 2010.

29. See the debate of the National Council and the Council of States: https://www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=29476 (last visited on October 3, 2016).

30. AB 2015 N 1165.

31. AB 2016 N 450 ff.

32. According to the Botschaft it is not legitimate to compare a request for the disclosure of documents with surveillance, as in the event of refusal to comply with the disclosure order, it is possible that a search warrant and a confiscation order are issued, which is not possible in the context of surveillance.

33. Jaggi, [24], 291 with further references.

UDC 343.241

Скрытое наблюдение за почтовой корреспонденцией и телекоммуникационным сообщением в уголовном процессе Швейцарии

Андреас Донач [a, *], Миша Демармелс [a]

[a] Университет Цюриха, Швейцария

Аннотация. Эта статья посвящена проблемам тайного наблюдения за почтовым сообщением и телекоммуникациями в качестве принудительной меры в уголовном процессе Швейцарии. Поскольку указанные действия затрагивают основные права человека, они допустимы лишь при соблюдении четырех требований. Во-первых, преступление должно быть "преступлением, включенным в каталог," согласно ст. 269 УПК Швейцарии. Во-вторых, у следствия должны быть "обоснованные подозрения", что деяние было совершено в действительности. В-третьих, тяжесть деяния должна соответствовать объему применяемой меры. В-четвертых, либо ранее предпринятые следственные действия оказались безуспешными, либо есть основания полагать, что неприменение такой меры приведет к "невозможности расследования или сделает расследование намного более сложным".

Авторы анализируют законодательство и правила уголовного судопроизводства Швейцарии. Подробно исследована процедура применения указанной принудительной меры. Авторы изучают процедуру тайной проверки сообщений и телекоммуникаций, характеризуют предмет и правила хранения метаданных.

Ключевые слова: Швейцария, УПК Швейцарии, уголовное судопроизводство, принудительные меры, тайная люстрация сообщений и телекоммуникаций, предмет наблюдения, наблюдение и метаданные, поиск IMSI, изменения Федерального закона о наблюдении за сообщениями и телекоммуникациями (BÜPF), правительственное программное обеспечение (GovWare), требования, управляющие использованием GovWare.

* Корреспондирующий автор
Адреса электронной почты: lst.donatsch@rwi.uzh.ch (А. Донач), mischa.demarmels@rwi.uzh.ch (М. Демармелс)