# National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies

## CZECH REPUBLIC

Version 3 November 2014

University of West Bohemia
Klára Kalibová and Martina Houžvová

# Summary


[1]. Surveillance (*sledování telekomunikačního provozu)* in the Czech Republic is widely limited by civil rights, namely right to privacy granted by the Constitution and the Data Protection Act. Therefore any surveillance activity targeting an individual has to be granted by a prior court approval.

[2]. Non-individual surveillance is limited by powers granted and control imposed over the intelligence services.

[3]. The Security Information Service (*Bezpečnostní a informační služba)* is entitled (Art. 8 para 2 of the Act on the Security Information Service) to non-individual surveillance, meaning surveillance which does not target individual rights and freedoms because it uses openly accessible information sources and does not infringe private space and private correspondence. Non-individual surveillance is not considered as using of intelligence technology (*použití zpravodajské techniky)* and consequently no prior permission is requested. The Security Information Service is entitled to capture, listen, monitor and evaluate information that are disseminated in a manner that allows an access of previously undefined group of persons, to make video and audio recordings, to use of preventive (*zabezpečovací)* and bait (*nástrahové)* techniques and to monitor the telecommunications, radio communications and other similar operation without tapping its contents.

[4]. Similarly, The Military Intelligence (*Vojenské zpravodajství)* is entitled (Art. 8 para 2 on Military Intelligence) to non-individual surveillance, meaning surveillance which does not target individual rights and freedoms because it uses openly accessible information sources and does not infringe private space and private correspondence. Non-individual surveillance is not considered as using of military technology (*použití vojenské techniky)* and consequently no prior permission is requested. The Military Intelligence is entitled to capture, listen, monitor and evaluate information that are disseminated in a manner that allows an access of previously undefined group of persons, to make video and audio recordings, to use of preventive (*zabezpečovací)*and bait (*nástrahové)* techniques and to monitor to monitor the telecommunications, radio communications and other similar operation without tapping its contents.

[5]. There are three safeguard bodies responsible for the control of surveillance mechanism and its execution, two parliamentary and one executive - The Permanent Commission on Control of Security Information Service (*Stálá komise pro kontrolu činnosti Bezpečnostní informační služby*), The Permanent Commission on Control of Military Intelligence (*Stálá komise pro kontrolu činnosti Vojenského zpravodajství) (both parliamentary*) and Office for Data Protection (*Úřad na ochranu osobních údajů*) (executive). However, the scope and the real impact has been discussed.

[6]. Judicial remedies are both administrative, civil and criminal. An illegal behaviour of and individual state official is a crime and a victim of such a behaviour may fill in a criminal complaint and within the criminal proceedings seek an appropriate remedy, may it be apology or monetary compensation. If a person claims breach of civil rights such a dignity, right to privacy or right to family life, he/she can fill a civil lawsuit and seek both, an apology or a monetary compensation within a district court (appeal

regional Court). Such compensation can be claimed also from the state when exercising public authority. After exhausting these remedies a person may fill in a constitutional complaint for breach of his or her basic rights and freedoms.

[7]. There are three intelligence services – the Security Information Service (*Bezpečnostní a informační služba, BIS)*, the Office for Foreign Relations and Information (*Úřad pro zahraniční styky a informace, ÚZSI)* and the Military Intelligence (*Vojenské zpravodajství, VZ)*, and the Police which to some extent are permitted to use surveillance methods. The general legal base for their activities is laid by the Act on Intelligence Services (*Zákon o zpravodajských službách České republiky*).[1] A special Act on the Security Information Service (*Zákon o Bezpečnostní a informační službě)*[2] and the special Military Intelligence Act (*Zákon o Vojenském zpravodajství*[3] specify powers and competences of the Security Information Service, Military Intelligence respectively. The Police is governed by the Police Act (*Zákon o Policii České Republiky).*[4] Hereinafter, the report is focused on surveillance outside the criminal proceedings.

[8]. The scope of powers of the Security Information Service includes collecting information (a) on the intentions and activities directed against the democratic foundations, sovereignty and territorial integrity of the Czech Republic, (b) on the intelligence services of a foreign power, (c) on activities threatening the state and official secrets, (d) on activities consequences of which may threaten the security or important economic interests of the Czech Republic, or (e) related to organized crime and terrorism. The Security Information Service has a national-wide scope of competence over inhabitants of the Czech Republic regardless their citizenship.

[9]. The Office for Foreign Relations and Information provides information originating abroad, important for the safety and protection of foreign political and economic interests of the Czech Republic.

[10]. The Military Intelligence provides information (a) originating abroad, important for the defence and security of the Czech Republic, (b) the intelligence services of foreign powers in the field of defence, (c) on the intentions and activities directed against the defence of the Czech Republic, (d) on the intentions and activities affecting classified information in the field of defence of the Czech Republic. The Intelligence is active both abroad and domestically (nation-wide).

[11]. All above mentioned intelligence services may within the scope of their competence request from public authorities the necessary assistance and information held by these authorities in connection with the scope of their powers. The security services may seek information from various registries, such as the register of inhabitants, register of various legal entities, register of vehicles, central register of drivers, register of travel documents, register of national identity cards, register of weapons, register of criminal records etc. The security service is entitled to request intelligence data only to the necessary extent needed for the performance of a particular task (Art. 11 of Intelligence Services Act). No specific court warrant is needed.

---

[1] Czech Republic, Act on Intelligence Services (*Zákon o službách České Republiky)*, 7 July 1994.
[2] Czech Republic, Act on Security Information Service *(Zákon o bezpečnostní informační službě),* 7 July 1994.
[3] Czech Republic, Military Intelligence Act (*Zákon o vojenském zpravodajství),* 16 June 2005.
[4] Czech Republic, Police Act (*Zákon o policii České republiky),* 17 July 2007.

[12]. For the performance of specific tasks related to suppression of financing of terrorism the intelligence services are entitled to request from banks and branches of foreign banks information on matters on their clients, which are subject to bank secrecy, or the provision of such information in the future, provided that the data may not be obtained otherwise. The security services need a warrant of the High Court issued prior to the request (Art. 11a of Intelligence Services Act).

[13]. Online and telecommunication surveillance conducted by the Police is a subject to permission granted only within the criminal proceedings. The prior court approval is needed to conduct any wire or wireless mas surveillance activity (Art. 88a of the Criminal Proceedings Code).

[14]. Annually, the Security Intelligence Service publishes report on mass surveillance activities within the criminal proceedings. According to Art. 7 of Act on Security Information Service, the Service is allowed to use various means of technology (incl. equipment) to achieve goals of the Service (Art. 8 para 1). A prior court warrant issued by the President of the High Court is needed (Art. 9).

[15]. Data retention *(uchovávání a využívání provozních a lokalizačních údajů)* is governed by Data Protection Act (*zákon o ochraně osobních údajů)*[5]and mainly the Electronic Communications Act (*Zákon o elektronických komunikací*).[6] According to the Art. 97 para 3 a legal or a natural person providing a public communications network or a publicly available electronic communications service is required to store the call detail record of telephony and internet traffic and transaction data for a period of 6 months by providing that the content of communication is neither stored nor transmitted. Those data may be demanded by the Police, Security Information Service, Military Intelligence, and the Czech National Bank.

[16]. The intelligence services are controlled by the Government and by the Parliament (Art. 12 of Intelligence Services Act). Annually, the intelligence services are request to submit a report to the Government. Security Information Service is controlled by the Permanent Commission on Oversight over the work of the Security Information Service (*Stálá komise pro kontrolu Bezpečnostní informační služby)*[7] and Military Intelligence by the Permanent Commission on Oversight over the work of Military Intelligence (*Stálá komise pro kontrolu činnosti Vojenského zpravodajství).* The control of the Office for Foreign Relations and Information is not supervised by a special Committee or body.

[17]. Mass surveillance safeguards are established by the governmental control and by the system of judicial control, or the possibility to challenge the unlawful surveillance by a civil lawsuit against the State (Art. § 12 of Act On liability for damage caused in the exercise of public authority decision or incorrect official procedure)[8] or by a

[5] Czech Republic, Data Protection Act (*Zákon o ochraně osobních údajů),* 4 April 2002.
[6] Czech Republic, Electronic Communications Act (Zákon o elektronických komunikací), 22 February 2005.
[7] The Permanent Commission on Oversight over the work of the Security Information Service, http://www.psp.cz/ff/17/14/62/1c.htm.
[8] Czech Republic, Act On liability for damage caused in the exercise of public authority decision or incorrect official procedure, 17 March 1998, available at: http://www.zakonyprolidi.cz/cs/1998-82.

criminal complaint against the responsible state official who acted in breach of his powers (Art. 158 of Crimianl Code).

# Annex 1 – Legal Framework relating to mass surveillance

## A- Details on legal basis providing for mass surveillance

| Name and type of the mass surveillance-related law | A definition of the categories of individuals liable to be subjected to such surveillance | Nature of circumstances which may give rise to surveillance | List purposes for which surveillance can be carried out | Previous approval / need for a warrant | List key steps to be followed in the course of surveillance | Time limits, geographical scope and other limits of mass surveillance as provided for by the law | Is the law allowing for mass surveillance in another country (EU MS or third countries)? |
|---|---|---|---|---|---|---|---|
| Act on Intelligence Services (Zákon o informačních službách): this does not include surveillance as such, but rather collecting information from various sources. | Anybody (Art.11) within the territory of the Czech Republic; banks (Art. 11a) | Need of information to perform a task in its competence (Art.11); need of information in a concrete case to supress the financing of terrorism. | National security, economic interests of the Czech Republic, terrorism. | No warrant when state bodies are requested for information; prior warrant when banks are requested for information (Art. 11a); prior warrant when other private bodies are requested. | The access into most national registers is permanent online, some (like Register of Criminal Records) provide ad hoc information on request. | The territorry of the Czech Republic against both the Czech and foreign citizens, no time limits as no lasting surveillance is exercised. | No, as no lasting surveillance is exercised. |
| Act on Security Information Service (*Zákon o bezpečnostní* | Everybody (Art. 7 et sq.). | Performance of a task of the Security Information Service. | National security, economic interests of the Czech Republic, terrorism, activities on foreign power | Prior warrant by the President of the High Court (*Vrchní soud*) when a surveillance against individual is used (Art. 9 Act on | The Service requires the warrant from the High Court; the Court issues the warrant; the Service uses surveillance; the Court may ask the | Perfomed within the territorry of the Czech Republic against both the Czech and foreign citizens. | No |

| Name and type of the mass surveillance-related law | A definition of the categories of individuals liable to be subjected to such surveillance | Nature of circumstances which may give rise to surveillance | List purposes for which surveillance can be carried out | Previous approval / need for a warrant | List key steps to be followed in the course of surveillance | Time limits, geographical scope and other limits of mass surveillance as provided for by the law | Is the law allowing for mass surveillance in another country (EU MS or third countries)? |
|---|---|---|---|---|---|---|---|
| *informační službě*)[9] | | | within the territory of the Czech Republic (Art. 5 of Act on Security Service). | Security Information Service). | Service to provide it with necessary monitoring reports; when the Court finds out that the Service acts in breach with protection of individual rights or acts outside its scope, it may void the warrant; the Service informs the Court when it cancels the surveillance. | | |
| Act on Military Intelligence (*Zákon o Vojenském zpravodajství*) | Everybody (Art. 7 et sq.). | Performance of a task of the Military Intelligence. | The Military Intelligence provides information (a) originating abroad, important for the defence | Prior warrant by the President of the High Court (*Vrchní soud*) warrant when a mass surveillance against individual is used (Art. 9 Act | The Service requires the warrant from the High Court; the Court issues the warrant; the Service uses mass surveillance; the Court may ask the | Perfomed within the territorry of the Czech Republic against both the Czech and foreign citizens. | No |

[9] Czech Republic, Act on Security Information Service (Zákon o bezpečnostní a informační službě), 7 July 1994.

| Name and type of the mass surveillance-related law | A definition of the categories of individuals liable to be subjected to such surveillance | Nature of circumstances which may give rise to surveillance | List purposes for which surveillance can be carried out | Previous approval / need for a warrant | List key steps to be followed in the course of surveillance | Time limits, geographical scope and other limits of mass surveillance as provided for by the law | Is the law allowing for mass surveillance in another country (EU MS or third countries)? |
|---|---|---|---|---|---|---|---|
| | | | and security of the Czech Republic, (b) the intelligence services of foreign powers in the field of defence, (c) on the intentions and activities directed against the defence of the Czech Republic, (d) on the intentions and activities affecting the classified information in the field of Defence of The Czech Republic. The Intelligence is active abroad and national wide. | on Military Intelligence). | Service to provide it with necessary monitoring reports; when the Court finds out that the Service acts in breach with protection of individual rights or acts outside its scope, it may void the warrant; the Service informs the Court when it cancels the surveillance. | | |

## B- Details on the law providing privacy and data protection safeguards against mass surveillance

| **Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance** | **List specific privacy and data protection safeguards put in place by this law(s)** | **Indicate whether rules on protection of privacy and data protection apply:**<br><br>**only to nationals or also to EU citizens and/or third country nationals** | **Indicate whether rules on protection of privacy and data protection apply:**<br><br>**only inside the country, or also outside (including differentiation if EU or outside EU)** |
|---|---|---|---|
| Include a reference to specific provision and describe their content | e.g. right to be informed, right to rectification/deletion/blockage, right to challenge, etc. | Please, provide details | Please, provide details |
| Data Protection Act (Zákon o ochraně osobních údajů)[10] | Right to be informed on scope of data collection performed by any official or private data collector; right to understand the scope of data collection; right to ask to widraw from data collection; however the Security Information Service is not obliged to provide those information to an individual (Art. 16 para 3 of Act on Security Information Service). These safeguards do not directly apply to surveillance activities since an individual may be prevented from obtaining any | All nationals | Also outside, EU and non EU |

[10] Czech Republic, Data Protection Act (*Zákon o ochraně osobních údajů),* 4 April 2002

| | | | |
|---|---|---|---|
| | information (see. Art. 16 para 3 of Act on Security Informationa Service.) | | |

# Annex 2 – Oversight bodies and mechanisms

| Name of the body/mechanism | Type of the body/mechanism | Legal basis | Type of oversight | Staff | Powers |
|---|---|---|---|---|---|
| *in English as well as in national language* | *e.g. parliamentary, executive/government, judicial, etc.* | *name of the relevant law, incl. specific provision* | *ex ante / ex post / both/ during the surveillance/etc. as well as whether such oversight is ongoining/regularly repeated* | *including the method of appointment of the head of such body **AND** indicate a total number of staff (total number of supporting staff as well as a total number of governing/managing staff) of such body* | *e.g. issuing legally binding or non-binding decisions, recommendations, reporting obligation to the parliament, etc.* |
| **The Permanent Commission on Control of Security Information Service (Stálá komise pro kontrolu činnosti Bezpečnostní informační služby)** | parliamentary | Art. 12 of Security Services Act; | Ex post | 7 PMs; head is appointed , 1 employee of supporting staff[11] | Powers of the Commission are limited. There are no investigative or financial powers, nor the opportunity to inspect directly the operational files. There is only reporting obligation by the Security Information Service. The Commission may report any shortcomings or illegal acts to the Supreme Public Prosecutor. |

[11] Wills, Aidan, Vermeulen, Mathias, Parliamentary Oversight of Security and Intelligence Agencies in the European Union, DG for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, European Parliament, Brussels, 2011. Available at: http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf.

| | | | | | |
|---|---|---|---|---|---|
| **Office for Data Protection** | Executive | Art. 3 of Data Protection Act | During, ex post | The President, 100 employees (supporting staff)[12] | Office for Data Protection may inspect any denial of providing the information to an individual by a public or private body which collects personal data. However, the intelligence services are excluded from its competence. |
| **The Permanent Commission on Control of Millitary Intelligence (Stálá komise pro kontrolu činnosti Vojenského zpravodajství)** | Parliamentary | Art. 21 of Military IntelligenceAct; | | | Powers of the Commission are limited. There are no investigative or financial powers, nor the opportunity to inspect directly the operational files. There is only reporting obligation by the Millitary Intelligence. The Commission may report any shortcomings or illegal acts to the Supreme Public Prosecutor. |

[12] Office for Data Protection (Úřad na ochranu osobních údajů), Annual Report 2013 (Výroční zpráva 2013), availalble at: http://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=9302.

# Annex 3 – Remedies[13]

| Act on Intelligence Services (Zákon o  informačních službách), Act on Military Intelligence, Act on Security Information Service, Act on Free Access to Information (*Zákon o svobodném přístupu k informacím).* | | | | |
|---|---|---|---|---|
| **Stages of surveillance process** | **Is the subject informed?** | **Does the subject have a right of access to the data collected on him/her?** | **List remedies available to an individual concerned** | **Legal basis for using the available remedies** |
| | No | No | Please list the type of remedial action that can be taken: e.g.: claims lodged with court(s), claims lodged with the oversight body, request to the surveillance authority, etc. **AND** please specify also the name (e.g. Supreme Court) and type of the body (e.g. judicial, executive, parliamentary) providing such remedies. | Violation of data protection, private life, specific legislation, etc. |
| **Collection*** | NO | No | Admnistrative lawsuit against the State to the Regional court; civil rights for breach of personality rights criminal complaint against an individual officer to the District court; court of appeal – Supremene Administrative Court, resp. Regional Court; then constitutional complaint for breach of basic rights | Violention of data protection, unlawful proceedings, abuse of power of a state official |

[13] In case of different remedial procedures please replicate the table for each legal regime.

* For the definitions of these terms, please refer to the FRA/CoE (2014), *Handbook on European data protection law*, Luxembourg, 2014, pp. 46-47, available at: http://fra.europa.eu/en/news/2014/council-europe-and-eu-fundamental-rights-agency-launch-handbook-european-data-protection.

| | | | | |
|---|---|---|---|---|
| | | | and freedoms after all remedies are rejected. | |
| **Analysis*** | NO | No | Admnistrative lawsuit against the State to the Regional court; civil rights for breach of personality rights criminal complaint against an individual officer to the District court; court of appeal – Supremene Administrative Court, resp. Regional Court; then constitutional complaint for breach of basic rights and freedoms after all remedies are rejected. | Violention of data protection, unlawful proceedings, abuse of power of a state official |
| **Storing*** | NO | No | Admnistrative lawsuit against the State to the Regional court; civil rights for breach of personality rights criminal complaint against an individual officer to the District court; court of appeal – Supremene Administrative Court, resp. Regional Court; then constitutional complaint for breach of basic rights and freedoms after all remedies are rejected. | Violention of data protection, unlawful proceedings, abuse of power of a state official |
| **Destruction** * | NO | No | Admnistrative lawsuit against the State to the Regional court; civil rights for breach of personality rights criminal complaint against an individual officer to the District court; court of appeal – Supremene Administrative Court, resp. | Violention of data protection, unlawful proceedings, abuse of power of a state official |

| | | | | |
|---|---|---|---|---|
| | | | Regional Court; then constitutional complaint for breach of basic rights and freedoms after all remedies are rejected. | |
| **After the whole surveillance process has ended** | Yes | No | Admnistrative lawsuit against the State to the Regional court; civil rights for breach of personality rights criminal complaint against an individual officer to the District court; court of appeal – Supremene Administrative Court, resp. Regional Court; then constitutional complaint for breach of basic rights and freedoms after all remedies are rejected. | Violention of data protection, unlawful proceedings, abuse of power of a state official |

# Annex 4 – Surveillance-related case law at national level

*Please provide a maximun of three of the most important national cases relating to surveillance. Use the table template below and put each case in a separate table.*

| | |
|---|---|
| **Case title** | N/A |
| **Decision date** | |
| **Reference details (type and title of court/body; in original language and English [official translation, if available])** | |
| **Key facts of the case (max. 500 chars)** | |
| **Main reasoning/argumentation (max. 500 chars)** | |
| **Key issues (concepts, interpretations) clarified by the case (max. 500 chars)** | |
| **Results (sanctions) and key consequences or implications of the case (max. 500 chars)** | |

# Annex 5 – Key stakeholders at national level

*Please list all the key stakeholders in your country working in the area of surveillance and divide them according to their type (i.e. public authorities, civil society organisations, academia, government, courts, parliament, other). Please provide name, website and contact details.*

| **Name of stakeholder** (in English as well as your national language) | **Type of stakeholder** *(i.e. public authorities, civil society organisations, academia, government, courts, parliament, other)* | **Contact details** | **Website** |
|---|---|---|---|
| **Bezpečnostní informační služby (Security Information Service)** | Inteligence service | Bezpečnostní informační služba<br>P. O. BOX 1<br>150 07 Praha 57 | www.bis.cz |
| **Úřad pro zahraniční styky a informace (Office for foreign relation and information)** | Inteligence service | Úřad pro zahraniční styky a informace<br>P.O. Box 153<br>160 41 Praha 6<br>E-mail: uzsi@uzsi_cz | www.uzsi.cz |
| **Vojenské zpravodajství (Military Inteligence)** | Inteligence service | Ministerstvo obrany – 4730<br>Tychonova 221/1<br>160 01 Praha 6 | www.vzcr.cz |
| **Vrchní soud (High Court)** | Court | Nám. Hrdinů 1300, Praha 4, 140 00 | N/A |
| **Iuridicum Remedium** | CSO | Iuridicum Remedium, o. s.<br>Pplk. Sochora 40 | www.iure.org |

| | | | |
|---|---|---|---|
| | | 170 00 Praha 7<br>tel.: +420 776 703 170 | |
| **Asociace pro mezinárodní otázky (Association for International Questions)** | CSO | Asociace pro mezinárodní otázky – AMO<br>Žitná 608/27<br>110 00 Praha 1<br>+420 224 813 460 | www.amo.cz |
| **Úřad na ochranu osobních údajů (The Office for Personal Data Protection)** | Public authority | Pplk. Sochora 27<br>170 00 Praha 7<br>+420 234 665 111<br>posta@uoou.cz | www.uoou.cz |

# Annex 6 – Indicative bibliography

Please list relevant reports, articles, studies, speeches and statements divided by the following type of **sources *(in accordance with FRA style guide)*:**

1. Government/ministries/public authorities in charge of surveillance

   Security Inteligence Service: Annual Report[14]

   Office for foreign relation and information: Annual Report[15]

   Vojenské zpravodajství: Annual Report 2012[16]

2. National human rights institutions, ombudsperson institutions, national data protection authorities and other national non-judicial bodies/authorities monitoring or supervising implementation of human rights with a particular interest in surveillance

   The Office of Personal Data Protection: Annual report 2013 [17]

   The Public Officer of Rights: Annual report 2013[18]

3. Non-governmental organisations (NGOs)

---

[14]Czech Republic, Security Information Service (2014), Annual Report (Výroční zpráva Archivu Bezpečnostní informační služby za rok 2013), available at: http://www.bis.cz/vyrocni-zpravy.html.

[15] Czech Republic, Office for foreign relation and information (2013), Annual Report 2012 (*Výroční zpráva pro rok 2012),* available at: http://www.uzsi.cz/cz/vyrocni-zprava-podle-zakona-c-106-1999-sb-za-rok-2012.html.

[16] Czech Republic, Vojenské zpravodajství (2013), Annual Report 2012 (*Výroční zpráva pro rok 2012) available at: http://www.vzcr.cz/shared/clanky/21/V%fdro%e8n%ed%20zpr%e1va%202012.pdf*.

[17] Czech Republic, The Office of Personal Data Protection (2014), Annual Report (*Výroční zpráva),* available at: http://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=9302.

[18] Czech Republic, The Public Deffender of Rights (2014), Annual Report (*Výroční zpráva),* available at: http://www.ochrance.cz/fileadmin/user_upload/zpravy_pro_poslaneckou_snemovnu/Souhrnna-zprava_2013_PDF_A.pdf.

Iuridicum Remedium: Data Retention in the (not only) Police practice[19]

4. Academic and research institutes, think tanks, investigative media report.

   Not available for the period

[19] Czech Republic, IuRe (2012), Data retention not only in the Police practice *(Data retention v (nejen) policejní praxi),* available at: http://www.slidilove.cz/sites/default/files/dr-analyza-final2.pdf.