SOME QUESTIONS ON THE ACT NO. 300/2008 – E-GOVERNMENT ACT

by

TOMÁŠ ŠČERBA*

The paper investigates the legislative context of the creation of the Act No. 300/2008 Coll., on electronic acts and documents authorised conversion which is to come into force as of 1 July 2009. This act, also called as the eGovernment Act, is a landmark case of the technical advance in the field of ICT law in the Czech Republic as the act aims to simplify and speed the complex process of mutual communication between the individuals (natural persons) and/or the legal persons (entities) on one side and the bodies of state authority on the other. The paper provides for information on several new legal instruments, e.g. data inboxes, the information system of the data inboxes, and the documents authorised conversion. Several specific issues regarding these newly instated instruments are observed, e.g., inter alia, the access to the data inboxes, the security of the information system of the data inboxes, technical feasibility of the whole system, distinction for which subjects the new law allows the data inboxes to be created, etc. Furthermore, the article deals with a brief legal comparative study of the Austrian framework which served primarily as inspiration for the Act on eGovernment and which set up corresponding milieu for the Czech act. The article further names several actual problems which the new framework brings to the issue and tries to provide corresponding answers thereto.

KEYWORDS

Communication with state authorities, eGovernment, information system of the data inboxes, data inbox, electronic storage area, access, authorised document conversion

1. INTRODUCTION

The current legislative environment certainly generates a number of legal normative acts which fulfill a teleological purpose for better or worse. Act No. 300/2008 Coll., on electronic acts and authorized document conversion

* E-mail: tomas.scerba@gmail.com

(hereinafter the "Act" or "Act on electronic acts"), coming from the workroom of the Ministry of Interior, was a masterpiece in the field of e-contractions which took a long time in its development. Initially, the Act arose under the sponsorship of the Ministry of Informatics and later the whole agenda was complexly passed over to the Ministry of Interior. The Act at issue changes, to a certain extent, the traditional perception of a legal act or, alternatively, an electronic legal act. The interesting point on the Act is that for proper fulfillment of its purpose it requires the cooperation of various bodies, e.g. courts, the Ministry of Justice, or professional chambers – Czech Bar Association, Notarial Chamber of the Czech Republic, the Executor Chamber of the Czech Republic etc. Therefore, one can call this Act an Act on the e-Government. The Act on electronic acts cannot be compared with the same acts throughout the European communities as, in the present case, it is a unique legal norm. It can only be shortly summarized that the legislator found some inspiration in neighboring Austria where a similar regulation applies; however, not identical.

As far as the Austrian perspective is concerned, in all cases the Austrian act serves as a model for our Czech act on basic registers (see below). The substance of the Austrian law lies in several key facts. The Austrian legislator instated the front-office represented by a brand new portal under the website myhelp.gv.at and the back-office represented by a system of internal communication ELAK (Der Elektronische Akt). Along with this, Austria has also been famous for its specific system for electronic filings (so-called e-Zustellung). This system is, *inter alia*, famous for its special delivery system. If a state authority finds out that a person disposes with a commercial data inbox, then it is obliged to deliver, as of 1 January 2009, the respective document to such a commercial data inbox. Otherwise, a state authority can deliver the document into a data inbox created by the state. Since the beginning of 2009, a dual system for delivering documents has existed in Austria.[1]

2. WHAT IS SO BREAKTHROUGH ABOUT THE ACT AND WHAT ARE ITS ADVANTAGES?

As was already stated, the Act is part of the e-Government structure, which, in itself, shows a high degree of revolution in the traditional sense of legal perception. At the same time, the Czech Republic has realized several significant changes, not only in the area of law itself, which have been important

[1] A so-called "Dualle Zustellung" system operates in way that a public authority clerk may decide whether to deliver the document electronically or not. Once the recipient is not reachable via his/her electronic inbox, a clerk will print the document and send it via registered post. This dual system was first developed by two companies – Raiffeisen Informatik and HPC and nowadays allows for the sending of documents to a special send station which automatically decides whether the document is to be sent.

for improved interconnectivity of the whole society. One of the positive elements attesting to this trend of an "information revolution", which we are currently facing, is the wording of the Act on electronic acts. In the first place, it is because of this that the Act, indisputably, provides many positive aspects which are usable for everyday practice of many subjects to which this act in its wording refers.[2]

Above all, it is the profound simplification and acceleration of the process of communication itself which is being realized between the corresponding subjects. It can be noted that such a regime of "electronic" legal acts presupposed by the new Act on electronic acts has not had an equal in the Czech legal environment, namely due to the fact that for communication with the respective state authority, it has always been necessary to dispose with electronic signature of a precisely defined standard. Acceleration of the communication pursuant to this new Act then means, *inter alia*, the electronic signature is not required. Thus, many complications are *de minimis*.

The next substantial advantage is, without doubt, the trend of continual enhancement in terms of security, namely with regard to the data inboxes (which will be dealt with later) as well as with regard to the complex system of particular elements within the information system. It can be predicted that the risk flowing from the dispatching, transfer and receiving of the documents via unsecured electronic channels (e.g. electronic channels of third parties) is to a large extent limited. On the other hand, in this respect, several risks or even relatively sophisticated computer threats may appear. These, too, will be dealt with shortly.

If this is the right place for an illustration of the direct practical advantages for particular physical persons on which the wording of the Act impacts, it cannot be ruled out that one of the most positive aspects of the new Act on electronic acts is the simplicity lying in the digitalization of the document (i.e. it is not absolutely necessary that the particular physical persons dispose with the paper document). This is practical, among other things, when practicing multilateral (perpetual) communication with state authorities. In other words, with the help of a digitalized document and a data network with state guarantee the waiting hours and other barriers typical for "classic" dispatching of documents to the filing room of a particular state body are done away with. Naturally, as stated earlier, the fact that the electronic signature is not needed for a particular communication makes the Act

[2] Such a complex system may seem to be, in this respect, unique in the Czech Republic. For instance in Austria, the massive development can be seen in a system of mutual communication with state authorities via so-called citizen-cards (Burgerkarte). It is a information card which is used for almost all services provided for by the Austrian state. One can conclude that this citizen-card system is key to the Austrian system of data inboxes.

on electronic acts, from the point of view of real "civic usability," an instrument with a high level of practical application.

3. LEGISLATIVE CONTEXT

A no less interesting matter, which can be historically traced, is the bundle of circumstances under which the wording of the Act was originated. Not many would remember today that the name of the Act contained a link to so-called "personal numbers".[3] In the end, the regulation concerning the personal numbers as unique identifiers was dropped the contents of the Act (naturally from the promulgation list as well). The questions concerning these identifiers is so complex and vast that it became part of the newly prepared bill (also from the workroom of the Ministry of Interior) which shall, at least, contain the "Act on basic registers" on its promulgation list. This act shall then consistently regulate the problems of agenda and source identifiers.[4] It can be asserted that the Act on electronic acts, the preparatory act on basic registers as well as the preparatory act on electronic identifiers shall construe the fundamental skeleton of the aimed practical legislation towards not only physical persons but also other subjects in the Czech Republic, this all in the era of the information and communication technologies revolution. This general framework of ICT Law (Information and Communication Technology Law) shall be, within the limits stated by law, amended and altered by bylaw acts (legal decrees).

Furthermore, for the avoidance of any instance of doubt, it should be stated that the Act No. 40/1964, the civil code, as amended, which provides for general regulation of legal acts, still remains in force together with the Act on electronic acts. First of all, the civil code states the solution for essential questions of the validity, enforceability and form of each particular legal act et seq. The newly prepared Act on electronic acts does not supplement the civil code and does not derogate it. It only clarifies the problems of electronic legal acts and further instates new legal categories which the Czech law did not encompass before. The Act also has several connections to the Act No. 500/2004, the Rules of administrative procedure act, which cannot be dealt with in detail due to the brevity of this lecture. The aim of this lecture is not to provide the comparative study of the respective provisions of the above acts (i.e. the Act on electronic acts, the civil code and the Rules of administrative procedure act) but rather to pinpoint several interesting questions which turn up with regard to the operation of the Act. For the

[3] The unique identifiers are considerably important due to the fact they do not contain the contested identifying attribute which, for example, typical for personal number of physical persons.

[4] Currently, this bill holds No. 598 of its Parliamentary print.

sake of simplicity, one should talk about the pros and cons of the new regulation set out by the Act. Concerning the negative sides of the Act, it should be stressed that such negative aspects are latent in the period before the act has come into force, and therefore have to be handled with an eye on the future. In order to perceive the Act correctly, one must discriminate between two major key levels of the Act. One is the level related to the data inboxes and the other is the level concerning the legal framework for authorized conversion. Following these two main levels, all subject matter of the Act can be successfully traced.

4. SCOPE OF APPLICATION OF THE ACT

The scope of application of the Act is briefly defined in the legislation in Section 1 of the Act. In principle there are three main areas of the scope of application of the Act. The act presumes that it shall be used for the regulation of relations in connection with electronic acts of public authorities, municipality bodies, or other state organs or institutions (e.g. the Czech Television), including organs of public authorities (i.e. public notaries or court executors) and this all vis-à-vis physical persons and legal entities and then legal entities vis-à-vis state authorities. One of the immediate intentions of the legislation is to allow for communication among the state organs themselves so that they can communicate more efficiently, more quickly and more sophisticatedly than they are able to nowadays via conventional communication channels of public administration. Therefore, the Act sets out, in its Section 1, that the electronic acts among state organs also belong to its scope of application.

The information system of the data inboxes is the second major level of the scope of application of the Act.[5] This regulated area of law is utterly new in area of the Czech legislation framework and therefore Section 2 of the Act provides for a legal definition of the data inbox, i.e. the explanation what this legal institute means. In accordance with this provision the data inbox means an electronic storage area determined for delivery of state bodies and for the realization of acts against state authorities. The Act, however, does not provide at all what the legal expression "electronic data storage" actually means, though this matter-of-law is of vital importance. The respective definition of this legal term cannot be found in any of the currently

[5] For the sake of clarity it should be noted that Austria successfully implemented a similar information system which is composed of three main sections: i) the sending service (Absendeservice), (ii) the delivering service (Zustelldienst) and (iii) the registration of addresses. Nevertheless, for registration within the electronic delivering system (e-Zustellung), one needs his/her citizen card. In order to harmonize the private and state system of electronic delivering, the Austrian government has arranged the creation of one system whose immediate objective is to enable smooth and direct mutual communication.

valid and effective legal normative acts of the Czech Republic. It will most probably be a question for the corresponding bylaw legislation who will have to adequately state a definition of such a legal term in order to, inter alia, exclude many interpretational problems as well as threatening risks. Should the case be vice versa, i.e. if the particular definition elements of the legal term electronic data storage are not specified, it cannot be ruled out that the absence of this definition's elements (or the non-existence of clear and addressed rules for its legal interpretation) may, under some circumstances, enable limitation or, *ad absurdum*, degradation of the peace of respective subjects operating with the electronic data storage on either side of the legal relation at issue.

Third main level of the scope of application of the Act represents the regulation of the documents authorized conversion. Like with the data inbox, the Act sets out a legal definition of this term in its Section 22.

5. THE DATA INBOX

As addressed before, the legislation defines the data inbox as meaning the electronic data storage separately attributed to physical persons, undertaking physical persons, legal entities, bodies of public authority and finally bodies of municipalities.[6] As far as the time aspect of the creation of a data inbox, the Act is favorable for bodies of public authorities as the data inboxes are in this case created immediately whereas for physical persons a three day waiting period applies. Such intention of the legislation has to be envisaged positively because it is true, however taken, that the biggest practical use of the data inboxes is to be seen exactly within the activity of the concrete organ of public authority or in connection therewith. The questionable fact remains if these time periods are technically feasible or, in other words, if the state authority can manage to avoid delays in connection with the instatement process and the creation of the data inboxes. The answers to these questions will perhaps be reached after this new legal instrument has been used for a number of months or perhaps years.

Without doubt, one of the most crucial questions is the one concerning the presumed amount of costs for the creation and maintenance of the data inbox. Within this context it should be pointed out that the Act does not set out any amounts as to the maintenance of the data inboxes (or controlling the corresponding technical infrastructure). Nevertheless, it provides for

[6] When compared to the Austrian system of the data inboxes, it can also be, generally speaking, created for all legal subjects. The Austrian data inbox (MEIN BRIEF.at) was first developed on the platform AustriaPro attached to the Austrian Chamber of Commerce in September 2008. Unfortunately, as of the issue date of this article, no official statistical data (e.g. on the number of users of this system) were made publicly available.

regulation of costs for creation of the data inbox while stating that no administrative fees shall be collected by the respective state authorities. Thus, in accordance with the Act, for all companies duly registered in the commercial register the Act stipulates the respective body authorized to implement and enforce the Act, i.e. the Ministry of Interior, shall create the data inbox for free upon a written request.[7] As Sections 4 and 5 of the Act stipulate all the conditions for the aforementioned in a thorough detail one should not await any additional specification in this respect. For the sake of clarity, it should be reiterated that for companies entered into the commercial register after the Act comes into force (i.e. as of 1 July 2009), the creation of the data inbox shall also be performed free of charge. To sum up the questions arising in connection with the costs, there needs to be discernment between the aforementioned costs and the costs resulting from various administrative fees which are also presumed by the Act. The latter do not normally exceed the amount of several hundreds of Czech crowns.

Together with instating the legal instrument of data inboxes, the vital question of access arises, i.e. who exactly and under what circumstances and conditions may gain access to the data inboxes. When considering the data inbox of a physical person the access to this type of the data inbox does not allow for many interpretation problems. *A priori* this shall be just this physical person. In the case of the legal entity, the situation remains, at the first glance, a lot more complicated as the legal entity usually has a collective statutory body. The Act itself does regulate this in Section 8 Par. 3, when it provides that, *"For the access to the data inbox of a legal entity for which the data inbox has been created the statutory body of the legal entity, a member of the statutory body, head of the organization branch of the enterprise of the foreign legal entity registered in the commercial register shall be authorized."* Nonetheless, it cannot be ruled out that the Act does not provide any solution for a situation when the owners of the said company cannot reach the agreement on who shall have the access to the data inbox of this company. It is most obvious that this issue might arise in joint stock companies in which the dispute over one particular document can evoke many heated discussions.

In everyday life there can arise many different situations in which the subject for which the data inbox has been created cannot communicate with its data inbox, i.e. to retrieve and read the documents delivered to this inbox. A simple illustration of this sort of problematic situation might be if a physical person (for which the data inbox of a physical person has been cre-

[7] For the sake of completeness it should be noted that the Austrian system which was an inspiration for the Czech legislation which allows citizens to use the data inboxes free of charge.

ated) falls ill and gets hospitalized for a period he/she is unable to enter the data inbox. In procedural legal normative acts there is used the legal institute of *recovery of a time period*. On the other hand, the Act on electronic acts construes the institute of an "*agent*" – in Czech "pověřená osoba". Furthermore, a number of other real examples may come into consideration. For instance, when a company has a confidential clerk (proxy) – in Czech "prokurista" - he shall be authorized to enter into the data inbox as based on the granted proxy. In this respect it needs to be reiterated that while assessing the access to the data inbox a dichotomist structure can be seen there: the subject for which the data inbox has been created and it is permitted that this person shall have access to all documents of any nature which have been delivered to the data inbox as opposed to the subject called the agent. Such a person, being a person for whom the data inbox has not been created, i.e. the agent, shall have no rights to get access to the documents marked as documents "*strictly private*" or "*personal delivery*". Should there arise on the side of the agent the need to get access to, and also read, the documents marked as personal delivery, the agent shall have to gain an appropriate permission (authorization) from the subject for whom the data inbox was been created. In reality this may be done through the power of attorney. The Act aims to follow the standard diction of delivery pursuant to applicable laws of the Czech Republic. Beside this, in the context of personal delivery, it instates a new institute of the "administrator" (please see Section 8 Par. 7 of the Act). This is practical in big corporations or branches of large enterprises where it is very unlikely that the responsible director will monitor all documents which are delivered to the data inbox.

The regulation concerning the access data needed for successful log in to the data inbox shall be the contents of the soon-to-be decree coming from the Ministry of Interior. According to the statements of Ministry of Interior representatives, there shall be two decrees drafted, one providing a close specification of the data inbox and the second offering some criteria for the documents authorized conversion which shall be dealt with below. But even now it is certain that in the case, e.g., of the physical person losing the access data or the data having been stolen, the Ministry invalidating the data and subsequently issuing new access data (by sending it via registered mail to the address). Accordingly, in the case of the agent, should the case be that the physical person elected its agent, such access data shall be delivered to the address of the agent.

Considering various eventualities related to the access to the data inbox, the legislation managed to avoid using such terms as "activation" or "deac-

tivation" of the data inbox while using the terms "make accessible" (in Czech zpřístupnit) and "lock up" (in Czech znepřístupnit). Concerning this issue the legislation deserves praise as the Act consistently sets out all requirements for making the data inbox accessible. As far as the physical persons are concerned, the data inbox is made accessible by the first log in to the data inbox. The legislation also keeps in mind the situation when the physical person, no matter the reasons (e.g. its hospitalization in a heath centre, is unable to log into the data inbox). In this case the data inbox was logged into on the fifteenth day of the delivery of the access data to the entitled person (see Section 9 of the Act). The Act construes a similar legal situation of a delivery as it is within civil and administrative laws. Basic modalities of the lock up of the respective data inbox are then set out in provision of Section 11 of the Act on electronic acts.

The systematics of the Act also discriminate between the *invalidation* of the access data and the variety of cases representing the cancellation of the data inbox. The legislation, one may conclude, has taken a big step forward when the former very long period for cancellation of the data inbox was limited to today's three years of the death of the physical person or of the wind-up of the legal entity (without a legal successor). It would be immensely difficult to argue in favour of further prolonging of this period (such a prolongation *ad absurdum* would be under the above circumstances perhaps detrimental or counter productive).

6. INFORMATION SYSTEM OF THE DATA INBOXES

Another legal instrument introduced by the Act on electronic acts which has a direct link with the data inboxes (while simultaneously using the information system for evidence of the residents) is the so-called information system of the data inboxes. The main task for this information system shall be the creation of a complex database administered by the Ministry of Interior as a guarantor which shall maintain all relevant data, namely about the data inboxes as well as about their users. In this connection it is of utmost importance to say that the *administrator* of the information system of the data inboxes is the Ministry of Interior, whereas the *operator* of this system is a quite different subject, i.e. the holder of the postal license. This issue was inserted to the wording of the Act by a parliamentary draft. Certainly, from the side of the legislator, it is an effort to secure a technical feasibility of the Act. On the other hand, the Czech Post (which is hidden under the expression of the holder of the postal license) itself is not able, as a universal guarantor, to secure the operation of such a complex system. Therefore, the Czech Post, as a submitter, prepared a tender for the supply of the needed

hardware and software from a commercial subject. Up to this point, it remains questionable who shall actually be the real operator of the information system. What is clear at this current stage of the implementation of the act is that both subjects, i.e. the administrator as well as the operator of the information system are responsible for the security parameters of the whole system. For the sake of completeness it is important to say that all particular information, stored within the information system of the data inboxes, is set out in the provision of Section 14 Par. 3 of the Act. Generally it may be concluded that the information system stores all information
concerning the log in to the data inbox and log off from the data inboxes as well as information concerning the dispatching and delivery of the document and *invalidation* of the access data and the *cancellation* of the data inbox. Such a scope of information seems to be proper and, nowadays, even desirable especially in the light of various security risks.

Based on the aforementioned it is suitable to point out that all documents which are delivered to the data inbox in accordance with the Act on the electronic acts will take the form of a data message. To a certain extent it is a pity that the wording of the Act does not provide for a legal definition of a data message for purposes of the Act. A variety of interpretational possibilities of what shall be finally *concretely* perceived as a document delivered via and into the data inbox cannot thus be ignored. For this reason it shall be very important to proceed, as of the efficiency date of the Act, in full accordance with the interpretation rules of the civil code or with the traditional terminological apparatus of the law of information and communication technologies.

7. SEVERAL QUESTIONS ON THE SECURITY OF THE DOCUMENTS DELIVERED VIA THE DATA INBOXES

As addressed earlier, the administrative body concerned with the sector of the security of the data inboxes is the Ministry of Interior of the Czech Republic. The wording of the Act even stipulates (cf. Section 22 Par. 2 of the Act) that it is in power of the Ministry to delete a data message which contains an incorrect format or contains computer programmes capable of causing harm to the information system and subsequently inform the addressee of such an act. Simply said, the data message containing a computer virus or any other unsolicited software (not closely specified by the Act) shall be deleted provided it is detected by the respective technical resources.

However, there arise several more practical problems not dealt with by the legislator. The most fundamental is that if the mechanisms of the information system select such a problematic message, there exist a probabil-

ity almost equal to certainty that the data message (to which the computer virus has been bundled) shall be deleted, whereby the addressee of such a data message will not be anyhow (in respect of any available technical means) provided with the contents of such a data message. The liability for the cleanness (i.e. that the data message is error-free) is lying on the Ministry of Interior, however, this described approach may not ultimately bring about the desired result. Another huge problematic issue is that the user of the data inbox *ipso facti* loses control over the data message itself and is left with only the information that the data message containing the computer virus or the message otherwise infected (according to the findings of the mechanism of the information system) has been deleted. Obviously, the list of (potential) security problems does not end at that and by using more in-depth analysis several more threats can be tracked down which can materially jeopardize the successful fulfilment of the purpose of the Act.

8. AUTHORISED DOCUMENT CONVERSION

When talking about the authorized conversion of the document, it should be noted that further conditions for this shall be the content of the soon-to-be decree prepared by the Ministry of Interior, once it has passed through the internal suggestion process. In this light we can expect several more specifications. But even today it can already be said that this "electronic verification" shall function as follows: the relevant document is transformed via a scanning machine into the electronic version, then it is printed into a physical document and finally a verifying clause is attached to it (legal requirements for this are provided for by Section 25 of the Act). The wording of the Act presumes two types of the authorized conversion – conversion at request and conversion by virtue of holding the office or position (so called authorized conversion *ex officio*). In the first of the above cases the authorized conversion can be performed at offices of public authority which are quite common these days, i.e. Czech POINTs. These Czech POINTs then shall keep evidence of all performed conversions.

The authorized conversion the Act defines in its Section 22 Par. 1: "*The documents authorized shall mean a) the full conversion of a document in a documentary form into a document contained in a data message, compliance verification of the contents of these documents and attachment of the verification clause, or b) the full conversion of a document contained in the data message into a document in a documentary form, compliance verification of the contents of these documents and attachment of the verification clause.*" Probably the most significant part of the Act can be seen in the fact that once the documents authorized conversion has been carried out, the former (original) document and the newly created

document are, from the legal point of view, possible to be fully used interchangeably. In this context one can reckon a large amount of usefulness in everyday life when both documents as addressed have the equal power in terms of their forms as well as effects. Then, by all means, when the corresponding law stipulates the requirement of a written form of a document (typically the procedural laws, e.g. the civil procedure), the electronic document created within the documents authorized conversion shall be perceived as satisfactory for this requirement.

9. WHEN CANNOT THE AUTHORISED DOCUMENT CONVERSION BE USED?

The Act also enumerates the cases in which the conversion cannot be used. In the majority of cases it is an impossibility *ipso facto* and *ipso iure* (please see Section 24 Par. 5 of the Act). For illustration attention can be drawn to the situation when a particular document is not in documentary or electronic form (for instance it is situated in another physical medium), a document is indeed in a documentary form but its uniqueness cannot be substituted in anyway(e.g. identification cards, passports or other documents of similar nature), a document whose truthfulness may be limited (e.g. the document contains some cutouts or pen dashes etc.) or a document which contains some plastic elements as well as documents which have already been created by the documents authorized conversion. In all above cases the use of the documents authorized conversion is not acceptable and prohibited by law.

Another issue which should be borne in mind is the fact, redundantly reiterated by the legislation, that by using the documents authorized conversion, the contents of any particular document are not anyhow confirmed or approved, i.e. the particular data are not confirmed in terms of truthfulness and correctness. The contents of the document are fixed only in terms of completeness. Moreover, by using the documents authorized conversion the accordance of the data contained in a particular document with the applicable legal order of the Czech Republic is not considered in any way to be inspected or approved.

10. SOME AILMENTS AND PROBLEMS (POTENTIALLY) BROUGHT BY THE ACT

What were previously dealt with were the positive aspects of the wording of the Act, but here one should consider several drawbacks of the Act which cannot be omitted.

Probably the biggest problem of the Act is the insufficiently stated regime of the security of the documents delivered to the data inboxes. This

question was dealt with above and therefore it can only be noted that the Act, in this context, could not handle the issue of deletion of a document (details) after it has been marked as risky or dangerous with a threat of a computer virus by the information system. Problems connected with the access to the data inbox were also pointed out (especially with regard to plurality of subjects of the entity for which the data inbox was created). A rather big problem may be represented by the fact that the capacity of a data message has a set limit (currently 10 MB). No responsible person can now persuasively argue what would happen if a subject wishes to send a data message that exceeds the 10 MB limit. As a representative of the Ministry says, such a big data message will not be able to be dispatched. In this context, implementation of a system for the splitting of big messages would definitely be of vital importance.

In connection with the data inboxes several more risks start to appear. The wording of the Act provides for many legal relations, nevertheless, it does not stipulate a regime for legal regulation of the relations *causa mortis* as to the existence of the data inbox. Simply said, until now the question of the disposition with the documents remains unsolved when the person for whom the data inbox was created dies or has been declared dead. Accordingly, the same problem appears with closure of a company without a legal successor. Thus, it is well possible that if the person had some receivables against some other subjects (e.g. the employees) which could be claimed before a court (subsequently enforced by the court decision), it would be unclear how it would be possible to deliver the documents to such a company and what would be the further practice of the corresponding state authority involved.

Another problematic issue is the case when a data inbox was created for a physical person to whom the particular documents, *inter alia*, decisions of public authorities as well as court decisions were delivered. Even a court decision awarding a sentence to a physical person for a committed offence is delivered to such an inbox. The question which remains unsolved then is what would be the actual significance of a court decision granting a pardon to a physical person when an electronic decision in the data inbox created for such a person is still present by which this physical person was granted the sentence. It is not without analysis, whether the wording of the Act, provided it is stated in this way could not be, *cum grano salis*, in contradiction with constitutional or civil instruments, for instance the right to privacy.

The next disputed part of the Act is its financial side. Naturally, for every particular breach of the provisions of the Act the responsible public

authority may, within its discretion in an administrative procedure, award a fine. Irrespective of these fees the Act itself does not count on any further fees for the creation of the particular type of data inbox. However, should the case be otherwise, an obligation of contract could be reached, i.e. a situation where a large number of subjects (for whom the creation of the data inbox is prescribed by the wording of the Act as mandatory) would be obliged to pay the fee for the creation of the data inboxes. This issue might then have an even deeper aspect – monopoly position when charging this fee. Another issue which has a direct relation to finance is the following fact. The state authority is obliged to provide the customer, most probably via the abovementioned CZECH-POINTs, the service of the authorized document conversion. On the other hand it is questionable whether the price of the data carried (e.g. a DVD disc) shall be included in the price for the data conversion. Up to this point in time, it has been impossible to gain a satisfactory answer from the competent persons.

11. CONCLUSION

The questions on electronic legal acts are not new in the Czech legal field, however, these issues are by their nature somewhat unique. To summarize, the new adopted Czech Act on electronic acts and documents authorized conversion amends the legal milieu in a desirable way. What still remains unclear is the question of how the real implementation of the provisions of the Act in practice will be successful. It can be concluded that particular legal elements of the data inboxes bring practical positives for physical persons as well as for legal entities. Those who wish to communicate with state bodies effectively, quickly and without the necessity to have a secured electronic signature shall benefit most from the wording of the Act. The largest amount of use can be expected in the day to day practices of the corporate entities when they are in contact with state authorities. Nevertheless, the Act does not manage to avoid several ailments which sometimes follow new laws. It shall be the question of practice as well as further legislative specifications *de lege ferenda* to what extent it will be possible to fulfill the purpose of the Act and to adapt it as much as possible to practical use in everyday life of the subjects concerned. From the *pro future* perspective it will not be without interest to monitor how the Act shall work with the electronic form of (court) decisions (especially with their delivery) or with electronic filing rooms and electronic archive systems. Currently, with regard to the actual wording of the provisions of the Act and without the amendment to the Act, it cannot be declared that the Act is fully effective for the electronic justice system.