VERSITA

10.2478/v10103-011-0030-2

ZOFIA WYSOKINSKA[*], RADOSŁAW DZIUBA[**]

Social Aspects of New Technologies – the CCTV and Biometric (Framing Privacy and Data Protection) in the Case of Poland

Abstract

The purpose of this paper is to review the institution responsible for the protection of personal data within the European Union and national example - Polish as a country representing the new Member States. The analysis of institutional system - providing legal security of communication and information institutions, companies and citizens against the dangers arising from the ongoing development of innovative new technologies in the European Union and Poland. This article is an attempt to analyze the possibility of using security systems and Biometry CTTV in Poland in terms of legislation. The results of the analysis indicate that, in terms of institutions Poland did not do badly in relation to the risks arising from the implementation of technology. The situation is not as good when it comes to the awareness of citizens and small businesses. This requires that facilitate greater access to free security software companies from data leakage or uncontrolled cyber-terrorist attacks. With regard to the use of security systems, CCTV and biometrics, Poland in legal terms is still early in the process of adapting to EU Directive. The continuous development of technology should force the legislature to establish clear standards and regulations for the application of CCTV technology and biometrics, as it is of great importance in ensuring the fundamental rights and freedoms of every citizen of the Polish Republic.

* Ph.D., Full Professor at the University of Łódź

** University of Łódź

Introduction

This article is an overview[1] of institutions and legal regulations on the European and national level guaranteeing the security of communications and information of businesses as well as citizens. Its objective is the undertaking of efforts to perform a basic analysis of the institutional and legal system in terms of guaranteeing the security of the above entities against threats on the part of a progressing world. The average citizen of the European Union does not know what is happening with his or her personal date when making airline reservations, opening a bank account, or uploading a photograph to a social network service—and all the more so, has no knowledge of how to permanently remove it.

Monitoring information about oneself, access to personal data, changing such data or eliminating it are all fundamental rights that must be guaranteed in today's world of digital media. It is for this reason that it is important for the administrative bodies of the European Union, individual countries, and regions to guarantee security to as high a level as possible as well as for them to propagate knowledge on the subject. The intention of this paper is also a basic analysis of problems facing business entities in connection with technological progress and the potential for stopping threats.

To a significant extent, this article fits in with the COM(2010) 609 Communication from the European Commission on the strategy intended to protect personal data in all areas of policy, including the enforcement of the law, while at the same time decreasing bureaucracy for companies and guaranteeing the free flow of data in the European Union. As a result of public consultations, the European Commission has taken it upon itself to modify legislation in this field by the end of 2011. It is also for this reason that this article is intended to foster further discussion on possibilities for better regulation and legal solutions aimed at improving security against threats stemming from technological progress.

---

[1] The base of this article are results of research done by the Polish team of the University of Lodz within the international Project organized within the 7th Framework Programme of the EU. Project full title: *Privacy Awareness through Branding of Security Organisations*; Grant agreement no.: *230473;* Technical University Berlin (coordinator of the Project); Interdisciplinary Center for Technology Analysis and Forecasting at Tel Aviv University; Turku School of Economics, Finland Futures Research Centre ; Lancaster University, Department of Organization, Work and Technology; Vanderbilt University, Department of Human and Organizational Development and University of Lodz. The aim of PATS is to increase privacy awareness across various sectors, from firms to government agencies, focusing especially on the development and use of Closed Circuit Television (CCTV) and biometrics. http://pats-project.eu/

Part I. Legal and Institutional Aspects

1. European Institutions Guaranteeing the Information and Communication Safety of Businesses, Companies, and all European Union Citizens

Talk of security within the framework of the European Union began at the moment of its establishment. Article 5 of the Treaty Establishing the European Economic Community (Treaty of Rome), signed on March 25, 1957, provided the basis for regulating this matter, so important to the unity of the Community.

"Member States shall take all appropriate measures, whether general or particular, to ensure fulfillment of the obligations arising out of this Treaty or resulting from action taken by the institutions of the Community. They shall facilitate the achievement of the Community's tasks. They shall abstain from any measure which could jeopardize the attainment of the objectives of this Treaty"[2].

General conditions guaranteeing the security of the European Union seen as a whole are contained in the following documents:

- Treaty on the Functioning of the European Union, Article 16,
- Charter of Fundamental Rights of the European Union, Article 8,
- Directive 1995/46/EC of the European Parliament and of the Council,
- Directive 2000/31/EC of the European Parliament and of the Council,
- Directive 2005/58/EC of the European Parliament and of the Council,
- Directive 2006/24/EC of the European Parliament and of the Council, and
- Directive 2009/136/EC of the European Parliament and of the Council.

The Data Protection Directive of 1995 is a milestone in the history of the security of personal data in the European Union. The Directive encompasses two of the oldest and equally important aspirations in the process of European integration. On the one hand, there is protection of fundamental rights and fundamental liberties of the individual, especially the legal basis for the protection of data. On the other hand, there is the implementation of the internal market, which in this case means the free flow of personal data. After fifteen years, this dual purpose is still in effect, just as the principles written into the

[2] Treaty Establishing the European Economic Community, 1957, Article 5, Journal of Laws of the European Union, EUR–LEX, http://eur-lex.europa.eu/pl/treaties/index.htm#founding, November 20, 2010.

Directive remain in force. However, the rapid development of technology coupled with globalization have resulted in far–reaching changes to the world around us, ushering in new challenges in the area of personal data protection[3].

Vice–President of the European Commission Viviane Reding, European Commissioner for Justice, Fundamental Rights and Citizenship, stated that the protection of personal data is a fundamental right and that it is for this reason that, in order to guarantee this right, it is necessary to have clear and consistent regulations in the area of data protection. She went on to say that the European Union's own regulations must be brought up to date in terms of challenges stemming from new technology and globalization, and that in the upcoming year the Commission shall develop new legal acts to strengthen the rights of the individual, while simultaneously guaranteeing the free flow of data within the framework of a unified European Union market by eliminating bureaucratic barriers[4].

It is for this reason that the Communication of the European Commission of November 4, 2010—COM(2010) 609—proposes the following strategy for the modernization of the European Union legal framework in the area of data protection, where several objectives have been formulated to be served by:

- Strengthening of individual rights so as to limit the accumulation and utilization of personal data to an absolute minimum,
- Expanding the extent of the unified market by decreasing bureaucratic burdens on companies and guaranteeing identical conditions of competition,
- Examining regulations governing data protection in collaboration with the police and judicial services in criminal cases, so that the data of individuals in these fields are also protected,
- Guaranteeing a high level of protection in the case of data transfer outside the European Union by improving procedures for international data transfer as well as making them more efficient, and
- Greater effectiveness in the enforcement of regulations by strengthening the position and increasing the powers of data protection bodies as well as their further harmonizing.

[3] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, Brussels, November 4, 2010.

[4] "Twoja Europa" [Your Europe] Internet portal, "Personal Data Protection in the European Union" [in Polish], http://www.twojaeuropa.pl/2156/ochrona-danych-osobowych-w-ue---nowa-strategia, December 1, 2010.

Below is a proposed list of concrete Agencies directly responsible for the implementation of decisions derived from the provisions of European Union law relating of the protection of personal data.

ENISA – European Network and Information Security Agency

The prime purpose of ENISA is to enhance the capability of the Community, the Member States, and as consequence the business community, to prevent, address, and respond to network and information security problems.

To this end, ENISA is focusing its activities on:

- Advising and assisting the Commission and the Member States on information security and in their dialogue with industry to address security–related problems in hardware and software products,
- Collecting and analyzing data on security incidents in Europe and emerging risks,
- Promoting risk assessment and risk management methods to enhance the capability to deal with information security threats, and
- Awareness–raising and cooperation between different actors in the information security field, notably by developing public–private partnerships with industry in this area.

ENISA is headed by Dr. Udo Helmbrecht, Executive Director, who is responsible for all questions related to Information Security falling within the Agency's area of activity. The work of the Agency is overseen by the Management Board. This Board is composed of representatives from the European Union Member States and the European Commission as well as industry, academic, and consumer organization stakeholders. Moreover, the Executive Director is responsible to the European Parliament, the Council of the European Union, and the Court of Auditors.

As ENISA's budget is derived from the budget of the European Union, its expenditures remain subject to normal European Union financial checks and procedures[5].

[5] European Network and Information Security Agency, "General Information on ENISA," http://www.enisa.europa.eu/media/faq-on-enisa/general-faqs-on-enisa, November 21, 2010.

EUROPOL – European Police Office

Europol is the law enforcement agency of the European Union. Its aim is to help achieve a safer Europe by supporting the law enforcement agencies of European Union member states in their fight against international serious crime and terrorism.

A staff of more than 620 at Europol headquarters in The Hague, Netherlands, works closely with law enforcement agencies in the twenty–seven European Union member states as well as in non–European Union partner states such as Australia, Canada, the United States, and Norway.

International crime and terrorist groups operate worldwide and make use of the latest technology. To ensure an effective and coordinated response, Europol needs to be equally flexible and innovative, and make sure its methods and tools are up to date. EUROPOL has state–of–the–art databases and communication channels offering fast and secure capabilities for storing, searching, visualizing, and linking information.

Gathering, analyzing, and disseminating this information entails the exchange of large quantities of personal data. Europol sets and adheres to the highest standards of data protection and data security[6].

The Directorate of Europol is appointed by the Council of the European Union (Ministers for Justice and Home Affairs). It currently consists of Director Rob Wainwright (United Kingdom) and Deputy Directors Tom Driessen (Netherlands), Michel Quillé (France), and Eugenio Orlandi (Italy).

EDPS – European Data Protection Supervisor

The position of European Data Protection Supervisor (EDPS) was created in 2001. The responsibility of the EDPS is to make sure that all European Union institutions and bodies respect people's right to privacy when processing personal data. When European Union institutions or bodies process personal data about an identifiable person, they must respect that person's right to privacy. The EDPS makes sure they do so and advises them on all aspects of personal data processing. "Processing" covers activities such as the collecting of information, recording and storing it, retrieving it for consultation, sending it, or

[6] European Police Office, "EUROPOL Profile," http://www.europol.eu/index.asp?page+facts&language=en, November 21, 2010.

making it available to other people, as well as blocking, erasing, and destroying data.

There are strict privacy rules governing these activities. For example, European Union institutions and bodies are not allowed to process personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, and trade–union membership. Nor may they process data on health or sexual orientation, unless the data is needed for health care purposes. Even then, the data must be processed by a healthcare professional or other person who is sworn to professional secrecy. The EDPS works with Data Protection Officers in each European Union institution or body to ensure that the data privacy rules are applied. In 2009, Mr. Peter Hustin was reappointed as European Data Protection Supervisor and Mr. Giovanni Buttarelli nominated as the Assistant Supervisor. Their mandate will run until January 2014[7].

The European Ombudsman

The position of European Ombudsman was created by the Treaty on the European Union (Maastricht, 1992). The Ombudsman acts as an intermediary between the citizen and European Union authorities. He is entitled to receive and investigate complaints from European Union citizens, businesses and organizations, as well as from anyone residing or having their registered office in a European Union country. The Ombudsman is elected by the European Parliament for a renewable term of five years. This corresponds to Parliament's legislative term. Nikiforos Diamandouros, the former national ombudsman of Greece, took up the post of European Ombudsman in April 2003 and was re–elected in January 2005 for a successive five–year term.

He helps uncover "maladministration" in European Union institutions and bodies. "Maladministration" means poor or failed administration. In other words, "maladministration" occurs when an institution fails to act in accordance with the law, or fails to respect the principles of good administration, or violates human rights. Some examples are:

- Unfairness,
- Discrimination,
- Abuse of power,

[7] EUROPA Gateway to the European Union, "European Union Institutions and Other Bodies: European Data Protection Supervisor," http://europa.eu/institutions/others/edps/index_en.htm, November 21, 2010.

- Lack or refusal of information,
- Unnecessary delay, and
- Incorrect procedures.

The Ombudsman carries out investigations following a complaint or on his own initiative. He operates completely independently and impartially. He does not request or accept instructions from any government or organization[8].

2. Legal and Institutional Aspects of Guaranteeing the Information and Communication Security of Businesses, Companies, and Citizens in Poland

Alvin Toffler, the American writer known for his work on digital communication and the corporate revolution considers the *flow and exchange of information as becoming the leading creative and power factor of Man*. It is for this reason that information and economic security of the state are so important to so many countries in the 21st century, and are becoming a priority in national safety. Poland is also aware of this problem. This is particularly seen in the "National Security Strategy of the Republic of Poland" document [in Polish]. Fighting threats to government tele–information and telecommunication systems is intended to act against computer crime as well as other hostile acts aimed against the telecommunication infrastructure, including the prevention of attacks on the components of that infrastructure. Of special importance is the protection of nonpublic information held or transferred in electronic form. An important task is the development and implementation of transparent principles of access by duly authorized state bodies to contents sent by electronic means. This requires the continuous adapting of the provisions of laws governing telecommunications so they meet current reality in spite of rapid technological progress and take into account the security of Poland[9].

[8] Ibid., "The European Ombudsman," October 21, 2010.

[9] "National Security Strategy of the Republic of Poland" [in Polish], page 2, http://www.mon.gov.pl/pliki/File/zalaczniki_do_stron/SBN_RP.pdf, November 22, 2010.

Regulations Governing Personal Data Protection on a National Level in Poland[10]

Legislation

- Constitution of the Republic of Poland (Articles 47 and 51),
- Act of August 29, 1997 on Personal Data Protection (uniform wording in the Journal of Laws of 2002, No. 101, item 926, with subsequent amendments), and
- National legal acts in the realm of personal data protection.

Procedural Regulations

- Executive acts supporting the Act on Personal Data Protection,
- Directive of the Minister of Internal Affairs and Administration of December 11, 2008 on the model form for submission of a database for registration by the Personal Data Protection General Inspector (Journal of Laws of 2008, No. 229, item 1536),
- Directive of the President of the Republic of Poland of November 3, 2006 on conferring the Statutes of the Office of the Personal Data Protection General Inspector,
- Directive of the Minister of Internal Affairs and Administration of April 29, 2004 on documentation for the processing of personal data, and technical and organizational conditions to be met by equipment and information systems serving the processing of personal data, and
- Directive of the Minister of Internal Affairs and Administration of April 22, 2004 on model forms for the named authorization and official identification of inspectors of the Office of the Personal Data Protection General Inspector.

Below is a proposed overview of institutions responsible for the implementation of the above legal acts in the area of personal data protection. They are also obliged to guarantee the security of institutions and companies

[10] Generalny Inspektor Ochrony Danych Osobowych [Personal Data Protection General Inspector], *Prawo* [Law], http://giodo.gov.pl/138/id_art/1975/j/pl, November 23, 2010.

against the spreading of danger resulting from the implementation of new technologies within the territory of the Republic of Poland.

Institutional aspects

MON – Ministry of National Defense

This Ministry is the principle body in Poland with responsibility for the security of its citizens—not only in terms of information or the economy, but also militarily. Although pursuant to the Constitution of the Republic of Poland, the President of the Republic of Poland is the Commander–in–Chief of the Armed Forces, Article 134 of the Constitution states that in times of peace, the President is the head of the Armed Forces through the Ministry of National Defense. It is for this reason that the Ministry is such an important body in matters of security[11]. The Minister responsible for managing the Ministry is Bogdan Klich.

Legislative provisions define the Minister of National Defense as being the primary state administration body in the area of national defense. The Minister manages the Ministry of National Defense, which mainly signifies the whole of activities of the Armed Forces of the Republic of Poland. It is the Minister who develops guidelines for the security of the country and is the overall head in matters relating to the common responsibility for defense.

Among the detailed tasks of the Ministry of National Defense are[12]:

- Managing the whole of activities of the Armed Forces in times of peace and developing national security guidelines, including proposals relating to the development of the Armed Forces as well as its structures,
- Implementing general assumptions, decisions, and guidelines of the Council of Ministers with respect to national security,
- Providing general supervision over the performance of security tasks by bodies of the state administration, state institutions, local government, economic entities, etc. to the extent as assigned by the Council of Ministers, and

[11] Sejm [Parliament] of the Republic of Poland, Constitution of the Republic of Poland, http://www.sejm.gov.pl/prawo/konst/polski/kon.htm, November 30, 2010.

[12] The Ministry of National Defense, "Tasks," http://www.mon.gov.pl/pl/strona/1/LG_1_2, November 30, 2010.

- Providing general management in matters dealing with the common obligation of national defense, the concluding of international agreements as stemming from decisions of the Council of Ministers relating to the participation of Polish military contingents in international peace missions and humanitarian operations as well as in military exercises conducted jointly with other countries or international organizations.

Two departments in the Ministry look over communication and information security—the Department of Information Technology and Telecommunications and the Department of Protection of Nonpublic Information.

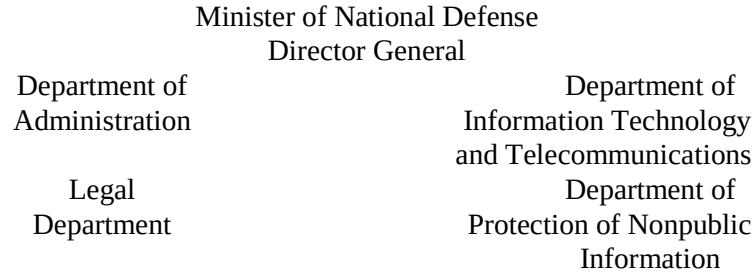
The **Department of Information Technology and Telecommunications** plans, oversees, coordinates, and identifies directions of development of information technology and telecommunications in the Ministry and functions as the organizer of the military telecommunication system. It is responsible for the functioning of information technology and telecommunications in the Ministry as well as for collaboration with the NATO, European Union, and public administration systems. It is the relevant cell with respect to defining technological standards for information technology and telecommunications in the Ministry and for developing and implementing standards as well as documents regulating the processes of design, implementation, operation, use, and maintenance of such systems[13].

The **Department of Protection of Nonpublic Information** coordinates and oversees the implementation of tasks relating to the protection of nonpublic information as well as the protection of facilities by the security divisions of organizational entities. It monitors the observance of regulations governing nonpublic information and military facilities and defines general, organizational, and technical requirements for systems serving the protection of such information as well as protection of the facilities of organizational units. It implements tasks related to providing office services for organizational cells[14].

[13] Ministry of National Defense, Department of Information Technology and Telecommunications, http://www.diit.mon.gov.pl, November 30, 2010.

[14] Ministry of National Defense, Department of Protection of Nonpublic Information, http://www.mon.gov.pl/pl/strona/1/LG_1_2, November 30, 2010.

Figure 1. Location in the Structure of the Ministry of National Defense



Source: Ministry of National Defense, Department of Information Technology and Telecommunications, http://www.diit.mon.gov.pl, November 30, 2010.

MSWiA – Ministry of Internal Affairs and Administration

As a part of its operations, this Ministry bears responsibility for the drafting of the legal, organizational, and technological foundations for the development of an information society as well as the development of directions and strategic programs for such development in the state. Its actions in the area of information security are implemented by the Information Society Department and the Office of Protection of Nonpublic Information.

The former is particularly responsible for the coordination of ventures linked with the development of an information society as undertaken by institutions implementing public tasks, especially the management of matters related to education in the area of implementing modern information technology solutions and the building of an information society as well as the related financing of projects in the area of the development of an information society by outside sources. The Director of the Information Society Department is Włodzimierz Barciński. He is directly responsible before Piotr Kołodziejczyk, the Undersecretary of State[15].

The latter Department involved in information security is the Office of Protection of Nonpublic Information. Its Director is Jarosław Rocławski who is directly responsible before Jerzy Miller, the Minister of Internal Affairs and Administration. The main tasks of this body include the managing of matters related to the performance of tasks by the Ministry as derived from the

[15] Ministry of Internal Affairs and Administration, Departments, http://www.mswia.gov.pl/portal/pl/78/6004/Departament_Spoleczenstwa_Informacyjnego.html, November 30, 2010.

provisions of the Act of January 22, 1999 on the Protection of Nonpublic Information, and it is in this field that it is primarily involved in:

- Administration of TEMPEST grade tele–information systems,
- Managing the NATO Contact Center, including supervision over the functioning of encoding systems—NATO e–mail, NATO telephone communications, and BERYL tele–copying communications,
- Participation in the drafting of international agreements in the area of the protection and exchange of nonpublic information, and
- Monitoring and training Ministry staff members in the area of observance of the provision of the Act of January 22, 1999 on the Protection of Nonpublic Information in Ministry Organizational Cells.

GIODO – Personal Data Protection General Inspector

Wojciech Rafał Wiewiórowski, Doctor of Law, is filling the post of Personal Data Protection General Inspector in the 4th term. The jurisdiction of the Personal Data Protection General Inspector is defined by the Act of August 29, 1997 on the Protection of Personal Data (uniform wording in the Journal of laws of 2002, No. 101, item 926, with subsequent amendments).

The Personal Data Protection General Inspector is empowered to:

- Monitor agreement between data processing and regulations governing the protection of personal data,
- Issue administrative decisions and adjudicate complaints in matters relating to the execution of regulations governing the protection of personal data,
- Manage a register of databases as well as provide information on registered databases,
- Review draft legislation and directives involving the protection of personal data,
- Initiate and undertake efforts in the area of improving the protection of personal data, and
- Participate in the work of international organizations and institutions concerned with questions of the protection of personal data.

In the event of any violation of regulations governing the protection of personal data, the General Inspector orders the reinstatement of a state in agreement with the law either by virtue of his office or upon application by the interested party by way of administrative decision. Specifically:

- Elimination of infringement,
- Supplementing, up–dating, correcting, granting access, or blocking access to personal data,
- Applying additional means securing the accumulated personal data,
- Stopping the transfer of personal data to third countries,
- Securing data or transferring them to a different entity, and
- Eliminating the personal data.

Should it be discovered that action or negligence on the part of the manager of an organizational unit, its staff, or a private individual who is the administrator of the data demonstrates the features of crime as defined in the act, the General Inspector directs notification of the commission of a crime to the body established to pursue crime, attaching evidence documenting the suspicion[16].

ABW – Internal Security Agency

The Internal Security Agency is a special service established to protect the constitutional order of the Republic of Poland. The range of its tasks concentrates on the protection of the internal security of the state and citizens. As a special service it is subject to civilian control. Its operations ore overseen by the Prime Minister and monitored by the *Sejm* [Parliament]. The responsibilities and powers of the Internal Security Agency are defined by the Act of May 24, 2002 on the Internal Security Agency and Foreign Intelligence Agency[17]. Primary responsibility for managing the Internal Security Agency lies with Brigadier General Krzysztof Bondaryk. The Internal Security Agency performs its tasks through the following activities:

a) Fighting terrorism, especially cyber–terrorism,
b) Counterespionage,
c) Fighting the proliferation of WMD,
d) Fighting economic crime,
e) Fighting organized crime,

[16] Personal Data Protection General Inspector, "Tasks and Jurisdiction," http://www.giodo.gov.pl/138/id_art/1975/j/pl, November 31, 2010.

[17] Internal Security Agency, http://www.abw.gov.pl/portal/pl/2/4/Agency_Bezpieczenskta_Wewnetrznego.html, November 31, 2010.

f) Fighting corruption,

g) Protection of state secrets, and

h) Analyses and information.

With respect to studies into the security of information and communications carried out in this report, several tasks managed by the Internal Security Agency are worth a closer look.

A) Cyber–Terrorism

There is no univocal definition for *cyber–terrorism*. The term first appeared in 1979 when a Swedish ministry included it in its strategy aimed at national threats. Looking further, a possible solution is to use the definition as assumed by specialists from the Academy of National Defense who, in their "Analysis of the Systemic Phenomena of Cyber–Terrorism" [in Polish], define it as a "politically motivated attack or threat of attack on computers, networks, and information system in order to destroy infrastructure, intimidate, or compel governments or people to meet far–reaching political or social objectives" (Sienkiewicz, Świeboda, Lichocki 2008).

An attack on one element of the system may disrupt the functioning of other elements (the "domino" effect) because they are all so closely interlinked.

The most serious source of threat to the tele–information network, apart from imperfect technical solutions, is purposeful actions. These may take on the form of:

- The disruption of system operations,
- Unauthorized introduction or copying of data, and
- Breaking through security, thus taking over control over individual components of the infrastructure—e.g. in the event of war.

The special services of hostile states or terrorist organizations may reach for the latter method. In their turn, organized crime groups may be interested in stealing data or making unauthorized modifications—e.g. in the systems and networks of financial institutions.

The Internal Security Agency bears responsibility for guaranteeing the security of key state systems and tele–information networks. To this end,

Internal Security Agency structures include the Governmental Computer Security Incident Response Team[18].

B) Counterespionage

Foreign intelligence strives to acquire nonpublic information, while camouflaging its operation and choice of people it works with. It undertakes efforts to procure knowledge on politicians, state defense systems, critical infrastructure, strategic economic entities, and scientific–technical centers[19].

On the one hand, tasks related to state security involving counterespionage encompass the protection of entities that may be the subject of interest on the part of foreign intelligence services. On the other hand, the monitoring of actions taken by such services within the territory of the Republic of Poland, especially so as to identify and neutralize efforts at procuring information using methods in contravention of the law. This may take place by way of[20]:

- Efforts at making contact with government employees,
- Efforts at procuring information designated as secret,
- Efforts at procuring dual–use technologies and goods, and
- Activities in the economic sphere (especially in the power engineering sector) that may threaten the economic foundations of the Republic of Poland.

The security system is primarily concentrated on:

- Central and local government administration offices,
- Economic entities of significance in terms of the primary interests of the Republic of Poland, and
- Scientific and technical centers involved in research on dual–use technologies.

The **Governmental Computer Security Incident Response Team** (CERT) was established on February 1, 2008. The basic task of this team is guaranteeing and developing the capacity of public administration entities of the Republic of Poland to protect themselves against cyber–threats, particularly

[18] Internal Security Agency, "Cyber–Terrorism," http://www.abw.gov.pl/portal/pl/88/306/Cyberterrorism.html, November 31, 2010.

[19] Ibid., "Counterespionage."

[20] Ibid.

taking into account attacks aimed at infrastructure encompassing tele–information systems and networks whose destruction or disrupting may be a threat to human life or health, national and environmental heritage of significant expanse, or cause serious material losses as well as disruption of the functioning of the state. The Governmental Computer Security Incident Response Team operates within the framework of the Tele–Information Security Department of the Internal Security Agency (ABW)[21].

The Governmental Computer Security Incident Response Team is primarily involved in:

- Coordination in reacting to incidents,
- Publication of alerts and warnings,
- Servicing and analysis of incidents (including the gathering of evidence performed by teams of court experts and assessors),
- Publication of notifications (security bulletins),
- Coordination of reaction to security gaps,
- Conducting security tests, and
- Responding to incidents in networks encompassed by protection through the ARAKIS–GOV System.

BBN – National Security Bureau

The National Security Bureau, managed by Brigadier General (Retired) Professor Stanisław Kozieja, Ph.D., Habil., serves the President of the Republic of Poland by providing assistance and support in the performance of tasks in the realm of security and defense. These tasks stem from the fact that the President is the highest–ranking representative of the Republic of Poland and guarantor of continuity of state authority as defined in the Constitution of the Republic of Poland. The President also oversees the observance of the Constitution, guards the sovereignty and safety of the state, and the inviolability and integrity of its territories[22].

[21] Governmental Computer Security Incident Response Team, http://www.cert.gov.pl/portal/cer/27/15/O_nas.html. November 31, 2010.

[22] National Security Bureau, "National Security Bureau Mission," http://www.bbn.gov.pl/portal/pl/18/1287/Misja_BBN.html, December 1, 2010.

With respect to information and communication security, it is the Department of Nonmilitary Security (DBP) and the Plenipotentiary for Nonpublic Information Protection Division that bear responsibility.

Among primary tasks facing the Department of Nonmilitary Security (DBP), directed by Lucjan Bełza, are:

- The accumulation of information on internal and external nonmilitary threats to national security, with special stress on public and social–economic safety as well as the development of relevant assessment in this area,
- Participation in developing strategic concepts and tasks for state structures in nonmilitary fields of national security, especially public, information, social, and economic safety, and
- Monitoring, analysis, and assessment of running government service activities, especially those of the Intelligence Agency, Internal Security Agency, Central Anticorruption Bureau, Military Intelligence Service, Military Counterintelligence Service, Government Protection Bureau, Corrections Service, Border Guard, Polish Fire Brigade, and the Police.

The scope of tasks of the Plenipotentiary for Nonpublic Information Protection Division, directed by Sylwester Żedecki, include:

- Guaranteeing the security of nonpublic information in the Bureau, including physical protection,
- Guaranteeing the security of tele–information systems and networks in the Bureau, where nonpublic information is created, processed, stored, and transmitted,
- Monitoring the security of nonpublic information and observance of regulations on the security of such information in the Bureau,
- Periodic review of records, materials, and document circulation in the Bureau,
- Development of security plans for nonpublic information in the Bureau as well as the overseeing of their implementation, and
- The training of Bureau personnel in the area of nonpublic information security.

Intelligence Agency

The Intelligence Agency, like many contemporary intelligence agencies, including foreign ones, strives to achieve a natural and efficient fit in the democratic structures of a modern citizens' society. This objective is serves by

transparency, to a greater degree than in the past, in areas that do not infringe against the security interests of the state or fundamental rules governing the operations of intelligence services. These always include the absolute protection of sources and personnel as well as assets, resources, and intelligence operations[23].

The Agency's main objective is the procurement of public as well as nonpublic information outside Poland's borders. From the point of view of the information and communication safety of Poland, the Intelligence Agency may warn of possible cyber–terrorism attacks or electronic espionage through its services. Its main tasks are the procurement, analysis, processing, and transfer of information that may be of significance to the safety of the Republic of Poland, its international standing, and its economic and defense potential to the relevant bodies.

Government Security Program

As of 2007, the Government Security Program is a program aimed at collaboration between the Internal Security Agency and Microsoft. Its purpose is the facilitating of joint actions by public administration bodies in the area of computer security and the mollifying of the effects of attacks on public information infrastructure. Collaboration also serves the support of government administration bodies in effective reaction to threats against national and public security as well as against the economy, through common ventures and the exchange of information.

Public administration institutions of many countries throughout the world that are responsible for reacting to events tied with computer security, the protection of key information technology infrastructure using Microsoft technology, and information technology security are a party to the Microsoft Government Security Program. It is within the framework of this program that representatives of bodies and offices responsible for supervision over the safety of the most important information technology system sin Poland receive the opportunity to familiarize themselves with tested procedures for reacting to emergency situations caused by electronic attacks, viruses, and attempts at unauthorized entry into the system. Moreover, the project is aimed at the group of public administration entities taking direct part or coordinating actions vital to the security of critical tele–information infrastructure, primarily the Internal Security Agency, Ministry of Internal Affairs and Administration, Ministry of

[23] Intelligence Agency, http://www.aw.gov.pl/pol/witamy.html, December 1, 2010.

Justice, Ministry of Transportation, and the Office of Electronic Communications[24].

3. The Protection of Regional Companies and Institutions Against Hazards Stemming from the Implementation of New Information–Communication Technologies

The **ARAKIS–GOV System** is an early–warning system alerting of threats in the Internet. The system is an example of the effective collaboration of the state, through the Department of Tele–Information Security of the Internal Security Agency and research institutions operating within the framework of NASK of CERT Poland. ARAKIS–GOV was created to meet the needs for support in protecting the tele–information resources of state administration on a central level as well as on the local level and that of economic entities as a result of the expanding of the ARAKIS System as created by CERT Poland to encompass additional functionality.

ARAKIS–GOV is not a typical security system and in no case can it replace the functionality of standard network security systems such as firewalls, antivirus software, and IDS/IPS[25].

However, due to its specifics, it may be successfully applies as a supplement to the above systems delivering information on:

1. New threats (global) appearing in the Internet, including:
   - Newly identified self–propagating threats such as worms,
   - New types of attacks observed from the level of a large number of sites,
   - Network traffic activity trends at specific ports, and
   - Activity trends of viruses sent by electronic mail.
2. Local threats linked with a concrete, protected site:
   - Lack of up–to–date antivirus vaccines,
   - Infected hosts in internal networks,
   - Leaking edge configurations in firewall systems, and
   - Attempts at scanning public address space both from the Internet and internal networks.

[24] Microsoft Polska, Press Center, http://www.microsoft.com/Poland/centrumprasowe/prasa/07_10/06.mspx, December 1, 2010.

[25] Governmental Computer Security Incident Response Team, ARAKIS–GOV System, http://www.cert.gov.pl/portal/cer/4/310/System_ARAKISGOV.html, December 2, 2010.

Moreover, the tools implemented in the system can make possible the comparison of network traffic statistics seen from the level of a protected site with the global picture as derived form all installed sensors with geographical imaging of the locations of suspicious traffic. At the same time, a unique feature of the ARAKIS–GOV System is the fact that it in no way monitors the content of information exchanged between protected institutions and the Internet. System detectors are installed outside the protected internal networks of the institutions on the side of the Internet[26]. Currently, the system sensors are installed in over sixty government offices on a central as well as local level. There is also the possibility of completely free use of the system by many institutions and economic entities.

Economic Entities

Economic entities are exposed to many threats stemming from the implementation of new technologies. The greatest threat is primarily the informatization of companies. Currently, the problem is not just spam as most users have learned to ignore unsolicited information and anti–spam filters watch over just about every mail server or viruses that are taken care of by event the simplest, free antivirus programs.

The main problem for corporations is a Distributed Denial of Service (DDoS) attack. An example of such an attack may be the attack on servers in Estonia on April 27, 2007, where the tele–information network was thrust to a critical stage. The web pages of the government, the chancellery of the president, and the main newspapers were blocked, while bank networks and those of the Estonian police were brought down. Estonians were cut off from access to information in the Internet as well as from access to banks and money. The outcome of this cyber–attack was the complete paralysis of ATMs, electronic mail, Internet portals, and the cellular phone network[27]. DDoS attacks are one of the most serious types of attacks against which it is impossible to safeguard, while at the same time they are capable of making life difficult, even in the largest companies. Often, "cyber–terrorists" threaten such attacks to extort money from companies in exchange for desisting from the attack.

---

[26] Ibid.

[27] Aleksander Ścios, Gazeta Finansowa, *Cyberpułapka? Estonia, Gruzja… Polska* [Cyber–traps? Estonia, Georgia … Poland?], http://www.gazetafinansowa.pl/index.php/wydarzenia/kraj/3821-cyberpulapka-estonia-gruzja-polska.html, December 2, 2010.

Another problem facing companies is the leaking of data. Most data leaks are the result of negligence or purposeful actions by users who may have access to data within the framework of the company network. The company's most important resource—its workers—can also cause the gravest harm. Tools serving as protection against such threats offer interactive alerts relating to peripherals. They allow IT managers to define dialogue boxes that appear on the computer user's screen in the event of work on confidential data. Such windows teach workers the principles of procedures involving confidential data, increase the awareness of problems linked with security, and allow the company to receive worker support in the battle with data leaks. Dialogue boxes warning workers against threats serve as a basis for administrators to define and adapt warnings to workers and define steps taken by them in the event of security violations[28].

When a worker wants to purposefully steal data—e.g. by copying to a external medium or transmission by e–mail—there are DLP systems registering such events. Unfortunately their application is expensive and for this reason, with the exception of very large companies with the highest requirements with respect to security, most organizations do not have the funds, human resources, and often even the need to implement DLP systems on a major scale[29].

Another problem is the transfer of the personal data of the workers themselves to other companies providing outsourcing services. The Act on the Protection of Personal Data burdens companies with several obligations. These also involve the personal data of workers. Many companies forget that entrusting an outside company with bookkeeping, which involves the transfer of the personal data of workers, requires the conclusion of a written agreement regarding the entrusting of data for processing. An employee cannot be required to provide any data other than those indicated in the Act[30].

[28] Mariusz Szewczyk, *Biuletyn Bezpieczeństwa Informatycznego* [Information technology safety bulletin], http://www.dataq.pl/Rozwiazania/Bezpieczenstwo/Biuletyn-bezpieczenstwa/LeakProof-ochrona-przed-wyciekiem-danych, December 2, 2010.

[29] Józef Muszyński and Patryk Królikowski, *Net World*, "DLP – Zapobieganie wyciekom danych" [DLP: Preventing data leaks], http://www.network.pl/artykuly/349862_4/DLP.zapobieganie.wyciekom.danych.html, December 3, 2010.

[30] Andrzej Janowski, *Gazeta Podatkowa*, No. 705.

4. Summary

In terms of institutions, Poland does not fare badly with respect to threats stemming from the implementation of technologies. A good example is the ARAKIS–GOV System and the Government Security Program developed jointly by the Government and scientific and research institutions. The situation is not as good when it comes to the awareness of individual citizens and smaller companies. This necessitates the facilitating of broader access to free programs securing companies against data leaks or uncontrolled cyber–terrorist attacks by companies. Unfortunately, companies lacking greater knowledge on the above threats often make little of the problem and in order to avoid additional costs make security arrangements on a very basic and limited level.

Part II. – Current provision regarding the use of CCTV and Biometrics in Poland

1. Introduction

In the first section will be described **the legal provisions in regard to CCTV surveillance, taking into account the laws and the practice**. This section will close with some words on technical standards, CCTV Monitoring Systems and the Technical Security Employee License.

Afterwards will be explained **the main regulations affecting biometric technologies**. In this field Poland is still at the beginning of the process of adjustment to EU Directive.

Closed Circuit Television (CCTV)

"CCTV stands for 'closed circuit television.' It is a television system comprised of a camera or a set of cameras monitoring a specific protected area, with additional equipment used for viewing and/or storing the CCTV footage. The term itself originates from the fact that, as opposed to broadcast television, CCTV is usually a 'closed' rather than 'open' system with a limited number of viewers. CCTV has been traditionally used for surveillance in specific locations with increased security needs such as banks, airports, and military installations. In addition, in industrial plants, CCTV equipment has been used to remotely

observe processes, for example, in hazardous environments. Increasing use of CCTV in public places has caused debate over public surveillance versus privacy"[31].

Pursuant to Article 23 of the Civil Code, where "personal rights such as health, liberty, dignity, freedom of conscience, surname and pseudonym, image, secrecy of correspondence, immunity of residence, and creativity involving science, art, inventiveness, and rationalization, all fall under the protection of civil law regardless of any protection provided by other regulations." Thus, the right to a person's image is among the basic personal rights of a person[32].

The Act on Protection of Personal Data makes up superior–level legislation governing regulations on the processing and safety of a person's image in CCTV systems. Specifically, Article 7, Clause 2, and Article 23, Clause 1, worded as follows:

"Article 7. Whensoever's the Act makes mention of:

"2) Data processing, this shall be understood as any operation performed on personal data such as collection, recording, storage, analysis, modification, providing access, and elimination, and especially operations performed in information technology systems,

"2.a.) Information technology system, this shall be understood as an assembly of mutually collaborating equipment, programs, and procedures for information processing as well as programming tools applied for the purpose of data processing,

"2.b)The securing of data in information systems, this shall be understood as the implementation and use of applied technical and organizational measures guaranteeing the protection of data against unauthorized processing."

Article 23, Clause 1. The processing of data is only allowed when:

"1) The person to which the data pertain grants permission, unless it is a question of the elimination of data relating to that person,

"2) It is vital for the performance of rights or the meeting of obligations as stemming from the provisions of the law,

"3) It is vital for the performance of an agreement, when the person to which the data pertain is a party or when it is vital in order to undertake action prior to the conclusion of the contract as demanded by the person to which the data pertain,

---

[31] European Data Protection Supervisor Glossary, http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/73, dated January 6, 2011.

[32] Article 3, The Civil Code – Act of April 23, 1964, Chancellery of the *Sejm* [Parliament] of the Republic of Poland, http://isap.sejm.gov.pl/Download?id=WDU19640160093&type=3.

"4) It is vital for the performance of legally defined tasks performed for the public good,
"5) It is vital for the meeting of legally justified objectives performed by data administrators or data users and such processing in no way infringes against the rights and freedoms of the person to which the data pertain"[33].

An employer may oversee employees, but must take care that their privacy is not violated. Article 11.1. of the Labor Code states that "a person's personal rights, especially health, liberty, dignity, freedom of conscience, surname and pseudonym, image, secrecy of correspondence, immunity of residence, and creativity involving science, art, inventiveness, and rationalization, all fall under the protection of civil law regardless of any protection provided other regulations."

Successive provisions concerning the protection of privacy may be found in Article 49 of the Constitution:

"The freedom and privacy of communication shall be ensured. Any limitations thereon may be imposed only in cases and in a manner specified by statute."

Moreover, pursuant to the Constitution, an employee has the right to disclose his or her data only in line with his or her wishes (Article 51). The obligation of disclosing specific data may only be derived from legislation.

In order not to infringe against an employee's right to privacy, the employer should inform him or her of monitoring in the work bylaws or employment contract. Moreover, the placement of cameras at locations where an employee would be justified in expecting respect for his or her privacy—e.g. lavatories and changing rooms—is forbidden.

It is assumed that the monitoring of employees signifies operations undertaken in order to gather information concerning employees by subjecting them to direct observations as well as indirect observation by electronic means. Since recordings from such monitoring are also stored and processed on cassettes or discs, monitoring is subject to the Act on the Protection of Personal Data. Thus, the data administrator (the employer) must make a special effort to make sure that the recorded material is secured against access by unauthorized parties (Article 36, Clause 1 of the Act). What is more, the employer must also remember that information gathered in such a way may only be stored for the length of time as necessary for the purposes of monitoring (Article 26, Clause 1, Sub-clause 4 of the Act). Furthermore, only persons who were previously duly

[33] The Inspector General for Personal Data Protection, Act on the Protection of Personal Data of August 29, 1997, with subsequent amendments, http://www.giodo.gov.pl/plik/id_p/473/j/pl/ (accessed on January 6, 2011).

authorized by the employer may have access to the processing of data (Article 37 of the Act) and the obligation of registering persons so empowered rests with the employer (Article 39, Clause 1 of the Act).

The absence of legal regulations relating to monitoring in the work place impedes the identification of clear limits on the actions of employers. However, efforts are being made to define requirements to be met in the monitoring of employees.

It is assumed that monitoring must be in agreement with the law, which signifies that it cannot take on forms violating the law. Moreover, monitoring may only be carried out for justified reasons—e.g. protection of information technology systems or the prevention of actions on the part of employees that may harm to work place. In introducing monitoring, the employer must also be guided by principles of proportionality (adequacy). This signifies that the means undertaken must be in proportion to the objective to be achieved when using employee monitoring, and this must be done in a manner interfering in the employee's privacy to least possible extent.

One of the arguments applied by employers is use of video recordings to protect employees. Thanks to such an "approach" the employer may monitor employees while simultaneously protecting them against robberies (fuel stations, banks, hotels), for example.

Greater detail in CCTV use is seen in concrete regulations concerning specific locations for camera installation. Legislation identified in this area includes:

- Act on Municipality Security Forces—the monitoring of cities (Journal of Laws of June 23, 2009) "In connection with the performance of tasks as defined in Clause 1 of Article 10, security forces have the right to observe and register with the application of technical means of images in public places when such activities are necessary for the performance of tasks and in order to:

  "1) Record proof of crimes or misdemeanors,

  "2) Prevent disturbances of the peace and order in public places, and

  "3) Protect municipal and public facilities.

  The Council of Ministers shall define the manner of performance of actions as discussed in Clause 2 by way of Directive, taking into account the need for guaranteeing effective observation and registration by way of technical

means of images of occurrences in public places as well as the need to respect human dignity and observance and protection of human rights[34]".

- Act on the Safety of Mass Public Events of March 20, 2009 (Journal of Laws No. 62, item 504).
- Act of August 22, 1997 on the Protection of People and Property (Journal of Laws of September 26, 1997) concerning requirements relating to companies managing operations involving security as well we relating to the licensing of people performing the installation of CCTV equipment.

Unfortunately, in the case of work places, there is a lack of judicial precedent that might be helpful is defining absolute grounds as to application. The monitoring of employees with the help of cameras registering images is not forbidden. However, it is assumed that there are certain rules that employers should keep in mind. It should be remembered that:

- Cameras may not be placed at locations where the employee may reasonably expect that privacy be respected—e.g. lavatories and changing rooms, and
- The employer should warn subordinates that they may be within the range of cameras, where rules in this respect should be defined in the work bylaws or among the provisions of the employment contract.

Video monitoring (like all other methods of monitoring employees) involves data processing as understood by Article 7, item 2 of the Act on Protection of Personal Data, hereinafter referred to as the "Act" (as in Journal of Laws 2002, No. 101, item 926, with subsequent amendments). For this reason, the data administrator (employer) should take special care to make sure the recorded material is secured against falling into unauthorized hands (Article 30, Clause 1 of the Act). What is more, the employer must also remember that information procured in this way may only be stored for a period of time as needed for monitoring purposes (Article 26, Clause 1, Sub clause 4 of the Act)[35].

CCTV Systems: Basic Qualities and Requirements

In Polish terminology, closed circuit television is a fragment of television's applications in the monitoring and protecting of people and

[34] Act Changing the Act on Municipality Security Forces, the Act on Polish Forces, and the Traffic Code (Journal of Laws No. 97, item 803).

[35] Gospodarka.pl web pages: "Monitorowanie pracowników" [Monitoring employees], http://www.prawo.egospodarka.pl/34089.Monitoring-pracownikow-co-wolno.2.34.3.html (accessed on January 6, 2011).

facilities. The installation of closed circuit television requires the highest technical culture as well as the ability to foresee even highly improbable events. In systems related to security, each and every installer and user must be absolutely aware of the fact that equipment with parameters deemed poor when compared with the tasks assigned may, in the future, prove a threat to property or even human life. This also involves problems caused by failure.

The Technical Security Employee License

Installation of closed circuit television requires a license.

License – Certification for the performance of tasks related to the protection of people and property that should be held by every employee providing services in this field. A 1st Level License grants rights to install systems. A 2nd Level License also grants rights to perform design work. Ways of receiving certification and licenses, required documents, and the model forms of the relevant IDs are contained in the Directive of the Minister of Internal Affairs and Administration of June 4, 1998 concerning model forms and procedures for issuing licenses to physical security and technical security personnel as well as types and frequency of issuing of opinions on security personnel by law enforcement bodies (Journal of Laws of June 26, 1998).

A **license** covering economic activity in the area of rendering technical security services must be held by the company providing security services for facilities that are obligated to have security—the list of such facilities may be found in the Act of August 22, 1997 on the Protection of People and Property (Journal of Laws of September 26, 1997)[36].

CCTV Monitoring Systems Used in Security– The EN 50132–7 Standard

The **EN 50132–7 standard** discusses the process of design, execution, and acceptance of industrial systems. Its guidelines are important in that it is difficult to build a good system without applying the algorithms they contain. Each installer, or even each investor, should have a copy.

Due to the responsibility borne by such systems, it is important to apply tested algorithms for building systems. Such solutions may be found in the

[36] INNEX web pages, "Telewizja przemysłowa. Wymagania" [CCTV: Requirements], http://www.innex.pl/?urzadzenia:wymagania (accessed on January 6, 2011).

above standard. The following procedures for designing CCTV systems are recommended:

- Specification of user requirements,
- System design,
- Equipment selection,
- System installation and start–up,
- Release of the system to the customer, and
- Maintenance (keeping the system operative).

The formulation of detailed operating requirements prior to commencement of the project allows for proper design as well as optimum selection of equipment, keeping requirements and costs in mind[37].

2. Biometrics

Rapidly developing biometric technology is finding increasingly broad application in the public security sector as well as outside it. Equipment using biometric identifiers to identify people or to verify their identity is consistently improving with each passing year. Scientists are pointing to the possibility of replacing qualities used most often today (such as fingerprints) with new properties of the human body that are more difficult to fake (such as the iris or blood vessels of the palm). Raising the level of security and decreasing the risk of forging identity are the advantages of biometric identifiers that are behind their growing popularity in documents and various types of systems. However, it must be remembered that there is a price to pay for the introduction modern security. In this case, it is the partial loss of anonymity expressed in consent for the storage of such sensitive information in computer systems[38].

The term *biometry* is derived from the Greek, where *bios* means "life" and *metron* means "to measure." Thus, this is the science concerned with identifying people on the basis of their individual qualities such as fingerprints, irises, etc[39].

[37] Deenhor web pages, "Telewizja przemysłowa – informacje" [CCTV: Information], http://www.deenhor-poznan.pl/cctv_telewizja_przemyslowa_informacja.html (accessed on January 6, 2011).

[38] Polski Serwer Prawa [Polish Legal Server], "Biometria korzyści, koszty, zagrożenia" [Biometry: Benefits, costs, and threats], http://lex.pl/?cmd-artykul,6503 (accessed on January 6, 2011).

[39] K. Krasowski and I. Sołtyszewski, "Biometria – zarys problematyki" [Biometry: Introduction], *Problemy Kryminalistyki* [Questions of Forensics], 252/06, p. 39.

The only document within the territory of the European Union, and therefore also within Poland, where the application of biometric technology is obligatory is the passport (introduced by way of Directive No. 2252/2004 of the Council of the European Community). In Poland, this obligation is regulated by the Act on Passport Documents of July 13, 2006. The chief argument against biometric technology is the matter of data storage. The European Union level legislator left the storage of biometric data with the member states.

Poland, pursuant to the Act on Passport Documents of July 13, 2006, defines the manner of storage of biometric data (Article 50a and Article 53), where it may be stated that such data (fingerprints) are stored only until such a time as the passport is issued or the application rejected. Biometric data are subsequently destroyed.

"**Article 50a.**
"1. Biometric data in the form of fingerprints shall be stored as passport records until such a time as the passport issuing body makes an entry into such records confirming acceptance of the duly made passport document.
"2. In the event of the issuing by the passport issuing body of a negative decision regarding the issuing of a passport document, biometric data in the form of fingerprints shall be stored as passport records until such a time as that body makes an entry into such records including information as discussed in Article 50, Clauses 2 and 5."
"**Article 53.**
"1. In addition to centralize records and passport records, the passport issuing body maintains documents serving as the basis for the issuing or refusal to issue or cancellation of passport documents in the form of files.
"2. In the case of documentation as discussed in Clause 1, biometric data in the form of fingerprints shall not be stored"[40].

Biometric security is not only used by the state. Biometric identifiers are being seen in the private sector with increasing frequency. Banks verify the identity of customers with the help of signatures affixed to special tablets, computers secured by a fingerprint reader, and devices capable of comparing the voice of a caller are just some examples confirming the level to which the fruits of modern technology are encroaching into our lives. The group that has recently tried to benefit from the "goodness" of biometry is the employers. However, as seen in a recent decision of the Supreme Court of Administration (NSA), the attempt was not successful. LG Electronics of Mława used fingerprints in order

[40] Chancellery of the *Sejm* [Parliament], Act on Passport Documents (Journal of Laws of 2006, No. 143, item 1027), http://isap.sejm.gov.pl/Download:jsessionid=38C099FE7CCCEB73F210300481 A247A7?id=WDU20061431027&type=1 (accessed on January 6, 2011).

to monitor time worked by its employees. The employees, by way of a written consent form, agreed to the collection of their biometric identifiers (in the event of refusal, the monitoring of entries and exists of such people were conducted in line with old principles). However, the Inspector General for the Protection of Personal Data concluded that the Labor Code provides no legal basis for the use of such data, which means that the procedure should be stopped. The Voivodeship [Provincial] Court of Administration adjudicated that the decision of the Inspector General for the Protection of Personal Data was flawed as in order for the fingerprints to be processed the employees had to give their consent, which is a premise giving the actions of the employer legitimacy. The Supreme Court of Administration subsequently overturned that verdict as it concluded that for the above–cited consent to be legally binding it must be expressed by equal entities[41].

Thus, it may be stated that the procurement of employee biometric data (i.e. fingerprints, irises, etc.) for the purpose of registering work time is incommensurate. It does, in fact, strike out against the employee's privacy.

3. Conclusion

In summarizing this report, it may be stated that there is a lack of unequivocal legislation defining principles of application of CCTV in Poland. Regulations are based on general protection of personal data and concrete regulations on individual public locations (mass public events, city monitoring, etc.). The situation is similar in the area of biometric technology. Apart from the Act on Passport Documents, there is no unequivocal regulation relating to methods for guaranteeing security. The ongoing development of technology should force the legislator to create unambiguous standards and laws effective in this area, as this is of great significance in the securing of the basic rights and liberties of each and every citizen of the Republic of Poland.

[41] Association of Prosecutors of the Republic of Poland (SPRP), http://www.sprp.pl/tresc/procurator/e70c99d6173a1917d8e27f3a1457d93b.pdf (accessed on January 6, 2011).

References

Act on Changes to the Act on Municipality Security Forces, the Act on Police Forces, and the Traffic Code, www.lex.pl

Akademia Monitoringu Wizyjnego [Academy of Image Monitoring], publications, www.cctv.org.pl

Association of Prosecutors of the Republic of Poland (SPRP), www.sprp.pl

European Data Protection Supervisor Glossary, www.edps.europa.eu

Chancellery of the *Sejm* [Parliament], Act on Passport Documents, www.isap.sejm.gov.pl

Chancellery of the *Sejm* [Parliament] of the Republic of Poland, Act of April 23, 1964 – The Civil Code, www..isap.sejm.gov.pl

Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final

Deenhor web pages, "Telewizja przemysłowa – informacje" [CCTV: Information], www.deenhor-poznan.pl

European Network and Information Security Agency, www.enisa.europa.eu.

European Police Office, www.europol.europa.eu

EUROPA, Gateway to the European Union, www.europa.eu

Inspector General for the Protection of Personal Data, Act on the Protection of Personal Data of August 29, 1997, with subsequent amendments, www.giodo.gov.pl

Janowski A., *Gazeta Podatkowa*, No. 705

Generalny Inspektor Ochrony Danych Osobowych [Personal Data Protection General Inspector], www.giodo.gov.pl

Gospodarka.pl web pages: "Monitorowanie pracowników" [Monitoring employees], www.prawo.egospodarka.pl

Governmental Computer Security Incident Response Team (CERT), www.cert.gov.pl

INNEX web pages, "Telewizja przemysłowa. Wymagania" [CCTV: Requirements], www.innex.pl

Intelligence Agency, www.aw.gov.pl

Internal Security Agency, www.abw.gov.pl

Konstytucja Rzeczypospolitej Polskiej [Constitution of the Republic of Poland]

Krasowski K., and I. Sołtyszewski L., *Biometria – zarys problematyki* [Biometry: Introduction], 'Problemy Kryminalistyki' [Questions of Forensics]

Liderman K. (2009) *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Wydawnictwo Naukowe PWN, Warszawa

Microsoft Polska, www.microsoft.com

Ministry of National Defense, www.mon.gov.pl

Ministry of Internal Affairs and Administration, www.mswia.gov.pl

Muszyński J., Królikowski P., *Net World*, www.networld.pl

National Security Bureau, www.bbn.gov.pl

Paplińska-Kacperek J. (2008), *Społeczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa

Polski Serwer Prawa [Polish Legal Server], "Biometria korzyści, koszty, zagrożenia" [Biometry: Benefits, costs, and threats], www.lex.pl

Ścios A., *Cyberpułapka? Estonia, Gruzja … Polska*? [Cyber–traps? Estonia, Georgia … Poland?], 'Gazeta Finansowa', May 2010

Sienkiewicz P, Świeboda H., Lichocki E. (2008) *Analiza systemowa zjawiska cyberterroryzmu* [Systemic analysis of the cyber–terrorism phenomenon], AON, Warsaw

Strategia Bezpieczeństwa Narodowego RP [National Defense Strategy of the Republic of Poland).

Treaty Establishing the European Economic Community, 1957

Twoja Europa [Your Europe] Internet portal, *Ochrona danych osobowych w UE* [Personal data protection in the European Union], www.twojaeuropa.eu

Szewczyk M., *Biuletyn Bezpieczeństwa Informatycznego* [Information technology security bulletin], www.dataq.pl

Streszczenie

SPOŁECZNE ASPEKTY NOWYCH TECHNOLOGII - CCTV I BIOMETRII (KONCEPCJA PRYWATNOŚCI I OCHRONY DANYCH OSOBOWYCH) NA PRZYKŁADZIE POLSKI

Celem niniejszego artykułu jest przegląd instytucji odpowiadających za ochronę danych osobowych na poziomie Unii Europejskiej oraz na przykładzie narodowym – Polski jako kraju reprezentującego nowe państwa członkowskie. Przedmiotem analizy jest system instytucjonalno – prawny zapewniający bezpieczeństwo komunikacyjne oraz informacyjne instytucji, przedsiębiorstw jak i obywateli przed zagrożeniami wynikającymi z innowacyjnych rozwiązań postępującego rozwoju nowych technologii zarówno w Unii Europejskiej jak i w Polsce. Poniższy artykuł jest również próbą analizy możliwości stosowania systemów zabezpieczeń CTTV oraz Biometrii w Polsce w ujęciu prawnym.

Wyniki analizy wskazują, że pod względem instytucji Polska nie wypada źle w odniesieniu do zagrożeń wynikających z wdrożenia technologii. Sytuacja nie jest tak dobra, jeśli chodzi o świadomość obywateli i mniejszych firm. Wymaga to ułatwiania szerszego dostępu do darmowych programów zabezpieczających firmy przed wyciekiem danych lub niekontrolowanych cyber-ataków terrorystycznych. W odniesieniu do stosowania systemów zabezpieczeń CCTV oraz biometrii, Polska pod względem prawnym jest wciąż na początku procesu dostosowania do dyrektywy UE. Ciągły rozwój technologii powinien zmusić ustawodawcę do stworzenia jednoznacznych standardów i przepisów obowiązujących w zakresie stosowania technologii CCTV oraz biometrii, gdyż ma to ogromne znaczenie w zapewnieniu podstawowych praw i wolności każdego obywatela Rzeczypospolitej Polskiej.