DATA PROTECTION AND THE RIGHT TO PRIVACY IN THE COMPUTER AGE – THROUGH LAW ENFORCEMENT OR THROUGH EDUCATION?

Andrej Cvetkovski

Assoc. Prof. Dr., Mother Teresa University, North Macedonia, acvetk@gmail.com

Abstract

In the age of rising power of the electronic information and communication technology, processes of data aggregation and concentration about people are inevitable. Humans are slowly but surely losing control over computers and similar "thinking", artificially intelligent machines. Wherever centralized information systems for personal data are established, there are centers of strong control over life and activities of everyone. The bureaucrats and technocrats are thrilled by such possibilities. In the data centers they see new automated management tools and require detailed data collection for every human activity, however insignificant. The humanists, on the other hand, are distrustful of that novel management trend. They see it as a means of enslaving the humans.

In this paper we analyze the growing dangers of the growing capabilities for storage and processing of personal data in the triangle consisting of the technological developments, the drafting of data protection laws and the citizens. We argue that, in the long run, the only way out of potential abuse of the right to privacy as a human right is not through new data protection laws, supervisory instances, data policing and enforcement, but through education of all players in that triangle on all aspects of data protection and the right to privacy in the computer age.

Keywords: Privacy, Data Protection Law, Politics and Ethics.

1. INTRODUCTION

The roots of freedoms and rights are found in ancient Greece. However, the freedoms and rights in the Greek polis-states, the Roman Empire and the Middle Ages were not exercised in the modern sense of their meaning. In those days there were relations of physical slavery, and freedoms and rights were enjoyed only by certain privileged classes or groups of citizens.

In contemporary context, freedoms and rights are a matter of relations within a state and are subject to the regulation of internal law. But at the same time, they are subject to regulation in international law. In 1946, the United Nations established a commission to draft an international human rights charter. In 1948, the UN adopted the Universal Declaration of Human Rights. In 1966, the UN adopted the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights. Regional documents for realization and protection of human rights and freedoms have also been adopted. A more important document is the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed on November 4, 1950 in Rome and enacted on September 3, 1953.

The international community, through international and regional acts, seeks to standardize human rights and freedoms and to build control mechanisms for their realization in practice. The control mechanisms are realized through (1) monitoring the realization of freedoms and rights and imposing sanctions against a specific state for violation, and (2) institutionalized control mechanisms, such as the European Commission of Human Rights and the European Court of Human Rights functioning on the basis of the European Convention for the Protection of Human Rights and Fundamental Freedoms of 1951.

Personal freedoms and rights refer to the protection of the physical and spiritual integrity of the human being and his equality with other people. From the aspect of international law, one of the generally accepted rights is the right to privacy. The right to privacy means that a person, based on his or her own understandings and criteria, exercises the right to private and family life and to reputation and dignity. The authorities must not interfere in the exercise of this right, unless such interference is provided by law and is a measure necessary in a democratic society, which is in the interest of national and public security, the economic well-being of the country, the protection of order and the prevention of crime, the protection of health and morals or the protection of the rights and freedoms of others.

The collection, registration, storage, inference and disclosure of information relating to a person are always a potential ground for violating the right to privacy. In our age of electronic information and communication technology, processes of data aggregation and concentration about people are, however, inevitable. The identification of these processes as detrimental to the right to privacy is usually difficult to carry out until it is too late. Humans are slowly but surely losing control of computers and similar "thinking" machines, as they are accepting the new normal with each step forward.

Collection of accurate data and inference of information from it is a prerequisite for any rational human activity. Here, however, the discourse here is not about just any data. It is about personal data. Wherever organized centralized information systems are established, there are centers of strong surveillance and control over life and activities of everyone. Bureaucrats and technocrats of the controlling state are thrilled by such possibilities. They see a new, must-have management tool in the data control centers. They require such management for every human activity, however insignificant. The humanists on the other hand are distrustful of that novel management.

Those in power, or more gently put, the authorities, react as the chosen few to manage the collection and use of data about people. They feel empowered when they can, with the help of machines, record and control peoples' private lives. As if intoxicated by the possession of this digital, immediate power, they offer their strong arguments to appease the public, and to explain the importance of control machinery. Their explanations usually boil down to the following boilerplate: for the sake achieving new, unprecedented levels of efficiency and rationality in decision making, providing fast digital access to administrative services and facilitating the communication of the citizens with state bodies, public services and other organizations, the new important area of digital informatics is being developed. This goes along with the rise of the professions of data scientists and researchers, with whose help personal data are stored, processed and summarized. All this is to the benefit of the citizens and therefore justifies large expenditures of budget money for modernization and maintenance of digital data technology and hiring more data processing employees. But before everyone knows it, human privacy is irreversibly trapped in the big computer.

Storing data related to personal and family life in centralized electronic data marts is causing increasing concern among the aware people. With the development of advanced computer hardware and software, this trend acquires dangerous dimensions. Humans together with all of their privacy are put into a ubiquitous computer. What significance can personal freedoms and privacy on personal and family life have if they are bar-coded and replicated in thousands of computers, which by interconnecting and joint processing can infer every detail about people? The authorities, although not convincing enough, continue to try to convince the public: there is no danger. The constitution and the laws guarantee and protect privacy.

In order for a law to be able to effectively protect relations, phenomena, events, or situations, first and foremost, these need be precisely defined as objects of protection. If the object of legal protection is the privacy of personal and family life or private life, then the foremost problem becomes how to define it. Private life has many facets: individual activities, family relationships, social activities, communication with friends, communications with colleagues and collaborators. Each of these facets of life has political, legal, economic, biological and philosophical aspect. Can all of these be defined and specified as the object of legal protection?

Despite all the difficulties in defining it, the state authorities claim to have solved the problem legally – with a general law and detailed laws on personal data protection. The legislation on this problem, however, is faced with a number of difficulties. Some legal solutions that are crucial in the protection of personal data are worth

considering once again.

2. THE ANTAGONISM OF INTERESTS OF PRIVACY AND STATE

The state, with the help of computers and amenable to its own laws, creates many repositories of personal data of its citizens: records of births, marriages and deaths, citizenship, ID and driver's license cards, employment and social security, healthcare, residence, military service, retirement, cadaster and real estate, criminal records, tax records, etc., and the list is growing day by day.

With the help of computer networks, these data are fused together and provide answers to many indecent questions about people's private lives. The state, in its interest, will keep collecting personal data of the citizens anyway. Professional researchers of human lives will do their job at the behest of the state and aided by data processing machines. And they will have little mercy or empathy for the subjects at hand. Who can limit or prevent this? The problem of this relation seems to be unsolvable in a way satisfactory both for the person's private life and for the state.

The collection of personal data is done on the basis of the principle of immediacy: personal data are collected directly from the person to whom they refer. Does the citizen have the right to request any personal information not to be registered "for personal reasons"? There is no such right, because personal data are collected mechanistically, on the basis of law, and the law mechanically applies to everyone. So the citizens have the right only to find out that their private lives are dominated by the state interest and against their own interest.

The right to inspect the data collections is only a consolation, and not a solution to the breach of privacy that the state concocts for the citizens with the help of computing machinery. Worse, legal possibilities are created for one person to give out personal data about another person and for data to be copied from already established datasets into new datasets. This further obscures the possibility of insight. The citizens will seldom be informed that a new dataset has been created based on collections established earlier. State authorities are not obliged to make public their actions on databases of records.

Collections can be formed both on the basis of facts and on the basis of assessments and opinions. Will the citizen be able to inspect these latter collections compiled based on assessments and opinions, or will that opportunity be curtailed for the boilerplate reasons of security and defense of the country, conducting criminal proceedings, protection of economic interests, protection of health and human life or environmental protection? When there are no clear provisions in law for such subtle situations, every request for inspection can be rejected for some arbitrary contrived reason.

For specific uses of personal data such as statistical or scientific research, educational or other similar purpose, the maintainer of records is obliged to submit the personal data in a sanitized way i.e. in a form that does not allow identification of a particular person. It cannot be guaranteed however, that sanitized data for these specific purposes are harmless. By unifying and matching several sets of sanitized data, one can infer a lot more information than it is contained in the individual datasets. Therefore, the added requirement for sanitization of data before sharing does not add much more difficulty to the data processing entities for further legal use and abuse of personal data.

3. THE STATE THREATENS, PROTECTS AND CONTROLS

In an effort to mitigate the problem stemming from the antagonism of privacy and state, another player is added to the triangle consisting of the government, the state computer and the public: A key player in the protection of personal data for citizens becomes the state supervisory body for data protection – a higher body designated by law to oversee those who handle collections of personal data. The supervisor is the controller of the computer, its contents and the ways in which data are obtained and used. The supervisor is therefore a mediator between the government and citizens in personal data protection.

Both the supervisors and the data processors are government administrative bodies. Inspection over the implementation of the organizational and technological procedures and measures for personal data protection is performed by the administrative body responsible for the affairs of informatics and the information system, which is also a government administrative body.

Therefore, the problem arises: Who threatens whom and who protects whom? Who controls whom? It is the state government that threatens, protects and controls, all at the same time. The situation is ambivalent. Can one government body successfully control another government body? Further, can one government body successfully mediate between another government body and the citizens? Or can the government, as a supervisory body, protect the private lives of citizens from the dangers posed by the computer when it is abused by the same government?

It is hardly possible for bodies of the same rank to establish supervision over each other in the abuse of power. Which government has ever protected anyone from itself? "The notion of leaving the protection of individual privacy to Government officials has been compared to asking the fox to protect the chicken coop. But six months ago – when the most intensive investigation ever focused on a nominee for the Vice Presidency was directed at me – I awakened to the privacy issue in a very real and personal sense. I was one of the chickens.", spoke in 1974 the then vice president of the United States Gerald R. Ford at the Chicago Medical Association Convention.

The state authorities with their data protection laws do not provide better guarantees on personal data protection by introducing a state supervisory instance. In the triangle whose vertices are the government, the state computer and the people, the only hope of decent oversight off the protection of personal data can be placed in an independent control and supervision instance, that is, defined as an independent commission of experts.

And one more problem of the triangle government – computer – citizens, that is rarely considered. Computer repositories of personal data for citizens are an inevitable reality for both citizens and the government in the age of computerization. What would happen to those warehouses in a large-scale emergency, or an event such as a coup or occupation? The law on personal data protection ought to be drafted to precisely account for such situations. The crux of the problem is how to prevent a wild government from accessing hundreds of repositories containing millions of details on citizens' private lives. Emergencies require appropriate regulation and practice.

4. THE NEED FOR EDUCATION IN DATA PROTECTION ETHICS

From the above argument, it seems that waiting on the state alone to protect the right to privacy of its citizens with its laws is largely a bootstrapping logic. Personal data protection laws in many countries around the world are only scraping the surface of these problems. In the long run, potential abuse of the right to privacy as a basic human right is not to be achieved solely through new or more detailed data protection laws, supervisory instances, data policing and enforcement, but also through education of all players in the personal data triangle on all aspects of data protection ethics and the right to privacy in the computer age.

It is to be recognized that protecting the right to privacy of the citizens, at the same time means protecting the right to privacy of all individuals in the data triangle: not only the public, but also the participants of the government and the data collection and processing specialists. Everyone's privacy rights are at stakes, without exception. When law fails, it is the higher principles of ethics and morality that can break the circular spell and bring the behavior of each individual to the moral level necessary to cope with the challenges of data protection in the computer age.

Ethics have often been falsely equated with mere behaving in accordance with the law, social customs and religious values. It is the problems ensuing from the collection and processing of private data by the state, however, that vividly emphasize the distinction between ethics and law. While laws are structured as sets of rules to regulate the society with little regard of the individual differences, ethics are guidelines of moral values centered on the personal behavior, which is in turn closely related to personal data and the right to personal privacy.

The ethical dimension of data protection, then, shall be incorporated in the process of drafting data protection laws from the very onset. Data protection ethics shall be introduced as a major topic in the system of compulsory education. The goal of data protection and data privacy education shall be to facilitate universal, widely accepted understanding of the principles of purpose limitation, data minimization, storage limitation, integrity and confidentiality, and accountability as underpinnings of the mechanisms for protection of the right to privacy in the computer age of today.

5. CONCLUSION

In the age of rising power of the electronic information and communication technology, processes of data aggregation and concentration about people are inevitable. The humans are slowly but surely losing control over computers and similar "thinking", artificially intelligent machines. Wherever centralized information systems for personal data are established, there are centers of strong control over life and activities of everyone. The bureaucrats and technocrats are thrilled by such possibilities. In the data centers they see new automated management tools and require detailed data collection for every human activity, however insignificant. The humanists, on the other hand, are distrustful of that novel management trend. They see it as a means of enslaving the humans.

Are computers of the government making the citizens free or are they abusing the citizens' freedoms and

rights? Citizens are caught in the computer nets of the state. The space and the possibilities for free swimming become ever smaller. The significance of personal freedom for the human being, speaking at the mildest, diminished in these data sharing networks. The remedy proposed by the state seems a mere placebo for calming the worried down – data protection laws that have small odds to function well in reality.

In this paper we analyzed the growing dangers of the growing capabilities for storage and processing of personal data in the triangle consisting of the technological developments, the drafting of data protection laws and the citizens. We argued that, in the long run, the only way out of potential abuse of the right to privacy as a human right is not through new data protection laws, supervisory instances, data policing and enforcement, but through education of all players in that triangle on all aspects of data protection and the right to privacy in the computer age.

REFERENCE LIST

General Data Protection Regulation (EU) 2016/679.

Law on Personal Data Protection, Official Gazette of the Republic of North Macedonia, No. 42/2020.

Paul, Richard; Elder, Linda, The Miniature Guide to Understanding the Foundations of Ethical Reasoning. United States: Foundation for Critical Thinking Free Press, 2006.

Ford, Gerald R., Remarks of Vice President Gerald R. Ford at the American Medical Association Convention, Chicago Illinois, June 1974.