

HUMAN RIGHTS – REAL OF JUST FORMAL RIGHTS? EXAMPLE OF THE (UN)CONSTITUTIONALITY OF DATA RETENTION IN THE CZECH REPUBLIC*

Jan Kudrna

Charles University in Prague, Faculty of Law,
Department of Constitutional Law
Nám. Curieových 7, 116 40 Praha 1, Czech Republic
E-mail: kudrnaj@prf.cuni.cz

Received on 27 October, 2012; accepted on 5 December, 2012

***Abstract.** Approximately twenty years after it was necessary to fight for human rights, the time came when it was necessary to do it again. Or to begin at the very least to protect them very strongly and thoroughly in a preventive manner. Other methods and means will revert to time when human rights were formally anchored but their material establishment is not yet realized, or not at least to the extent expected corresponding to their real substance.*

The beginning of the 90's in Central and Eastern Europe was a success in that human rights began to be looked on as natural, forming the basis of democratic State respecting the rule of law. Today we are increasingly more often encountering the reality that human rights, on the contrary, to the same extent that they have been able to be established, they are losing in value. The biggest danger consists in the fact that limiting of human rights often is attended by silence, without wider public discussion or deliberations.

The lack of qualified discussion during the limiting of human rights by way of laws and implementing regulations is however a systemic problem. Correction of its results can be often very complex and doing away with the causes a long term effort. It is dependent on the quality of representative democracy and of the civil society as well.

* This article was worked on within the framework of the research project PRVOUK 04. Translation was done by James Critz, Ph.D.

This article is devoted to problem of implementation of evidence of data accompanying telecommunications traffic, the so-called data retention, and in its development from lack of legal regulation to roughly unconstitutional legal regulation and finally to hope for a reasonably constitutional solution.

Keywords: *data retention, Czech Republic, Constitutional Court, Parliament, government, privacy, right to privacy, human rights, European Union, directive.*

1. Endangerment to Human Rights under the Conditions of Democratic Rule of Law?

Approximately twenty years after it was necessary to fight for human rights, the time came when it was necessary to do it again. Or to begin at the very least to protect it very strongly and thoroughly, and this in a preventive manner. I am thinking that with other methods and means time will revert to when human rights were formally anchored but their material establishment is not yet realized, or not at least to the extent expected corresponding to their real substance.

The beginning of the 90's in Central and Eastern Europe was a success in that human rights began to be looked on as natural, forming the basis of democratic State respecting the rule of law. Today we are increasingly more often encountering the reality that human rights, on the contrary, to the same extent that they have been able to be established, they are losing in value.

The biggest danger consists in the fact that limiting of human rights often is attended by silence, without wider public discussion or deliberations. In the Czech Republic probably the most violated provision of the Charter of Fundamental Rights and Freedoms is its Art. 4 sect. 4, stating: „*During the using of the provisions on the limits of basic rights and freedoms their substances and sense must be preserved. Such limits are not allowed to be abused for other purposes than those for which they were specified.*“

Individual cases of infringement of human rights are essentially unwanted but in a State respecting the rule of law normally are able to be resolved. The lack of qualified discussion during the limiting of human rights by way of laws and implementing regulations is however a systemic problem. Correction of its results can be often very complex and doing away with the causes a long term effort. It is dependent on the quality of representative democracy and of the civil society as well.

One of the examples from the Czech Republic recently in which the existence of this problem is apparent is the problem of evidence of data accompanying telecommunications traffic. In this matter even the Czech Constitutional Court made a decision, and this on 22 March 2011, in its decision File No. Pl. ÚS 24/10.

2. The Beginning of the Monitoring of Telecommunication Traffic in the Czech Republic

Today in the Czech Republic one of the key standards for monitoring telecommunications traffic is Act No. 127/2005 Coll., on electronic communications and on change of some dependent laws (further only „law on electronic communications“), as amended.

The problem of monitoring accompanying data on communication, never of the content itself of the messages transmitted, is however older than the aforementioned law. In this matter it is possible to point to two decisions of the Constitutional Court already in the year 2000, specifically File No. II. ÚS 502/2000 and IV. ÚS 536/2000.

The situation at the time was not clear from the legal point of view since no legal regulation in the Czech Republic resolved the question of the collection of accompanying data, nor the problem of their eventual use for purposes of criminal proceedings.

The Constitutional Court had to solve the question of whether not only the content of the message transmitted but also the accompanying data about the connection, with the help of which the message was transmitted, was subject to Constitutional protection. To this question it answered affirmatively.

First it stated that this protection flows from Art. 13¹ of the Charter of Basic Rights and Freedoms² itself. The Constitutional Court justified the legal authority to obtain and use accompanying data on telecommunication traffic by the necessity for protection of society from criminal acts and the possibility of punishing them. The Constitutional Court also identified such infringement as allowable if it is essential in the given sense of the word. To this it further attached a basic condition in the interest of protection against violation of the limits on essentials. The mentioned infringements are contingent on the existence of corresponding and sufficient guarantees protecting against abuse. These should be appropriate legal rules and concurrently also a system of control for upholding them. The legal rules have to be *precise* in the sense that they give citizens clear information about under which circumstances it is possible to meddle with their privacy, and further in that sense that it will be clear which appropriate organ legal power is given to and in which manner it is able to apply it. The legal rules must also guarantee citizens protection against *arbitrary interference* with their privacy.

The Constitutional Court explicitly stated: „*In the case that these principles will not be respected on the part of the State power, interferences into the mentioned fundamental rights are excluded and if they should occur they are taking place unconstitutionally.*“

The Constitutional Court at the time was in agreement with the decision of the European Court for Human Rights of 2 August 1984 in the matter of *Malone v. United*

1 In this matter I would allow myself to polemize, because pragmatically the protection of traffic data about communications is dependent rather on the general protection of privacy anchored in Art. 10 of the Charter. Even though there is no doubt about the fact that from a practical viewpoint reference to Art. 13 of the Charter is more useful.

2 Its English translation is accessible, for example, at: <<http://www.psp.cz/cgi-bin/eng/docs/laws/1993/2.html>>.

Kingdom. In principle, however, it allowed the collection of accompanying data only for purposes of criminal prosecution, and this still with substantial restrictions.

In its finding the Constitutional Court also recommended the acceptance of a special amendment, which would regulate the described matters. This was done in later periods. As this special amendment in the area of the collection of accompanying communications data for the purposes of criminal prosecution it is possible to consider above all § 88a of the Criminal Procedure Code, dealing with the use of obtained data.

For collection and providing access to accompanying data there is the law on electronic communications passed in 2005. Its particularity is that it makes possible blanket preventive collection of a significant quantity of accompanying data, without a prior specified purpose. Its weakness is its marked general character, so that the extent of the collected data is defined later by the implementing rule.

This rule is Act No. 485/2005 Coll., on the extent of traffic and location data, the period of their storage, and the form and manner of their being handed over to organs empowered to use them. In the Czech Republic it was just this rule that was the key standard for determining what kind of data should be stored and made accessible.

The recommendation of the Constitutional Court at the time was *formally* carried out. In reality however never, because limits set by the Constitutional Court were disavowed by the blanket collection of data.

During the passing of the law on electronic communications the obligation to implement the European law was argued. Specifically European Directive 2006/24/ES, which expanded on the preceding Directive 2002/58/ES.

There it is recalled what the content above all of the first Directive is. That Directive mentions the obligation to blanketly collect key data on all manner of electronic communication in the member States of the European Union. The fundamental controversy lies in that data are collected blanketly, preventively, and, in a specific case, exceptionally, it is not possible to elucidate a reason why this is so.³

With respect to the fact that the Directive affects approximately 500 million residents of the European Union, of whom a vast majority has not been and is not a security risk, it is possible to make the judgement that one is dealing with one of the cases where it amounts to an exchange of „freedom for security“. Such an argument, in which emotion predominates, is very dangerous for human rights. Should limiting like this occur, then it would be necessary that it should occur through very full-blown deliberation. A well-qualified discussion about the problem and possible solutions must necessarily precede these. It is essential that the issue should be evaluated without prejudice about whether danger actually exists, whether it can be eradicated or minimalized, eventually by what manner, and whether the solution approved is able to fulfil its role at all. It is also necessary to choose a solution which will interfere with human rights and freedoms to the least extent.

3 A very pertinent and thorough discussion of this problem, as almost the only one/unique in Czech sources, can be found here: Hořák, J. Právo na soukromí versus bezpečnost ve sjednocené Evropě: zamyšlení nad problematikou „data retention“. (The right for privacy versus safety in unified Europe: thoughts on the problem of „data retention.“). *Acta Universitatis Carolinae. Iuridica*. 2006, 1: 81–98.

The preparation and passage of European Directive 2006/24/ES is very often criticized just for this reason, that the mentioned requirements were not fulfilled and that, on the contrary, the Directive at that time created room for further indirect infringement of human rights and freedoms, even though these led to substantial limiting or even the elimination of security threats.

The Czech Republic for the great part realized the measure contained in the Directive on the basis of the bill in the form in which it was debated and did this precisely through the law on electronic communication and its implementing rule.

In spite of the controversy of the substance of both directives it is necessary to say that their minimal standard was vastly exceeded by the Czech legal version.⁴

3. (Non-)Deliberation of the Substance of the Problems of Data Retention in the Czech Parliament

The question mentioned above was raised again in the beginning of 2008, when an amendment bill was introduced for the law on electronic communications with the goal of harmonizing the law with the second above mentioned Directive. With respect to the fact that the time period for implementing the Directive in the legal system of the Czech Republic had already passed and sanctions were threatened on the part of the European Union, the Government proposed that the bill be approved already on the first reading.

The amendment was characterized as „not too extensive“. The Government as its proponent stated that from the point of view of protecting the accompanying data on communications that had taken place the bill means a negligible expansion, consisting in the monitoring and recording also of unsuccessful attempts to connect. Further changes were not supposed to touch on this area but on the question of sanctions, the necessity of conducting certain statistics on the amount of data transmitted, etc.

In a similar spirit the Parliamentary reporter, who was a member of the government coalition party, also stepped forward. He did not mention the real problem of infringement on privacy but, on the contrary, emphasized that the collecting and transmission of accompanying data on communication should help during investigation of *serious criminal acts*.⁵

On the real problem of interferences with privacy and their extent a representative of the opposition Social Democratic Party (ČSSD) came forward. He drew attention to the massive volume of data which are collected blanketly, without limitation of their use to only investigation of *serious criminal acts*.⁶ He explicitly emphasized the problem

4 This however did not prevent many Czech politicians at the time, and especially later, from arguing along the line that they are not able to do anything, because it is a matter of „a requirement from Brussels“.

5 Both speeches, just as later ones following up on them, are accessible in stenographic records of the 1. reading at: <<http://www.psp.cz/eknih/2006ps/stenprot/027schuz/s027044.htm#r1>>.

6 For completeness it is suitable to add that the law on electronic communications was prepared in 2005 approved during the government led by ČSSD.

of localization of cell phones that were turned on, which *are not* used for making a connection at a given moment.

To this rebuttal the representative of the proponent of the amendment answered that transmitted data are collected only at that time when the telephone attempts to make an established connection with another device.⁷

The representative of the Government, however, was not speaking the truth when he said that the location of a cell phone that is turned on and which is not at that moment used for communication is not recorded. These records were made on the basis of § 2 sect. 3 letter c) of the mentioned rule.⁸

A whole series of further data, and this *beyond the framework* of the implemented Directive was never collected on the basis of the law but precisely of the implementing rule.

The most suitable time when Parliament could discuss these very sensitive matters was precisely in the period when it was debating the amendment to the subject law. At that time it could also clarify the law and also narrow the room in the framework of which the rule should be published.

Already the course of the first reading of the bill showed that such a discussion of the core problem would not occur, but most likely it would be rather that misleading information would sound out. This was also confirmed in later phases of the legislative process.

The Chamber of Deputies turned down the proposal for passage of the bill immediately on the first reading, but agreed with shortening the period of time for debate in committees to 30 days. The bill was ordered to the Economic, Constitutional and Safety Committees.

Not ever during the proceedings in the committees did a discussion occur on the essential problem - that is, whether and eventually to what extent to collect data, how to guard it against abuse, so that the privacy of individuals was preserved.

A similar situation occurred also in the second reading. In the context of narrowing the room for interference in privacy there was a single proposal for modification, and this by the representative for the opposition Communist Party (KSČM). She proposed that the law directly and not the implementing rule, specify what kind of data – strictly carried over from the executed Directive – could be collected. At the same time she proposed shortening the length of time for storage of data from one year to six months.

The remaining proposals for modification that were submitted either did not touch on the questions of protecting privacy or, on the contrary, they proposed to expand the circle of organs authorized to request this data and use it for their own purposes.

The modifying bill directed towards narrowing the room for collection of data was not passed on the third reading. It is worth mentioning the attitude of the Chamber of Deputies reporter, who expressed a negative point of view with reference to the fact that by its passage the Czech Republic would not fulfil the requirement coming from the

7 See the stenographic record at: <<http://www.psp.cz/eknih/2006ps/stenprot/027schuz/s027046.htm#r3>>.

8 In this sense also officials of the Police of the Czech Republic have repeatedly argued in the media for conservation of the legal possibility to locate a cell phone that is turned on.

implemented Directive. Specifically this reference was expressed in connection with the vote on the bill for the collected data to be stored at most six months from the time of its being acquired.

The reasoning in this point of view, however, was not correct, because the amendment was not in conflict with the requirements of the Directive. The Directive stipulates in Art. 6 the obligation of the States to ensure that data are stored for a period of at least six months and at most two years from the time of their acquisition. The amendment bill did not contradict this requirement. Even so the Chamber of Deputies reporter expressly characterized the bill in this part as being in contradiction with the Directive.

In the end the amendment was approved by a close majority of more than fifty percent. The debate finished three months after the submittal of the bill. The Senate approved the bill and the President of the Republic signed it on 25 June 2008. The law was published on 4 July 2008 under Act No. 247/2008 Coll.

It is possible to characterize the proceedings on the bill infringing blanketly on the privacy of all residents of the Czech Republic as a lost chance. Although at least one attempt to raise this question appeared, to argue it in a qualified manner and to eliminate indirect interference with human rights, in the end this opportunity was not used.

On the contrary in the discussion from the side of the submitter and the Chamber of Deputies reporter the arguments sounded misleading and expressly untrue, their intent was preserving the existing legal regulation which was going far beyond the requirements of the European law and in a fundamental manner blanketly breaching the privacy of the individual.

This manner of discussing meant the breaking of the provision Art. 4 sect. 4 of the Charter of Fundamental Rights and Freedoms. The essence and meaning of the law on privacy was not protected but, on the contrary, a method was chosen to avoid solving this problem. The result after was also, deviating from common practice, a petition to the Constitutional Court on 26 March 2010.

4. Decision of the Constitutional Court on Collecting of Accompanying Data

Through the aforementioned submittal a group of 51 representatives demanded the annulment of provision § 97 sect. 3 and 4 of the law on electronic communications and the implementing regulation No. 485/2005 Coll. It was paradoxical that it was particularly the representatives of the political parties which participated and shared in the exercise of government power. The whole situation was intensified even more by the fact that the vast majority of them *supported* the passage of the contested regulation during the legislative process by their own stance of agreement.

This led the Constitutional Court to issuing a definite warning as a result of its original review, whether the petition was „suitable for acting on“. The Constitutional Court pronounced that the submission of a petition by a group of representatives should

never serve as a path to obtaining an „judgement“ or „expert opinion“, but should act as an instrument guaranteeing protection of a Parliamentary minority (the opposition), against the actual majority. The Deputies of the majority, who participated in the exercise of government power have, according to the Constitutional Court, sufficient means for directly changing decisions that are in effect.

The Constitutional Court in the end did not explicitly say what kind of reasons led it to accepting the complete petition under these specific circumstances. Therefore it is not clear whether under other circumstances a similar petition could be rejected.

The petitioners in their submittal claimed a conflict of the contested legal rules with the fundamental rights guaranteed by Art. 7 sect. 1, Art. 10 sect. 2 and 3 and Art. 13 of the Charter and Art. 8 of the Convention on the Protection of Human Rights and Basic Freedoms (further only „Convention“). According to the petitioners annulment of the principle of proportionality anchored in Art. 4 sect. 4 of the Charter should also occur.

According to the petitioners there is no infringement of constitutionally guaranteed rights, only a breach of a right in a specific case, for example familiarizing oneself with accompanying data, but already creating conditions so that the State would be able to do so. That is, in the given case blanket and extraordinarily extensive collection of this data and this without clear reason in each individual case.

The petitioners saw a problem also in that it was not the State that collected the data but a private firm.

The petitioners also referred to the reality that, although traffic data in and of itself does not have a direct connection with the transmitted message, it is possible by combining them to infer the content of the message, that is the information - which means an infringement of the privacy of the individual. From the location data about the movement of the telephone in conjunction with the data about other telephones it is possible to safely determine who the person concerned has contact with, when and where. Similarly it is possible on the basis of information about the other person to often infer what kind of matter the person being monitored could deal with him, and by this deduce certain private characteristics of the person monitored.

The Constitutional Court during its decision making pointed on one hand to the existing development of its judicature, further to the fixed/stable and clear judicature of the European Court for Human Rights and on the other hand to the decision of the Constitutional Courts in other countries of the European Union.⁹

In the matters being decided there is, according to the Constitutional Court on the spot, the use of the concept „informational self-determination of the individual“, that is the possibility of the individual to influence what kind of information about himself he will expose to the world around. This requirement is more and more real, in proportion to the extent that the significance of electronic communications and data about the individual which can be or are being recorded grows.

9 This is concerned with the decision of the Constitutional Courts of Germany, Romania, Bulgaria and Cyprus. Moreover for example Sweden and Austria for reasons of serious constitutional concerns have not implemented this Directive so far.

The Constitutional Court recalled the necessity of evaluating the proportionality of each eventual breach of human rights in three phases.

First it is necessary to assess whether the proposed acquisition is being done at all in order to attain a declared goal. Then it is necessary to weigh whether in the selection of means a way was chosen that is most considerate towards the right that was being broken. And finally whether the result achieved is disproportionate in comparison with the encroachment into the right that was breached.

Beside this it is essential that appropriate standards be specific and contain mechanisms which will not create possibilities for their abuse and, as much as possible, that they will prevent such abuse. A part of this must also be the possibility of independent judicial control over specific breaches of human rights.

During its consideration in the same matter the Constitutional Court stated the following inadequacies of the contested amendment. First there is its non-specificity and vagueness. From the law itself it is not possible to determine for what kind of organs specifically are data able to be provided, because the law speaks about „organs empowered on the basis of specific rules“.

Non-specificity also lies in the fact that the purpose is not clearly stated for which data can be obtained. While the implemented Directive talks about harmonization for the purpose of determining accessibility of these data for purposes of investigating *serious* punishable acts, neither the law on electronic communications, nor the implementing regulation contain such restriction. Not even § 88a of the Code of Criminal Procedure contains this.

With respect to the fact that accessing collected data is not tied to well-founded suspicions from the committing of a criminal act, but according to the law data are able to be used any way within the framework of criminal procedure, the Constitutional Court concludes that the contested regulations do not fulfil the requirements of the second phase of the proportionality test.

Further the Constitutional Court acknowledged the petitioners were correct in the sense that the contested amendment does not in any way specify the conditions necessary for ensuring the safety of the collected data, nor even protection against their misuse. Moreover it is also unacceptable according to the Constitutional Court that it is not clearly stated after what period of time the data should be destroyed, how it is able to be handled along with transmitted data, nor even is responsibility established and sanctions for breaking the rules for collection of data and handling it.

The Constitutional Court also expressed a fundamental doubt whether preventive blanket and general collection of traffic data related to communication activities of the whole population is an *adequate and essential* instrument. It referred also to its apparent ineffectiveness in a situation when it is possible to acquire an anonymous SIM card. It further justified its doubts with German statistics as well, according to which after the commencement of the collection of traffic data hardly any decline in the number of committed criminal acts occurred, but *above all not even an increase of their detection occurred*.

In conclusion the Constitutional Court also expressed its doubt about whether private subjects should at all have the possibility to collect such sensitive data on the communication of its clients and to dispose freely with them, for example even for the purpose of collecting debts or development of marketing activities.

On the basis of all the reasons presented the Constitutional Court granted the petition in its full extent and annulled the contested rules. Moreover it stated that the data already obtained under criminal procedure can be used only under serious evidence of a criminal act, for the purpose of prosecuting which it was gathered, and this only with regard to the circumstance of each individual case.

5. The Quality of the Legislative Process as One of the Prerequisites for the Existence of the Rule of Law

As is clear from the above the described judgement of the Constitutional Court of the Czech Republic is fundamental and a breakthrough. All the arguments which were uttered and were considered by the Constitutional Court however should already have sounded in the Chamber of Deputies.

Naturally, and *unfortunately*, it is not the only case when Parliament in the Czech Republic steps forward solely as a „formal“ lawmaker, but it does not give its activity beseeching content. At the same time it leads in this way to a fundamental erosion of human rights and freedoms. The erosion is worse in that it is almost unobserved and steadily lowers the attained standards of human rights.¹⁰ The poor quality work of Parliament thus puts itself on one of the foremost places in the hypothetical ladder of factors threatening human rights in the Czech Republic.

Particularly in so far as there is supposed to be a so-called exchange of „freedom for security“, so there should also be proper and competent discussion. The place for this is, above all, Parliament.

References

Hořák, J. Právo na soukromí versus bezpečnost ve sjednocené Evropě: zamyšlení nad problematikou „data retention“. (The right for privacy versus safety in unified Europe: thoughts on the problem of „data retention.“). *Acta Universitatis Carolinae. Iuridica*. 2006, 1: 81–98.

Kindlová, M.; Petrův, H.; Kudrna, J.; Antoš, M. *The Introduction to Czech Constitutional Law*. Prague: Charles University, 2009.

Klíma, K., *et al. Komentář k Ústavě a Listině*. Plzeň: Aleš Čeněk, 2005.

¹⁰ The reality that this is not just a hypothetical problem but, on the contrary, about a fundamental collapse of the system, is borne witness to in the end by a case revealed by chance in the Spring 2011, where, thanks to unauthorized monitoring, there were high Constitutional officials, including the Chairperson of the Constitutional Court.

Pavliček, V.; Hřebejk, J., et al. *Ústava a ústavní řád České republiky. Komentář. 2. díl. Práva a svobody*. Praha: Linde, 1999.

Sládeček, V.; Mikule, V.; Syllová, J. *Ústava České republiky. Komentář*. Praha: C. H. Beck, 2007.

Šimíček, V., et al. *Ústava České republiky. Komentář*. Praha: Linde, 2010.

Wagnerová, E.; Šimíček, V.; Langášek, T. *Listina základních práv a svobod. Komentář*. Praha: Wolters Kluwer, 2012.

ŽMOGAUS TEISĖS – REALIOS AR TIK FORMALIOS? DUOMENŲ SAUGOJIMO (ANTI)KONSTITUCINGUMO PAVYZDYS ČEKIJOS RESPUBLIKOJE

Jan Kudrna

Praha Karolio universitetas, Čekijos Respublika

Santrauka. Duomenų rinkimas telekomunikacijų priemonėmis yra vienas iš jautriausių klausimų, kalbant apie konstituciniu lygiu ginamos asmenų teisės į privatumą pažeidimą. Savo esme toks informacijos rinkimas reikšmingai nesiskiria nuo tiesioginio perduodamos informacijos įrašinėjimo. Galima sakyti, kad asmenų sekimas yra viena iš didžiausių šiuolaikinių grėsmių euroatlantiniame regione.

Tokios stebėjimo priemonės turi būti naudojamos ypač atsargiai, kad nebūtų pažeista asmenų teisė į privatumą. Šios priemonės yra per daug galingos, kad būtų naudojamos neapdairiai ir be ypatingos kontrolės, todėl jų taikymo reglamentavimas turėtų būti svarstomas viešose diskusijose.

Nors Čekijos Respublikos Konstitucinis Teismas 2000 m., kai dar nebuvo naudojamas visuotinis duomenų rinkimas, suformulavo griežtus reikalavimus tokiam duomenų rinkimui ir leido šias priemones naudoti tik tiriant ypač sunkius nusikaltimus, nuo 2005 m. visuotinis duomenų rinkimas atliekamas išimtiniais atvejais, tačiau be aiškios kontrolės. Šiems veiksams pateisinti buvo pasitelktos dvi Europos Bendrijų direktyvos, tačiau tokių priemonių naudojimas nebuvo teisiškai įtvirtintas ir peržengė Europos teisės reikalavimus. Be to, tokių priemonių naudojimas nebuvo tinkamai aptartas parlamentinėse diskusijose.

Konstitucinis Teismas šią problemą vėl sprendė 2011 m., kai panaikino visas teises taisykles, leidžiančias rinkti ryšių duomenis, ir pakartojo, kad visuotinis duomenų rinkimas prevenciniais tikslais pažeidžia konstituciškai garantuojamą asmens teisę į privatumą bei yra nesuderinamas su taisyklėmis, užtikrinančiomis duomenų rinkimo apsaugą nuo piktnaudžiavimo.

Praėjus keliems mėnesiams po šio sprendimo, paaiškėjo, kad Čekijos Respublikoje neteisėtai buvo klausomasi aukštas pareigas užimančių asmenų, tarp jų ir Konstitucinio Teismo pirmininko, mobilaus telefono pokalbių. Šis pavyzdys patvirtino, kad tai nėra tik hipotetinė

problema, o tokių priemonių naudojimas valstybės saugumo tikslais ne visada garantuoja asmenų saugumą.

Reikšminiai žodžiai: *duomenų saugojimas, Čekijos Respublika, Konstitucinis Teismas, parlamentas, valdžia, privatumas, teisė į privatumą, žmogaus teisės, Europos Sąjunga.*

Jan Kudrna, Prahos Karolio universiteto Teisės fakulteto Konstitucinės teisės katedros docentas, socialinių mokslų (teisės krypties) daktaras. Mokslinių tyrimų kryptys: konstitucinių institucijų santykis ir jų tarpusavio ribojimai, nacionalinio saugumo konstituciniai aspektai.

Jan Kudrna, Charles University in Prague, Faculty of Law, Department of Constitutional Law, Associate Professor, Doctor of Social Sciences (Law). Research interests: relations between constitutional bodies and their mutual limitations, constitutional aspects of the national security issues.