Dulčić, Katerina

Conference Paper

New Technology User Liability for Data Loss and Damages

Provided in Cooperation with:
IRENET - Society for Advancing Innovation and Research in Economy, Zagreb

Suggested Citation: Dulčić, Katerina (2015) : New Technology User Liability for Data Loss and Damages, In: Proceedings of the ENTRENOVA - ENTerprise REsearch InNOVAtion Conference, Kotor, Montengero, 10-11 September 2015, IRENET - Society for Advancing Innovation and Research in Economy, Zagreb, pp. 303-309

This Version is available at:
https://hdl.handle.net/10419/183662

New Technology User Liability for Data Loss and Damages

Katerina Dulčić
Polytechnics Nikola Tesla Gospić, Croatia

Abstract

Information technology is spreading in all fields of our lives. We use new technologies for many purposes, but many of us are not willing to learn more than necessary basics. The author elaborates some of the legal cases that were discussed in courts, and that show the responsibility of the technology user for not applying essential security measures. Jurisprudence has determined that the level of security should be different for various types of data, depending on how sensitive information the subject is processing. It is hard, but needed, to elaborate the cost and benefit analysis in accordance for application of advanced information technology. Nevertheless, security of data could be expensive; it is always cheaper than damage reparation. The imminent risks are those of data loss and modification, but also of data steeling by interested subjects. New instruments give a great input in health and education services, but also the data they are elaborating are of great interest for predators, but also for data subjects. The use of cloud and grid technology is very productive for these fields, but, considering the risks, those should be used wisely and with great with. Goal of the paper is to examine the legal obligations of personal data storage in EU and general conditions of cloud storage services. The legal texts are going to be examined and analysed and correlated with legal obligations.

Keywords: Liability, Security measures for information technology, Data subject, Sensitive data, Grid technology, Cloud data storage.
JEL classification: K130

Introduction

Personal data include important parts of our private life, not all wanted to be known to others. Automatized processing of those data is great danger of our privacy. Council of Europe noticed the problem already in 1981, and created the Convention of for the Protection of Individuals with regard to Automatic Processing of Personal Data. In 1995 European Community regulated the personal data market, trying to protect the rights of individuals.

New information technologies allow faster processing of major quantity of personal data, and it is accessible by many subjects. This article shows that, nevertheless, the technology is accessible; it should be used carefully considering all the risks involved.

The history of personal data protection in Europe is going to be given, and legal definitions of personal data, as well of special categories of data are going to be explained. Also the legal definition in international legislation of liability for personal data is going to be examined also the contracts with third party and their liability.

Methods

The actual legislation on personal data protection in European Union has been examined. Nevertheless, the Council of Europe Convention is from 1981, it is still valid legal document in European countries. Also, there have been initiatives to change EU Data protection directive, it is still the same from 1995.

Their legal requirements have been compared with the general conditions and offers by cloud storage services, actually offered.

Results

Personal data protection

European Union has introduced Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal L 281, 23/11/1995, P. 0031-0050). The main scope of this Directive was to regulate the data market, but also to protect individuals and their right to privacy. In its introduction, it states that the principles provided by the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data should be respected.

Considering the state of technology in 1981, we can't expect the rules to be precise, especially for the data storage and management. Article 7 states: "Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination." The dangers of automatized data processing were seen already over thirty years ago. And the priority of protecting the individuals has been settled.

In 1995, there already was a "data market". So, European Community regulated it with its Directive, with a double scope: first to protect individuals of unlawful personal data management, and second to liberate the data market within the Community, nowadays within the European Union.

All personal data protection provisions are limited only at data about natural person, data on companies and other juridical persons, are protected by industrial secrets, but, if they are legally obtained, they can be freely elaborated. All personal data on natural persons should be always controlled by the data subject. The Directive does not say it explicitly, but with article 7 that determines the criteria for making data processing legitimate, and primary criteria is data subject's unambiguous consent for data processing. Non explicit consent is accepted in case of contracts, if personal data are vital part of contract performance, or it is legal obligation to collect such personal data to perform the contract. Other exceptions are vital interests of data subject and public interest, and controller's legitimate interest. In order to allow free development of data collecting and their commercialisation, the exceptions are wide. (See: Kuner, 2007, p.27-60, 114-135, Korff, Brown, 2010, p. 22-24)

Special categories of data

The European Council Convention determines special categories of data in its article 7. They are data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, and also data relating to criminal convictions. These data are data concerning especially sensitive part of individual's life, and these are supposed to stay private. Also, revealing such data on a subject could cause greater damage to that person.

EC Directive has extended the definition of special categories of data. In Article 8 it defines them as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and also data relating to offences, criminal convictions or security measures.

In both acts, it is forbidden to process these personal data, except with data subject's consent or it should be permitted and regulated by the law. (Bianca, Busnelli, 2007, p. 616-648, Solve et. al., 2005, p. 346-390)

Data quality

Most important quality, of the collected personal data, is that it should be accurate and correct.

Article 5 of European Council Convention states:

"*Personal data undergoing automatic processing shall be:*
obtained and processed fairly and lawfully;
stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
adequate, relevant and not excessive in relation to the purposes for which they are stored;
accurate and, where necessary, kept up to date;
preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."

Also, the article 6 of European Community Directive provides:

"*1. Member States shall provide that personal data must be:*
(a) processed fairly and lawfully;
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
2. It shall be for the controller to ensure that paragraph 1 is complied with."

The second paragraph of this Directive is the one that gives a great burden to the data controller. It doesn't mean that controller has to do everything about data processing, but it means that the controller is responsible to the data subject.

In order to maintain accuracy of collected data, the controller must limit access to the data, should consider the durability of storage media and have strict regulations how the data are collected and the way they are processed.

The control of the input of data is a method that already exists. Even in the "old paper databases", the input of data had to be controlled. The procedures for the control of collected data have been implemented for ages, and it is easy applying the analogy method to control the data inserted in a computer in the same way it has been done for data written on paper.

The rules for documents storage are not applicable for the electronic records. Therefore, new rules have to be made.

Strict liability for quality of data

The automatized data processing is considered a dangerous activity. The fact is that by automatized and electronic data processing can generate automatized decisions that can seriously affect data subject interests. Unauthorised divulgation of data can harm material and moral sphere of subjects. Recent example is the millions of loss by Jason Pierre-Paul caused by divulgation of his medical records. As a professional sportsman his health is viable part of his contract. Health records should have been protected better, not to allow third parties to access them. The moment a journalist got the possession of it, it was his professional right and duty to publish it and great damage has been caused.

For dangerous activities person that does it, especially as a professional activity, for all damage caused, they are responsible regardless of the guilt. It is important to prove that the damage is caused by that activity. The data controller can be exonerated if proofs that damage has been caused by sole damaged person, by third person, or by occasions that couldn't be influenced, predicted and prevented (*vis maior* – major force). (Gorenc, 2014, p.1749-1767)

The European regulations are implicitly concerning strict liability for personal data protection. By forming the paragraph 2 of article 7 of the Directive as a sole obligation of the controller to give guaranty for the quality of the data, there is no possibility to escape responsibility by implementing the guilt as necessary element of responsibility.

As Modesti (2003) accurately describes in his article, courts have accepted it as a rule. Data controller is responsible for inaccuracy of collected data, its unauthorised divulgation and loss.

This is a great financial burden for data controller. On one side, unauthorised access and use of data can gain profit to the person that obtains data, and on the other side, it is necessary to allow access to all people that need these data. Therefore it is necessary to allow web access to data, but to protect it with adequate information technology. This requires highly professional personnel that is not always possible to have. Therefore, the controller often uses third party services. (see also: Kuner, 2007, p. 191-218; Bianca, Busnelli, 2007, p. 682-684, Simitis, 2006, p. 623-645)

Contract with the third party

The European Council Convention does not have any regulations about engaging third party as effective data processing executor. It is logical considering the fact that it was made in 1981, when the IT industry was in its beginning. There were no commercial data processors on the market that offered their services to legally obliged electronic data controllers.

European Community Directive's scope was to regulate the existing data market. Therefore, it defines the processor as "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller" (art. 2, p. 1e of EC Directive). With the scope to protect the individual, the European Community Directive regulates especially confidentiality of personal data that are in possession of the processor. Its article 16 states: "*Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.*"

This regulation does not exonerate the controller of its responsibility; this is just obligatory part of any personal data processing contract. Whether it has been or has not been explicitly stipulated, the national loss of the Member States should include this clause.

Within article 17, the European Community Directive defines the security measures for the data processing. It requests of the Member States to provide constantly updated technical propositions for the data processing. Considering the fact that information technologies change on almost daily basis and considering the threats that are growing proportionately with the technology and the value of data national regulations for minimal standards of data protection should be constantly renewed. Also, the Directive requests that measures should be applied considering their costs and the importance of data that should be protected. The problem is that special categories of data are usually processed within non-profit organizations and these sensitive data are the most valuable on "black data market". Medical institutions elaborate most sensitive data and data technology is not their primary investment interest. Furthermore, data on children are extremely interesting to some not nice people and also schools have lack of money and other priorities.

To avoid constant renewing and copying of stored data, external storage could be acceptable and appealing. The contract with such third party, as EU regulations require, should be in written form and also should include confidentiality clause and should allow the controller to obtain information on directly involved processor's employees on this contract. It would be wise to predict the proceedings for eventual case of damage to data that causes damages to the data subject. For the data subject, the only responsible subject is the controller, but in case it is the processor's guilt that caused the damage, the controller has the right to obtain reparation for the damage paid to the data subject.

Cloud storage and processing could be attractive for its low cost and simple use from unlimited number of computers. It simplifies data access, but in the same way it facilitates it to the authorized personnel, it is much simpler for the hackers to attack it. Considering the EU regulations, another important fact should be examined when contracting cloud storage. It is important whether the server is situated within EU or not. The principle settled with the Lindqvist case (2003) considers it export of data if storage of the data is outside EU.

Many consumers orientated cloud companies have their privacy policy, but serious ones include disclaimer for damage or loss of data without their fault. (see: Kesan, 2013, p. 445). The majority of cloud general conditions are not adequate for personal data protection. This does not mean that it is forbidden to use cloud technology for personal data processing, but it requires negotiation about use of servers, use of security measures and employees included in the process.

Discussion

As examined material is mostly legal texts, there is hard to imagine the praxis. But, considering the strict liability for personal data quality, and personal data protection, storage of data is a very important part of it. Towards the data subject, the only responsible person is the data processor, the natural or legal person that collects the data and that processes them. It is legal to contract a third party that is doing the actual process, but it is very important not to accept a contract with general conditions, but to elaborate the responsibility clause. Therefore, in case of lost or modified data, there could be the right to get the retribution from the actual processor, in case they do not apply required data protection measures.

Information technology is rapidly progressing, and to regulate it for a longer time, legal requirements are not precisely defined. They only mention "adequate" measures. The definition of adequate should be given by the courts, but also by technical expert opinions. The lack of finalised court decisions, because, cloud storage is new technology, limits the precise requirements for data protection. Future decisions should be examined to see what is needed in precise writing of storage contracts.

Conclusion

Data management is important and viable part of today's IT industry. In intention to simplify procedures many legal regulations require the use of electronic records. They are easier to control and examine, but they are much more complicated to protect. If pupils changed their paper school records and registers, these unauthorised accesses were visible immediately. Alteration of computer records is not visible prima facie. Also, the whole file with uncountable number of data can be copied in short time, and the owner can continue to use them, without noticing the intrusion, and get aware in the moment when these data are unlawfully published on the internet, and then it is already too late.

The purpose of this research is to examine whether it is possible to reduce the storage costs by cloud computing. It is useful because it is physically distant from the processor, and should be safe in case of natural catastrophes. But there is a great risk to sign contract with someone you don't know. So some guidelines for the contract of data storage have been given.

Therefore, all the risks should be carefully examined and evaluated, and in accordance with results valuable decisions should be made, avoiding momentary savings that can cause greater damage in future, and without the right to obtain the reimbursement from responsible person.

References

1. Bianca, C.M., Busnelli, F.D. (2007) "La protezione dei dati personali" ["Protection of personal data"], CEDAM, Padova
2. Case law (2003) "Bodil Lindqvist, C-101/01", 6 November 2003.
3. Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data
4. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal L 281, 23/11/1995, P. 0031-0050)
5. Gorenc, V. et al. (2014) "Komentar Zakona o obveznim odnosima" ["Commentary on the Obligation Law"], Narodne Novine, Zagreb
6. Hammond, T. (2015) "Research: 68% report cost is biggest data storage pain point", available at: http://www.techproresearch.com/article/research-68-report-cost-is-biggest-data-storage-pain-point/ (accessed July 5th 2015)
7. Kesan, J. P., Hayes, C. M., Bashir, M. N. (2013) "Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency", Washington & Lee Law Review, Vol. 70, pp. 341-472.
8. Korff, D., Brown, I. (2010) "Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments", European Commission, available at: http://ssrn.com/abstract=1636706 (accessed July 5th 2015)

9. Kuner, C. (2007), "European Data Protection Law, Corporate Compliance and Regulation", second edition, Oxford University Press.
10. Modesti, G. (2003), "La responsabilità oggettiva e lo svolgimento delle attività pericolose ai sensi dell'art. 2050 Codice civile, con particolare riferimento al trattamento dei dati personali alla luce del decreto legislativo n. 196/2003", ["Strict liability and the execution of dangerous activities in aspects of art. 2050 of the Civil code, with the particular aspects of processing of personal data in accordance of legislative decret n. 196/2003"], available at: http://www.diritto.it/docs/22176-la-responsabilit-oggettiva-e-lo-svolgimento-delle-attivit-pericolose-ai-sensi-dell-art-2050-codice-civile-con-particolare-riferimento-al-trattamento-dei-dati-personali-alla-luce-del-decreto-legis (accessed May 15th 2015).
11. Mystral, E. (2015), "HIPAA Does not Apply To ESPN, You Freaking Idiots, Above The Law, Redline", available at: http://www.atlredline.com/hipaa-does-not-apply-to-espn-you-freaking-idiots-1716847857 (accessed July 8th 2015).
12. Simitis, C. (2006), "Bundesdatenshutzgesetz", ["Federal Data Protection Law"], Frankfurt, Nomos.
13. Solve, D.J., Rotenberg, M., Schwanrtz, P.M. (2005), "Information Privacy Law", New York, Aspen Publishers.

About the author

Katerina Dulčić was born on 1972. Graduated law at Law Faculty of University of Rijeka, and at the same faculty obtained master degree. Her interest is law regulating new technology and civil law. She works as civil law lecturer at Polytechnic Nikola Tesla in Gospić. Author can be contacted at: **katerina.dulcic@ri.t-com.hr**