

**Information privacy in Albania:
Principles and recommendations for effective
personal data protection in a public sector IT system**

MASTER'S THESIS

by GINA L. SCHAAR

IT University of Copenhagen

M.Sc. in E-business

December 2007

Thesis advisor

Leif Bloch Rasmussen

Table of Contents

1	<i>Executive Summary</i>	1
2	<i>Introduction</i>	2
3	<i>Research topics and delimitations</i>	3
3.1	Research topics	3
3.2	Delimitations	3
4	<i>Author's background and relevant prior research</i> 5	
5	<i>Overview: Structure of the report</i>	6
6	<i>Research methodology</i>	7
6.1	Theoretical study.....	8
6.2	Field study.....	8
6.3	Note on limitations of the research methodology	9
7	<i>Personal data protection evaluation criteria</i>	11
7.1	Data protection and privacy concepts	11
7.2	Fair Information Principles (FIPs).....	12
8	<i>Nature of the relevant data protection environment</i>	14
8.1	Relevant international policy instruments.....	14
8.2	Albanian national laws and regulations.....	16
8.2.1	Albanian laws relevant to personal data protection.....	16
8.2.2	Albanian laws relevant to E-cJS system	17
8.3	International regulatory institutions	17
8.4	National regulatory institutions	18
8.5	Self-regulation and technology measures	19
9	<i>Nature and structure of E-cJS system</i>	21
9.1	Background.....	21
9.1.1	ICT in Albania	21
9.1.2	Albanian public administration ICT initiatives.....	21
9.2	Process for issuing judicial status certificates	22

9.3	Types of data maintained.....	23
9.4	System functionality and design description	24
9.4.1	Operational context: business processes	24
9.4.2	Information flows.....	28
9.4.3	Systems and infrastructure architecture.....	30
9.4.4	Application architecture.....	31
10 Evaluation of data protection effectiveness regarding E-cJS system		33
10.1	Applicability of Data Protection Law to E-cJS system	33
10.2	Accountability principle	35
10.3	Purpose identification principle	40
10.4	Knowledge and consent principle	41
10.5	Limited collection principle	43
10.6	Finality principle	44
10.7	Limited retention principle	46
10.8	Accuracy and completeness principle.....	46
10.9	Security principle.....	48
10.10	Openness principle.....	51
10.11	Subject access principle	53
10.12	Sensitivity principle.....	54
11 Conclusions and recommendations		57
11.1	Outlining a set of data privacy principles aids research, communication and debate.....	57
11.2	Mechanisms are needed to introduce personal data protection concepts into legislative and administrative processes.....	58
11.3	An independent supervisory authority for data privacy is advisable in Albania.....	59
11.4	Attention to data protection matters must occur very early in the process of developing data processing systems.....	59
11.5	Information privacy cannot be created by legislation alone—a policy community of interested actors is needed.....	60
11.6	Personal data protection should be approached as a good governance issue. 61	
11.7	Technology can promote data protection, but beware of over-reliance.....	62

12 Critical perspectives on the research.....	63
12.1 Critiques of theory and methodology	63
12.2 Other critiques.....	64
13 References	66
13.1 International treaties and conventions	66
13.2 Albanian laws.....	67
13.3 Books, articles and other publications.....	68
13.4 Unpublished papers	71
14 Attachments.....	72

1 Executive Summary

The research investigates personal data protection law in Albania, by comparing internationally recognized Fair Information Principles with the data protection aspects of the automated data processing system for citizens' criminal history data (known as the E-certificates of Judicial Status or E-cJS system). The research provides insight concerning four questions:

- *What criteria can be used to evaluate personal data protection effectiveness in general?*

Through examining the academic sources, the research identifies 11 Fair Information Principles (FIPs) reflected across a wide range of international legal and policy instruments, which set standards for good practice in handling personal data.

- *What is the nature of the relevant regulatory environment for data protection in Albania?*

The regulatory environment is described, including the international instruments and national laws applicable in Albania, the regulatory institutions linked to these, as well as available self-regulatory and technological means for data protection.

- *What is the nature and structure of the E-cJS data processing system?*

Based on field interviews and documents as well as the specific authorizing legislation, the E-cJS system is described with respect to business processes and operational context, types of data processed and information flows, systems infrastructure and application architecture.

- *How do the evaluation criteria compare to the E-cJS system within the regulatory environment?*

The research assesses the effectiveness of the E-cJS system and regulatory environment by comparing them to the standards expressed by each of the FIPs. The assessment results in a number of conclusions and recommendations for personal data protection systems in Albania:

- **Outlining a set of data privacy principles aids research, communication and debate.**
- **Mechanisms are needed to introduce personal data protection concepts into legislative and administrative processes.**
- **An independent supervisory authority for data privacy is advisable in Albania.**
- **Attention to data protection matters must occur very early in the process of developing data processing systems.**
- **Information privacy cannot be created by legislation alone—a policy community of interested actors is needed.**
- **Personal data protection should be approached as a good governance issue.**
- **Technology can promote data protection, but beware of over-reliance.**

2 Introduction

The genesis of this research project was a desire to examine one aspect of the intersection of law and technology in the public administration reform process of a developing country. Computerization is an increasingly important part of reform of processes and services in government institutions to make them more effective and efficient—especially in developing countries, a great deal of donor financing is devoted to such initiatives. These computer-supported government reforms raise new legal issues, because they create new capacities and provide services through new means, challenging the existing legislative framework, which in developing countries may be weak to start with.

Albania is a country undergoing profound political, social and economic changes since its independence from communist dictatorship in 1991. The country is undertaking a number of computerization efforts as part of its democratization processes, including court case management, voter registration lists, and a proposed national identification number. These technological efforts raise new questions about legal issues; one of the issues just now coming to the forefront in Albania concerns the handling and protection of personal data. What are the situations created by these computerization efforts that implicate the legal protection of personal data? What protections exist under current Albanian law and conventions, and what protections or provisions are lacking? How does the existing law compare with European standards, and how might it be changed to comply with these?

Examining such questions in the abstract is impractical because the field is so broad and potentially encompasses nearly every field of endeavor in public life. A more helpful approach is to examine a concrete case where technological efforts intersect with legal issues. The resulting analysis is naturally limited, but at the same time easier to grasp conceptually and apply in practice. Accordingly, this thesis will take one specific computerization project in the Albanian Ministry of Justice, and analyze the implications it raises for personal data protection in Albania according to national and international standards.

3 Research topics and delimitations

The specific computerization project to be examined is the Ministry of Justice data processing system implemented in 2007 for issuing electronic certificates of criminal convictions history for individuals. These are referred to in Albania as “judicial status” records and certificates, and the data processing system is referred to in Albanian law as the system for E-certificates of Judicial Status. For convenience of reference, this report will use the abbreviation “E-cJS”.

The research evaluates the protection of personal data in the public sector in Albania, based on the issues raised by the digitalization of the system for judicial status registries and certificates, and its expansion to include online access to e-certificates by institutions outside the Ministry of Justice.

3.1 Research topics

The aim of the research is to explore these questions:

What criteria can be used to evaluate personal data protection effectiveness in general?

What is the nature of the relevant regulatory environment for data protection in Albania?

What is the nature and structure of the E-cJS data processing system?

How do the evaluation criteria compare to the E-cJS system within the regulatory environment?

3.2 Delimitations

Another author in the field of data protection has noted that “an eclectic approach” to research in this field “follows necessarily from the nature of the issues discussed,” containing elements of traditional rule-based legal analysis, jurisprudence, and legal sociology, as well as “computer and information science, sociology, philosophy and political science”—yet not fitting squarely within any of those categories [Bygrave 2002: 9-10] (see also [Bennett 2003: 4]). This research project likewise takes such an “eclectic approach”—thus, it is relevant to identify what is *not* intended to be covered.

The research project is not intended as a study of the political processes or those of policy formation concerning information privacy in Albania. However, political and policy processes and actors are considered in the analysis to the extent they are relevant to the societal and political interests implicated by the specific ICT projects examined. Nor is this research project intended as a complete legal analysis of Albanian legislation affecting personal data protection, although it draws heavily upon the main Albanian laws in this area. These laws are analyzed, however, only from the standpoint of the Fair Information Principles described by leading theorists—so not all jurisprudential aspects of the legislation are covered in the analysis. For example, the issue of cross-border transfers of personal data is not covered. The analysis is furthermore not intended as a catalog or map of all legislative changes needed to harmonize Albanian law with European or international standards.

Because it focuses on one specific computerization project, the research does not attempt to catalog the full spectrum of public sector computerization activities in Albania that may implicate information privacy issues. There are many such activities in process, some of them mentioned in section 9.1.2, where data about individuals are being collected for the first time and/or being digitalized for the first time. Such a full survey is beyond the limited resources and access available to one private researcher.

Personal data protection in the private sector is not examined here, due to resource limitations as well as the difficulty of studying a diffuse and little organized sector of Albanian society. Online presence of the private sector in Albania is increasing, so data processing and the need for regulation and control is also presumably increasing, but this remains beyond the scope of my research. My focus on the public sector is also consistent with the focus of the earliest data protection policy and legislation in other countries, which was primarily driven by concerns about information processing in the public sector [Bennett 1992: 18], and the early stage of attention to data protection issues in Albania.

This study examines the *effectiveness* of the various measures and elements of information privacy affecting a single public data processing system—that is, how well the system outputs measure against a chosen standard or benchmark (as further clarified in section 10). One of the main theoretical commentators in the field has observed that an evaluation of data protection principles ought to be aimed at assessing not only effectiveness, but also economy (cost of input resources), efficiency (benefits achieved in relation to inputs), and equity (how equally benefits are spread across social, economic, geographic or other groups) [Bennett 2003: 193-5]. These are extremely complex political, social and economic issues beyond the reach of my own time, access to data and background. Furthermore, the concept of equity is a new, still-evolving theory not easily susceptible of investigation. Efficiency, economy and equity of personal data protection in Albania are thus beyond the scope of this evaluation.

4 Author's background and relevant prior research

I chose this particular research project in order to put into practice my own background, interests and prior research in the areas of law, international development and IT management. I chose a topic that could contribute to the ongoing development of law and technology in the Albanian public sector.

As an M.Sc. student at the IT University of Copenhagen (ITU), I have completed coursework in the 'E-business' study track, including courses in E-business management, strategy and law; Interactive Design; Enterprise Architecture; and IT in Organizations. In addition, I have written several student project reports related to IT, law and international development:

- a case study based on my work in Albania with IT-based reforms in the legal system [Schaar 2005]
- an overview study of the general field of information and communications technology for development (ICT4D) [Schaar 2006]
- a study of the progress of court case management automation in US courts and its relevance for similar progress in developing countries [Schaar 2006a]
- a study of the organizational theory aspects of a database development project at an international development consulting firm [Schaar 2006b].

In addition, I was the principal author of a World Bank evaluation report on legal and justice sector reform projects from 2000 to 2005 [World Bank 2006].

My interest in law and international development stems from my work as a practicing lawyer in US private firms and the federal government, as well as two years working in Albania on a legal system reform project. From this work, I learned a good deal about the development assistance business, the donor agencies that finance it and the types of projects performed. I also have had experience working on international development projects as a short-term consultant, particularly in Albania. The knowledge gained as a result of this work contributed a great deal of background knowledge necessary for the research in this thesis. In addition, I learned to speak, read and write Albanian well enough to communicate about professional matters without an interpreter.

5 Overview: Structure of the report

The following sections present the development and results of the research project.

First, I describe the methodology used for theoretical research as well as empirical data gathering, and the limitations associated with these, in section 6. Next, section 7 defines the criteria chosen as evaluation standards, based on the review of theoretical sources. These are known as Fair Information Principles (FIPs).

Section 8 outlines the nature of the relevant data protection environment in Albania. It is composed of international policy-legal instruments, Albanian law, and the regulatory institutions associated with these, as well as industry self-regulation and technologies that affect privacy interests—together comprising what is called a *privacy regime*. Following this generalized look at the context for information privacy in Albania, section 9 gives a very brief background on the status of ICT development in Albania. It then proceeds to describe the specifics of the E-cJS system: its operational processes, information flows, systems and application architecture.

Finally, the evaluation of the data protection environment as exhibited by the E-cJS system, as compared to the FIPs criteria, is carried out section 10; while section 11 concludes with some recommendations based on the research and evaluation. Thereafter, section 12 attempts to anticipate and address some possible critical perspectives on the research and the conclusions.

6 Research methodology

No recognized or ideal methodology exists for analyzing personal data protection issues. Even leading data privacy experts believe that “there exists no satisfactory way of evaluating or measuring the approximation of regulatory laws and mechanisms to the goal of protecting privacy.” Indeed, even the attempt to make such assessments is “politically and conceptually controversial.” Nevertheless, the same experts consider it important and useful to undertake a systematic analysis of data protection as best possible within the constraints presented [Bennett 2003: 187-188].

While necessarily imperfect, some methodological models do exist. This research was planned and conducted based on two such models:

- a methodology tested for the EU Commission for purposes of analyzing the level of personal data protection in non-EU countries in connection with cross-border transfers of personal data outside the EU [Raab 1998] (referred to as the *EU adequacy assessment methodology*)
- the Privacy Impact Assessment methodology used in Ontario, Canada for assessing the data protection aspects of new IT systems in the public sector [Government of Ontario 2001] (the *Ontario impact assessment methodology*)

Both methodologies include several basic common elements:

1. identification of a recognized set of data privacy principles and standards for use as an evaluation framework
2. description of a system of automated (IT-based) data processing
3. description of the operational context for the data processing system (organizational policies, procedures and practices affecting data handling)
4. empirical data gathered through interviews and knowledge of persons involved in the data processing, together with documentary evidence
5. assessment of the data processing system to determine compliance with the relevant principles and standards
6. analysis focused on the entity controlling and processing the personal data, for the purpose of determining risks to individual privacy.

The EU adequacy assessment methodology is aimed at evaluating the overall data privacy regime in a particular country with regard to a particular set of cross-border data transfers (such as patient health records or bank transaction records). The Ontario impact assessment methodology is aimed at determining the actual and potential data privacy impact of a single IT system within the context of a single country's data privacy regime. The research for this thesis combines the two methodologies because its aim combines the two aims: the research aims to examine the overall data privacy regime in a single country, through the lens of the impacts created by one particular IT system.

The description of the E-cJS system, its operational context and regulatory environment (elements 2 and 3 above) are primarily based on interview data (element 4), together with a study of relevant Albanian legislation. The identification of a set of data privacy principles and standards (element 1) was the result of

theoretical study of selected literature. This report is the result of the assessment and analysis of the empirical and theoretical research (elements 5 and 6).

In planning the empirical and theoretical research, I recognized the need for certain types and sources of data and the limitations associated with these, as shown in Attachment 1.

6.1 Theoretical study

A number of sources were available for the theoretical study part of the research, identified through internet and library searches, and verified through contacts with professors and experts in the field. These included national and international laws and conventions concerning data protection. In order to understand and interpret these legal sources, a number of academic treatises on data protection were studied; chief among these being *The Governance of Privacy* [Bennett 2003] and *Data Protection Law: Approaching its Rationale, Logic and Limits* [Bygrave 2002]. In addition, documents and publications by governmental and non-governmental institutions interested in data privacy issues assisted in understanding the normative instruments in this field.

I also had the benefit of two unpublished expert analyses of an early proposal for the E-cJS legislation, obtained during the preliminary interview phase [Patijn 2006; Sutton 2006]. The authors are former data protection officials from Holland and Great Britain who are working with the Council of Europe to assist with development of a data protection regime in Albania [Interviews 1 and 2]. The final E-cJS legislation was modified significantly after the early drafts, so these opinions were extremely helpful and informative but not conclusive for the questions raised in this thesis.

6.2 Field study

Empirical research was conducted by field interviews in Albania. I made one preliminary field visit during the preparatory phase of the research in order to help frame the topic and identify the proper sources of information. The interviews from this preliminary phase are listed in Attachment 3.

The main purpose of this research is a description and comparison of an actual situation to certain normative principles and standards. This involves qualitative analysis, so quantitative methods are not appropriate. The only practical and relevant way to gather empirical data relevant to the topic was through interviews with persons involved with the personal data protection law and the E-cJS project in Albania. For this purpose, I used the recognized technique of open-ended interviews based on a pre-formulated list of questions [Andersen 2006: 168]. The list of interview questions (see Attachment 4) was developed based on a recognition of existing knowledge gaps after a desk study of the literature. The questions were adapted from similar lists contained in my two main methodological models [Raab 1998: Appendix; Government of Ontario 2001].

In preparing for the interviews, I had the benefit of a good deal of background knowledge about the country, its legal system, and IT reforms in the justice sector, as described above in section 4. One of the IT systems I reported on for the World Bank was the predecessor to the E-cJS system [World Bank 2006], and I had also studied the same system from an academic perspective [Schaar 2005]. The

Albanian laws on data protection and the E-cJS system, as well as the relevant international legal instruments on data protection, were available to me prior to my study visit. Thus, I began the field study with a good deal of specialized knowledge about the topic, as well as prior contacts with some of the interview subjects.

All interviews took place between October 4 and 11, 2007. Each lasted approximately 30 minutes to 1.5 hours. As suggested by Andersen, I prepared handwritten notes during and immediately following each interview, rather than recording and transcribing the full interview [Andersen 2006: 168]. This was done for two reasons: first, several interviews were conducted in Albanian language, making simultaneous note-taking and transcription difficult; second, recording devices stifle frankness and ease in the interview setting—especially in Albania where it is not the norm. Not all questions were asked of all interviewees; rather, following the EU adequacy assessment methodology, each interviewee was asked for the particular areas where he or she had relevant knowledge [Raab 1998: 207]. In this way, the collective group of interviews provided the necessary data for analysis.

The list of interviewees appears in Attachment 2. Each interviewee was asked about other possible interview subjects, in order to assure that the correct people were identified. In order to preserve some degree of anonymity for the individuals, they are identified only by their title and organization.

6.3 Note on limitations of the research methodology

The EU adequacy assessment methodology study identified a number of practical difficulties with carrying out the necessary research [Raab 1998: 200-202]. The research for this thesis encountered similar difficulties with respect to the interviews:

- subject identification (finding interviewees able to respond to questions about data privacy in a country where there is almost no awareness at all of the issue)
- access (many of the interviewees are in high-level, demanding positions; some might be reluctant to speak openly about internal ministry affairs)
- time limitations (the interviewees could not give me unlimited amounts of their time, and I was in Albania for six working days for the main research visit)
- bias (since every interviewee was interested in presenting him- or herself and their respective organizations in the best possible light, and might also be concerned about the potential audience of the report)

Not all of these limitations could be counteracted, but in the end I was able to gain access to at least short interviews with all identified subjects. The problem of willingness to speak openly was counteracted to some degree by the level of trust developed through my prior work and contacts in the country. Since these prior contacts were only brief and professional, they assisted me to gain access while not causing bias. However, the lack of anonymity of the interviewees probably caused them to hold back some of their true thoughts and opinions. While I have not used their names in this report, the interviewees could not be assured of complete anonymity because it would be possible (with some additional effort) to identify most of them just from their positions.

Not all questions could be covered or explored in detail due to time limitations, but enough information was gained to provide a basis for analysis. Bias was dealt with

to some extent by interviewing subjects from several different organizations with different perspectives and motivations, and by reference to my own prior background knowledge and research.

The research also involved language barriers. Some interviews were conducted in English, a foreign language for the subjects; and several interviews were conducted in Albanian, a foreign language for the interviewer. Especially in the latter case, as in any case where one party is not a native speaker, there is a possibility for miscommunication. However, I was familiar with the particular Albanian terminology in advance from my work editing the translations of the legislation, and I was careful to ask for clarification or translation when I was uncertain. This was possible due to the interviews being done in person with an open structure. The decision not to use an interpreter had the advantage of allowing much better use of limited time and creating a level of trust with the interview subjects.

One additional criticism might be directed at the research methodology—namely, that the research itself had an influence on the situation researched. Specifically, lack of awareness about data protection is one of the results identified through the study, but awareness increases by virtue of conducting interviews and making inquiries about the subject. However, this problem is of little import for this particular project, for two reasons. First, the data are qualitative, not quantitative, implying a degree of flexibility and subjectivity in the results. Second, the phenomenon studied is by nature constantly evolving in any event, research or no research, so it is possible only to capture a snapshot in time.

The theoretical study also entailed a bit of difficulty. Despite thorough research and cross-checking with contact persons in the field, I was unable to identify theoretical or academic literature concerning the application and practice of data protection specific to the public sector, and especially about criminal records. One explanation might be that the public sector keeps such written information internal within the operative institutions, and thus not publicly available on the internet or in libraries. Certainly a number of treatises exist concerning data protection laws and practices applicable in the private (commercial) sector, for example [Kuner 2007] and [Carey 2004].

7 Personal data protection evaluation criteria

The first topic of the research is to identify a set of criteria that can be used to evaluate personal data protection.

7.1 *Data protection and privacy concepts*

The concept of *personal data protection* is central to the topics discussed in this thesis. Personal data protection is also referred to by the term *information privacy* [Bennett 1992: 14], indicating its theoretical affiliation to the concept of privacy in general. The notion of a right to privacy is often cited as a conceptual basis or justification for personal data protection. Privacy, while never precisely defined, is a generally broad concept having to do with the private sphere of the individual, the right to be left alone, or the freedom from various kinds of intrusion by the state. It can be understood broadly to mean a condition of “limited accessibility [to a person or collective entity] along spatial, psychological or information planes” [Bygrave 2002: 130]. It is closely related to and influenced by the concepts of individual autonomy, dignity, individuality, and integrity [Bygrave 2002: 23-4].

The notion of personal privacy is protected as a matter of right under the European Convention on Human Rights (ECHR) [CoE 1950: Article 8]:

Article 8 – Right to respect for private and family life

1 Everyone has the right to respect for his private and family life, his home and his correspondence.

2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Personal data protection or *information privacy* is a narrower concept that forms a subset of the general principle of personal privacy. It is important to understand this theoretical connection to the general right of privacy, because the idea of personal data protection is often misunderstood to mean physical security of personal data (for example, fireproof and locked filing cabinets, or computer database backups and password access). Physical security is a part of personal data protection, but as a subset of the right to privacy, many other principles are involved as well.

It is also important to note, and Article 8 of the ECHR above recognizes, that the right to privacy is not absolute: it can be circumscribed for a number of legitimate reasons. With regard to personal data protection, the right of privacy is often limited in order to protect other rights, like freedom of the press, freedom of religion, or the right to education. In a government context, personal data privacy is often limited for the purposes of public safety, crime prevention and prosecution—important with respect to the E-cJS system.

Information privacy interests revolve around the protection of *personal data*, so it is helpful to discuss what is meant by the term. One of the simplest definitions is found in the Council of Europe's Convention No. 108 [CoE 1981: Article 2a], which defines “personal data” to mean “any information relating to an identified or identifiable individual.” This definition is expanded by the EU's Directive 95/46/EC [EU 1995:

Art. 2a], which specifies that an “identifiable” individual is “one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.” Similarly, Albanian legislation defines “personal data” as “any data about an individual identified or identifiable directly or indirectly from this data” [Law No. 8517, Article 2a]. These definitions are obviously *very* broad. They cover any information that is expressly linked to a particular person—including name, address, identification numbers, photographs, fingerprints and the like—as well as information that can reasonably easily be linked to that person using other available information. (For a discussion of reasonableness in this context, see [Bygrave 2002: 47-50].)¹

7.2 Fair Information Principles (FIPs)

Since the advent of data privacy as an issue in the late 1960s to early 1970s [Bennett 1992: 3], a number of recognized principles have been derived from the various policy and legislative instruments. This section, together with Attachment 5, summarizes the most important and relevant principles used for this research.

One attempt to catalog comprehensively the data protection principles embodied in national laws, international conventions and voluntary standards and is Bennett and Raab’s “Fair Information Principles”:

An organization (public or private):

- must be *accountable* for all the personal information in its possession;
- should *identify the purposes* for which the information is processed at or before the time of collection;
- should only collect personal information with the *knowledge and consent* of the individual (except under specified circumstances);
- should *limit the collection* of personal information to that which is necessary for pursuing the identified purposes;
- should not use or disclose personal information for purposes other than those identified, except with the consent of the individual (the *finality* principle);
- should *retain* information only as long as necessary;
- should ensure that personal information is kept *accurate, complete and up-to date*;
- should protect personal information with appropriate *security safeguards*;
- should be *open* about its policies and practices and maintain no secret information system;

¹ This definition of *personal data* relates only to individuals, but it must be noted that the CoE Convention does allow state parties to choose to apply its provisions to collective entities as well as natural persons (Art. 3, sec. 2a). In fact, Albania declared it would apply its data protection law to collective entities when ratifying the Convention [CoE 2005]. But this declaration has not been applied, interpreted or enforced in any way in actual practice; and it is unlikely to be included in the new data protection law currently being drafted [Interview 4]. Because the issue is not of practical relevance for Albania, this thesis concerns only data protection for natural persons. For an exposition of issues associated with data privacy for collective entities, see [Bygrave 2002:199-282].

- should allow data subjects access to their personal information, with an ability to amend it if it is inaccurate, incomplete or obsolete. [Bennett 2003: 19]

Bennett and Raab also point out, consistently with the underlying general principles of personal privacy, that “these principles are, of course, relative. However conceptualized, privacy is not an absolute right; it must be balanced against correlative rights and obligations to the community, and can be overridden by other important values and rights.” [Bennett 2003: 19]. Concepts of balance and importance can and do vary from country to country.

Other commentators have also tried to distill a set of underlying principles from the various policy and regulatory instruments, including [Bygrave 2002] and [Kuner 2007: 20-21] (the latter analyzes only the EU Directive). Several other sources contain a statement of data protection principles: the Council of Europe’s Convention 108 [CoE 1981]; the Organization for Economic Cooperation and Development’s Guidelines [OECD 1980]; the United Nations’ Guidelines [UN 1990]; and the UK-government-appointed Younger Commission [Carey 2004:1-2]. For purposes of this thesis, it is not necessary to elaborate all the contents and peculiarities of these principles. The comparison in Attachment 5 is provided to illustrate the apparent wide consistency of principles among the various sources.

The FIPs expounded by Bennett & Raab are indeed comprehensive, with a few exceptions: they do not include the principles of *fair and lawful processing*, *anonymization* or *sensitivity* (see last three lines of Attachment 5). Of these, the principle of *sensitivity* of certain types of data (described by [Bygrave 2002: 68-69] and included in other instruments) is relevant in particular to the E-cJS system since it deals with sensitive criminal records data. The principle of *fair and lawful processing*, while incorporated in many of the sources, will not be treated in this thesis analysis, because of its vagueness and cultural/situational relativity. “Fairness” is almost impossible to define without reference to specific situations and societal norms; “lawful” depends on the particular legislation at issue. Both of these concepts can also be viewed as embodied by the other principles [Bygrave 2002: 58]. Likewise, the *anonymization* principle overlaps with the principles of *limited collection*, *limited retention* and *finality*. Therefore, the analysis in this report uses as a framework Bennett and Raab’s FIPs, supplemented by the *sensitivity* principle.

Even though these principles appear in all national and international data protection legal instruments (with exceptions noted), each specific law or convention differs in the expression, breadth and scope of these principles [Bygrave 2002: 57-69]. Thus, a specific situation or type of data transaction might be covered by one and not another, depending on the particular facts circumstances.

8 Nature of the relevant data protection environment

Bennett and Raab discuss a number of instruments, mechanisms, actors and technologies that contribute to the protection of individuals' interests in the privacy of their personal data [Bennett 2003: 71-162]. These include:

- transnational policy instruments, such as international treaties and conventions, the European Union's directives, or United Nations resolutions
- national laws, rules and regulations
- governmental regulatory agencies active within particular countries
- self-regulatory instruments and mechanisms enacted by companies, trade organizations or non-governmental organizations
- technological means designed to allow control over personal data.

Thus, personal data protection encompasses not only formal, written legal rules, but also the public agencies which enforce them, as well as the other elements mentioned above. Together, these elements and their interactions can be thought of as a data protection *regime* [Bennett 2003: 163, 187-188]. In order to describe the relevant data protection environment, it is necessary to examine each of these elements. Sections 8.1 through 8.5 discusses each in turn in the case of Albania.

8.1 *Relevant international policy instruments*

A number of international bodies have adopted policy guidelines or legal instruments concerning personal data protection. Chief among these are:

- Council of Europe (CoE) *Convention [No. 108] on the Protection of Individuals with Regard to Automatic Processing of Personal Data* [CoE 1980], which was adopted in 1980 and since signed by 38 member nations. The Council also adopted in 2001 an *Additional Protocol [No.181] to Convention 108, regarding Supervisory Authorities and Transborder Data Flows* [CoE 2001]. The Convention, together with its Additional Protocol, will be referred to in this report as the "CoE Convention."
- European Union (EU) *Directive 95/46 on the Protection of Individuals with Regard to Processing of Personal Data, and on the Free Movement of Such Data* [EU 1995], which has been transposed into the national laws of all EU member countries. It is referred to in this report as the "EU Directive."
- Organization for Economic Cooperation and Development (OECD) *Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data* [OECD 1980], which are non-binding statements of principle that have been influential in non-European countries; they have also been adopted voluntarily by private organizations in otherwise unregulated jurisdictions [Bygrave 2002: 32-33].
- United Nations (UN) *Guidelines Concerning Computerized Personal Data Files*, adopted by the UN General Assembly in 1990 [UN 1990]. These guidelines are non-binding and were aimed mainly at encouraging non-European member states, as well as to international governmental and non-governmental organizations (such as the UN itself), to adopt legislation and to process data in accordance with its principles [Bygrave 2002: 33].

The first two of these are the most relevant for the situation in Albania, and will be examined in this report. Albania is a member of the Council of Europe and ratified both the CoE Convention and Additional Protocol in 2005 [CoE 2005]. As such, these instruments are fully binding on the country, though they must be implemented through national legislation.

The EU Directive is not binding on Albania, since it is not a member. However, Albania aspires to membership in the EU and has entered into a Stabilization and Association Agreement (SAA) with the European Union as of July 2006 [Council of the European Union 2006], which includes a gradual approximation of laws as part of its conditions. Thus, the EU Directive represents the aspirations of Albania in the field of data protection.

The other two international instruments are not considered in detail for purposes of this report. They are non-binding in Albania, and more influential in non-European countries; furthermore, to include them would unnecessarily complicate the analysis, because the FIPs are covered by the others in any event.

The various international instruments, and the national data protection laws based upon them, also differ in their scope in terms of several important variables [Bygrave 2002: 50-56]:

Types of data processing. Some instruments apply only to automated data processing—that is, with the aid of computers. Others apply also to manual processing of data, when the data is kept as part of an organized register or filing system. Most definitions of “processing” include all possible actions performed on the data, from collection to deletion and all actions in between.

Sectors. Some instruments apply only to the public sector or governmental institutions, while others (notably the EU Directive and CoE Convention) apply to both the public and private sectors. Commercial activity is an important and pervasive area where personal data is collected, used and transferred, and where technological developments and innovations that threaten personal data privacy often appear first; so excluding the private sector leaves unregulated an enormous area of concern for data privacy advocates. Nevertheless, it is a policy choice that a number of countries, among them the United States, have adopted [Bygrave 2002: 53]. As explained above, this thesis does not attempt to examine the issue of data protection in the private sector.

A number of countries also have data protection laws that cover only one particular functional area of the public or private sectors. Examples include special laws dealing with national identity registers, banking or insurance industries, or health care records. Particularly relevant with respect to the E-cJS system, some countries also have special laws dealing with the processing of criminal records data [Patijn 2006; Sutton 2006].

Supervisory authorities. Some instruments (including both the EU Directive and CoE Convention) specify that there should be a regulatory body designated to act as the data protection supervisory authority in a country, handling matters of information, policy advice, complaint processing and enforcement of data protection laws and regulations. Some instruments state simply that there must be an available remedy for violations of data privacy, without stating what body should enforce it. Others are silent on the matter.

8.2 ***Albanian national laws and regulations***

National laws and regulations are perhaps the most conspicuous and important feature of the regulatory environment for data protection.² There are several Albanian laws relevant to personal data protection and the E-cJS system. These are introduced below.

8.2.1 *Albanian laws relevant to personal data protection*

Albania adopted a general law governing data privacy in 1999 [Law No. 8517] (referred to in this report as the "Data Protection Law"; English translation appears in Attachment 6). This law aims "to guarantee the protection and lawful use of personal data and their processing by public authorities" [Law No. 8517: Article 1]. The Data Protection Law is thus the key piece of legislation relating to data privacy in Albania.³ Concerning the variables mentioned above:

- *Types of processing.* The law is wide in scope, including "any act carried out" on personal data both "with or without support of electronic equipment" [Law No. 8517: Article 2c].
- *Sectors.* The law does not govern the activities of private entities, but only applies to "any organ of the public administration, public institution, organizational unit, or person as well as any other subject which based on the law exercises public functions and/or services" in Albania [Law No. 8517: Article 2] (incorporating provisions of the Albanian law *On the Right to Information Over Official Documents* [Law No. 8503: Article 2]).
- *Supervisory Authority.* The law states that complaints may be presented to the office of the People's Advocate (a parliamentary ombudsman institution), which is also directed to "create a registry of personal data processing" [Law 8517: Article 15]; however, the ombudsman institution is not given other duties or powers with respect to information privacy (see discussion in sections 8.4 and 10.2).

The Albanian Constitution also contains certain data privacy guarantees:

Article 35

1. No one may be compelled, except when the law requires it, to make public data related to his person.
2. The collection, use and making public of data about a person is done with his consent, except for the cases provided by law.

² This section describes the applicable legislation in Albania only. It is not the intention here to describe or make a comparative analysis of national laws in other countries.

³ Some other national laws having an indirect relation to data privacy in some of their provisions include:

- Law No. 8503 *On the Right to Information Over Official Documents*, dated 30 June 1999
- Law No. 8485 *Code of Administrative Procedures*, dated 12 May 1999
- Law No. 9131 *On the Rules of Ethics in the Public Administration*, dated 08.09.2003

These and other indirectly related laws are not discussed or analyzed as part of this research.

3. Everyone has the right to become acquainted with data collected about him, except for the cases provided by law.
4. Everyone has the right to request the correction or deletion of untrue or incomplete data or data collected in violation of law. [Republic of Albania 2007]

8.2.2 Albanian laws relevant to E-cJS system

The E-cJS system was created and is governed by a special law *On Electronic Certificates of Judicial Status*, adopted on 21 September 2006 [Law No. 9614] (referred to in this report as the “E-cJS Law”; English translation appears in Attachment 7). Pursuant to the provisions of this law, the Council of Ministers issued a decision identifying the public institutions authorized to access the system and specifying the form to be used for self-declarations of judicial status (explained in detail in section 9.4.1) [Council of Ministers Decision No. 825].

In addition, the E-cJS Law refers to certain provisions of other legal codes:

- the *Criminal Code of the Republic of Albania* [Law No. 7895].
- the *Criminal Procedure Code of the Republic of Albania* [Law No. 7905]

The referenced provisions of these codes govern (1) the registry of criminal convictions, (2) issuance of certificates of judicial status (stating the person's status as convicted or not convicted, and the conviction type and date, if any), and (3) punishments for violations of the law. The relevant provisions of these Codes appear in Attachment 8.

8.3 *International regulatory institutions*

It has been argued that one of the criteria on which to judge the strength of information privacy instruments is the nature of the *policy community* surrounding it [Bennett 2003: 165, 171-83]. According to Bennett's analysis, the nature of the information privacy regime in Albania will be shaped by the relative roles, power, focus and actions of the stakeholders involved. These stakeholders are interdependent: they both affect and are affected by the positions and actions of the others as part of the policy regime.

The international policy instruments discussed here—CoE Convention and EU Directive—are products of international organizations which are officially represented in Albania. The Council of Europe, of which Albania is a member country, maintains representative offices in the capital, Tirana, including a public information library. The Council of Europe conducts international development assistance projects in Albania co-financed in a joint program with the Commission of the EU [Council of Europe (no date)]. One of the projects under the joint program is to provide advice and support to data protection issues within the context of the civil registry system, including a review and amendment of Albanian data protection legislation to bring it in line with EU standards [*id.*; Interview 2]. The opinions concerning early proposals for the E-cJS system [Sutton 2006; Patijn 2006] were written by experts from the Council of Europe involved in this data protection project [Interviews 1, 2].

Likewise, the EU Commission maintains a Delegation in Albania which acts as the EU's diplomatic representation in the country and undertakes numerous activities on behalf of the EU in Albania. Among these activities are those supporting the

Stabilization and Association Agreement (SAA) signed between the EU and Albania on 22 May 2006 [Council of the European Union 2006], which charts the necessary goals and steps for Albania's rapprochement and potential accession to the EU. The lure of eventual membership in the EU is an extremely strong force for change in Albania, as it has been for other countries who have joined in recent years. The SAA, and the processes it sets in motion, are therefore an extremely influential force in Albanian politics, law and society. In addition, the SAA carries with it financial and other assistance from the EU, which in the agreement expresses its "willingness to provide decisive support for the implementation of reform and to use all available instruments of cooperation and technical, financial and economic assistance on a comprehensive indicative multi-annual basis to this endeavour" [Council of the European Union 2006: Preamble].

The SAA defines a first phase, lasting five years, during which a primary focus is on approximation of laws to the European *acquis communautaire* [Council of the European Union 2006: Articles 6 and 70]. In particular, under Article 79 on "Protection of personal data,"

Albania shall harmonise its legislation concerning personal data protection with Community law and other European and international legislation on privacy upon the date of entry into force of this Agreement. Albania shall establish independent supervisory bodies with sufficient financial and human resources in order to efficiently monitor and guarantee the enforcement of national legislation on personal data protection. The Parties shall cooperate to achieve this goal.

8.4 National regulatory institutions

In accordance with the mandate of the EU Commission in the SAA, the Albanian Ministry of Justice has convened a working group within the Department of Legislation to harmonize the existing Data Protection Law with European standards. A draft is in process as of late 2007 and will be released upon review and approval by the Minister of Justice [Interviews 2, 4 and 9]. The Ministry of Justice is named in Albania's declarations ratifying the CoE Convention as the body responsible for cooperation with other countries who are parties [CoE 2005]. Thus, to date the Ministry of Justice is in a position to take a leading role in data protection in Albania. It remains to be seen whether the new draft legislation will create a new specialized, independent body to deal with data protection, or whether this capacity will be created within an existing governmental structure.

There are some other governmental institutions with the potential to play a role in shaping information privacy policy in Albania. The office of the People's Advocate is named in the Data Protection Law as the body responsible for creating a registry of personal data processing and receiving complaints about it. However, this institution's practical and legal position is limited with respect to fulfilling the role as a supervisory institution, as explained below in section 10.2 on accountability. Nevertheless, the People's Advocate may play a more limited role as an oversight institution with investigative and persuasive powers in the public sector.

The courts also have a role to play, since they are the last recourse if the ombudsman institution and public administrative authorities can or do not act. Just

as elsewhere in the Albanian public sector, there is a need for increased awareness and knowledge among judges about the Data Protection Law and information privacy issues in general⁴. Thus, the role of the courts will be influenced by the actions of other players, such as academics in the field, business or civil society organizations, as well as influencing them.

The Council of Europe organized a conference in Tirana on 27 June 2007 on the topic "Privacy and Data Protection in Albania: What is at Stake?" [Interview 2]. This conference gathered representatives from the Ministry of Justice and other government bodies, civil society and human rights organizations, international experts, academics, private businesses, media and courts. The presentations and discussions concerned primarily the drafting of new legislation for data privacy and its impact on the new civil registry system now under development. This conference marked the first time interested groups from diverse arenas of public and private life had come together around the issue of personal data protection, and was intended to create awareness about issues that have been virtually unknown until now. Another conference is planned for after the release of the proposed new legislation. These conferences are a critical first step in the development of a *policy community*, as Bennett calls it, which will shape information privacy in Albania.

8.5 Self-regulation and technology measures

Other elements in Bennett's concept of a *privacy regime* include self-regulatory mechanisms and technology measures [Bennett 2003: 121-159].

Self-regulation refers to codes of conduct, privacy guidelines, statements of best practice or the like developed by regulated entities or industry or business groups. Since the Data Protection Law does not apply to the private sector and awareness of information privacy as an issue is almost non-existent in Albania, there has been no activity or indications of such to date. Business representatives from banks and insurance companies did participate in the Council of Europe's June 2007 seminar on data privacy [Interview 2], indicating that there is an expectation that private business will have a role to play. However, self-regulatory mechanisms do not figure in the analysis of this research project due to their embryonic stage.

Technology measures can also enhance information privacy [Bennett 2003: 139-151]. One of the most notable are encryption and digital signature schemes. The latter do not exist in Albania, and are not likely to arise in the near future. Encryption, such as SSL (secure sockets layer) and Virtual Private Network (VPN) technology does exist and can be built into systems at the application level. This is particularly relevant for a system such as the E-cJS system. Insofar as possible and where relevant, technology measures to protect privacy are analyzed in the sections concerning Fair Information Principles (FIPs).

Although technology measures can and do enhance data privacy, it is interesting to note that no technology companies or providers took part in the Council of Europe's June 2007 conference in Tirana. Given the potential role of technology, awareness

⁴ Based on a conversation on 11 October 2007 between the author and a law professor at the Albanian judges' training academy and law school.

and inclusion of this sector in the policy community would enhance information privacy in Albania.

9 Nature and structure of E-cJS system

Having established the analytical framework of Fair Information Principles (FIPs), and having examined the nature of the factors creating an information privacy regime in Albania, the analysis now turns to a description of the nature of the specific personal data processing system at issue, the E-certificates of Judicial Status (E-cJS) system. Following this description, the FIPs are used to evaluate the effectiveness of the Albanian information privacy regime with respect to the E-cJS system.

9.1 *Background*

9.1.1 ICT in Albania

In general, Albania came into the information age relatively late and is struggling to advance in this regard. When Albania's dictatorship ended in late 1991, there were few telephones in use and computers were more a phenomenon for academic research than practical use in either public or private spheres. Almost all developments in information and communications technology (ICT) have occurred since 2000 [World Bank 2005].

The national telephone company, Albtelecom, was finally privatized in 2007 [Tirana Times 2007], bringing modernizations such as availability of dial-up e-mail and internet connections in all regions of the country. The first broadband internet service also began to be offered in the capital city in 2007⁵, while in 2005 international internet bandwidth was at 4 bits per person (compared to 211 in Europe and Central Asia as a whole). The level of mobile telephone subscribers has risen dramatically in recent years in all regions of the country, but the penetration of computers in the population is still quite low, with only 12 computers and 60 internet users per 1000 population in 2005 (compared with 98 computers/1000 and 190 internet users/1000 for the Europe and Central Asia region) [World Bank 2005].

9.1.2 Albanian public administration ICT initiatives

Computerization efforts are ongoing throughout the whole Albanian public administration. For example, numerous initiatives exist in the Albanian courts and various justice authorities [Schaar 2005]. The Albanian police are receiving US assistance to develop an information management system that will provide the "technology to connect all border entry/exit posts through a computer network" [US Dept. of Justice 2007]. In September 2007, the Business Registration Center opened in Tirana with US assistance; this center is expected to operate as a "one-stop shop" for business entity creation and registrations with a variety of government authorities, including tax, labor, social and health insurance, offering online application and search functions [National Registration Center 2007]. Healthcare patient records are beginning to be automated as well [USAID 2004].

⁵ Based on advertisements from Tirana telecommunications companies seen by the author in October 2007.

Computerization of the country's civil registry is one project that may prove to be a focus for information privacy issues. The OSCE, with international financing, is helping the Albanian Interior Ministry to "computerize the country's civil registry and create a new address system... as well as provid[e] biometric ID cards for citizens" [OSCE 2007]. As mentioned above in section 8.3 above, the Council of Europe organized a conference for various public and private organizations concerning personal data privacy issues specifically related to the civil registry computerization. These are merely a few examples of many similar ongoing efforts; all of them will have significant information privacy aspects and impacts.

Of particular relevance for the E-cJS system, the UNDP is in Phase II of a project called Gov-Net, which aims at creating a comprehensive telecommunications network linking Albanian ministries and other public authorities, with facilities for e-mail, internet access and document management [UNDP 2007].

These examples show that the E-cJS system is being developed in the context of intense and wide-ranging computerization efforts throughout the public sector in Albania. With that context in mind, the following sections describe the nature and structure of the E-cJS system.

9.2 Process for issuing judicial status certificates

The Judicial Status Office (JSO) within the Ministry of Justice is responsible for administering data about criminal convictions, acquittals, dismissals and punishments. The JSO maintains a registry of information about individuals' criminal convictions and issues official "certificates of judicial status" certifying an individual's criminal convictions history [Law 7905; Interview 5].

The Criminal Procedure Code provides that all individuals have the right to obtain a certificate about their own criminal history without giving a reason [Law No. 7905: Article 484]. In addition, judicial authorities, state administration and entities providing public services may obtain judicial status certificates containing the information on file about an individual, if necessary for the person's assignment. Prosecutors may obtain judicial status certificates about criminal defendants and, with court permission, about victims and witnesses; and in the case of victims and witnesses the defense lawyer may also obtain such a certificate [*id.*].

Requesters must apply for the certificates in person at the JSO in the capital city, Tirana. A special office was set up for this purpose in 2005, at a location separate from the main Ministry of Justice building. Each day, the JSO receives between several hundred to a thousand applications for judicial certificates. There were extremely long lines of applicants and delays in processing requests [World Bank 2006: 12; Schaar 2005].

Until approximately 2005, the criminal history data registries were kept in manual form, and certificates of judicial status were issued manually. In 2005, the records and registry were digitalized, and a computer system was created and implemented which permitted electronic search of the records and automated preparation and printing of certificates for individuals or state authorities who requested them for employment or other purposes. This reduced processing time to about one business day [Schaar 2005; Interview 8]. However, the JSO was not able to perform the system maintenance needed to keep the system up to date, and no additional data was input since sometime in 2006 [Interviews 5 and 6]. Searches can be performed

automatically in the existing database, but the old manual system must be used for the time period since the last update in 2006. Processing time increased accordingly [Interview 5].

Ministry of Justice officials again sought a way to reduce waiting times and reduce the need for applicants to travel from the provinces to the capital. Ministry officials began discussing ways to allow public and private institutions to obtain the necessary certifications directly, rather than having citizens apply to the office for certificates which they then provided to the institution [Interview 8]. Based on advice from international organizations, mainly based on data privacy principles, the ministry ultimately decided to restrict access to a limited number of institutions, and to restrict online data to only a confirmation of whether a person has or has not been convicted, rather than full access to conviction history data. This would be done with a self-declaration and written authorization from the individual. [Interview 8; Sutton 2006].

After the enabling legislation was passed, an Albanian software development firm was contracted to develop a new software application to handle the processes for online access and verification, which became the E-cJS system [Interviews 1 and 3].

Under the new law enabling the E-cJS system [Law No. 9614], only institutions authorized by order of the Council of Ministers can have access to the system. Each institution designates only one person to have access on behalf of that institution. Access is obtained by fingerprint scan, and is only for the purpose of verifying individuals' self-declarations of judicial status (convictions or no convictions).

9.3 *Types of data maintained*

Data on criminal convictions are required to be maintained under the Criminal Procedure Code [Law 7905: Articles 481-484]. The data come from paper files, called "bulletins", sent to the JSO by the court which entered the conviction. The header of the file contains the person's name and bulletin number, while the conviction details such as the type of crime and the type of punishment (imprisonment or fine) is contained in the full bulletin document. Other identifying data about the individual are also included: the person's date and place of birth, mother's and father's name. The latter are used to distinguish among persons with the same name [Interviews 6 and 7].

Criminal convictions are considered "null and void" if the person commits no further crimes during a certain period of time after the last day of their sentence, according to article 69 of the Criminal Code [Law 7895: Article 69]. Such nullified convictions are referred to as "rehabilitations." While the Criminal Procedure Code does not specifically mandate registration of rehabilitations in the criminal records registry, the practice of the Office of Judicial Status is to maintain records of rehabilitation in the registries [Interview 3]. According to law, all types of data must be deleted from the register upon certain conditions (death, reaching age 80, review or abrogation of the offence). Data about acquittals, dismissals and punishments by a fine must be deleted after 10 years [Law 7895].

9.4 System functionality and design description

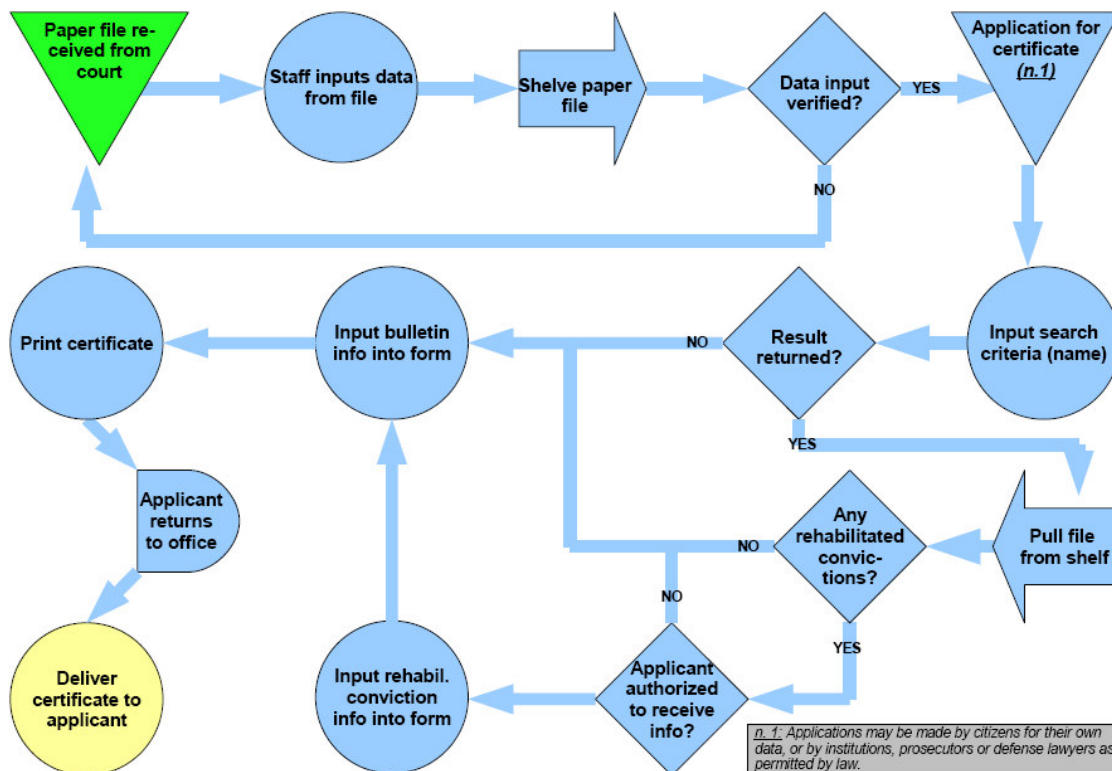
The organization of this section generally follows the framework in the Ontario Privacy Impact Assessment methodology for describing an information processing system [Government of Ontario 2001].

9.4.1 Operational context: business processes

Institutional operations undergoing automation are often referred to as *business processes*; the workflows in these business processes can be charted graphically using process modeling symbols [Chaffey 2004: 468-473]. This section describes and graphically models the business processes automated by the E-cJS system.

The operational processes are different for the JSO and for the authorized institutions. The business process for administration of judicial status records and certificates in the JSO is illustrated in Figure 1.

Figure 1. Business process for E-cJS in Judicial Status Office



Source: author's illustration based on Interviews 3, 5 and 6

Key to symbols: ▽ =Inbound information; ● =Processing; ◆ =Decision; ➡ =Info. transfer; ⬇ =Delay

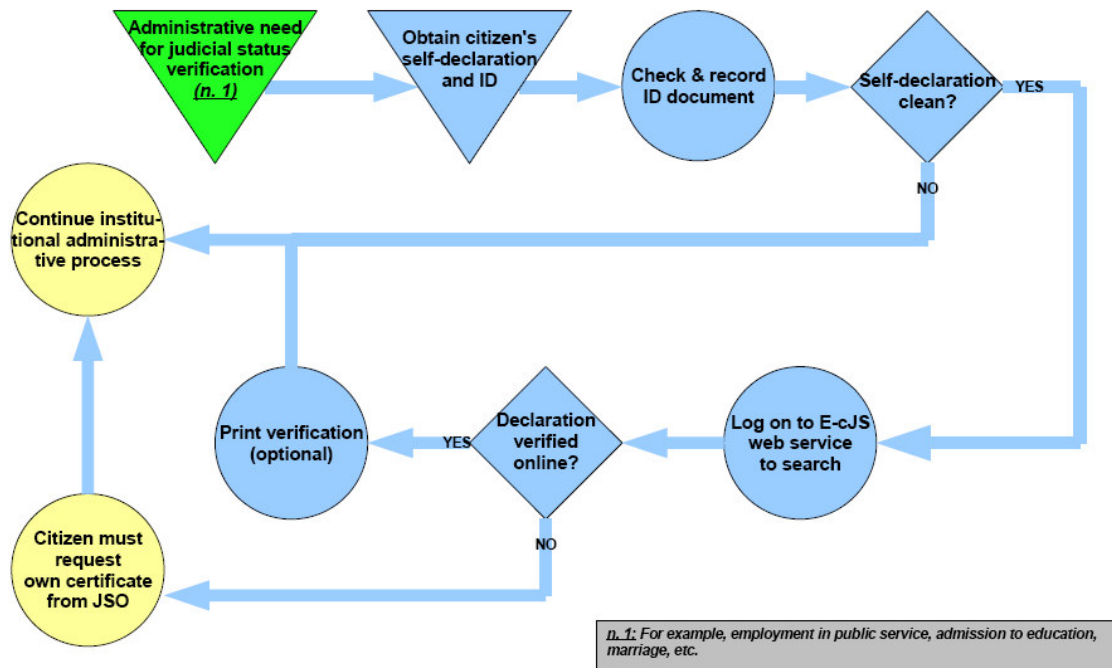
When the JSO receives a bulletin file from the court, staff members input the data from the bulletin into the computer system, while the paper record goes into a manual filing system. In the E-cJS, only information from the bulletin header is digitalized, while the conviction details remain only on paper. In order to assure accuracy of the digitalized data, a double check is performed each week to verify data entry before the computer record becomes final.

Applications are received by the JSO for judicial status certificates from individuals or from public institutions, prosecutors or defense lawyers. For individual requests for their own judicial status certificate, the name is taken from the identification documents presented to the staff in person at the time of the request. In order to process these requests, the staff uses the search function of the E-cJS system to determine whether or not the individual's name exists in the database. If it does not exist, then the person's criminal history is clean (no convictions). If the name is found in the database, then the staff must go to the paper bulletins to determine the detailed information about the person's conviction history. This information is then manually typed into the fields in the computerized form provided by the system, and an official certificate is printed. The printed certificate is then stamped and sealed. Normally, certificates do not contain any information about rehabilitated convictions; the person receives an ordinary clean certificate of no convictions. However, there are a few instances where the information can be revealed. If the staff determines it is appropriate, they will supply this information.

Because it takes at least one day to complete this process, the printed certificates are held until the applicant returns to claim it.

The diagram in Figure 2 shows the operational processes under the E-cJS system for institutions authorized by order of the Council of Ministers.

Figure 2. Business process for E-cJS in authorized institutions



Source: author's illustration based on Interviews 3, 5 and 6

Key to symbols: ▽ =Inbound information; ● =Processing; ◆ =Decision

Each of the institutions authorized by the Council of Ministers may designate one authorized system user, who will have his or her fingerprint scanned to allow access.

However, at the time of this research not all authorized institutions had in fact designated a user.

The authorized institutions are:

1. Office of the President of the Republic
2. High Council of Justice
3. General Prosecutor's Office
4. Central Elections Commission
5. Ministry of Justice
6. Ministry of the Interior
7. Ministry of Defense
8. Ministry of Public Works, Transport and Telecommunications
9. Ministry of Foreign Affairs
10. Ministry of Labor, Social Affairs and Equal Opportunities
11. Ministry of Finance
12. Ministry of Economy, Trade and Energy
13. National Intelligence Service
14. General Directorate of Prisons
15. General Directorate of the State Police
16. Interpol
17. Albanian Home Guard
18. Department of Public Administration
19. General Directorate of Customs
20. General Directorate of Taxation
21. Diplomatic representations, by authorization of the Ministry of Foreign Affairs
22. National Bank of Albania
23. Representation of the European Union in the Republic of Albania
24. Representation of the Council of Europe in the Republic of Albania
25. Representation of NATO in the Republic of Albania

[Council of Ministers 2006].

The administrative proceedings of these institutions create a need for information about judicial status. For example, citizens must provide this information for purposes of employment in public service, educational assignments, marriage, appointment to certain positions, and a variety of other situations. Another proceeding that creates a large need for judicial status information is for the purpose of obtaining travel visas. However, diplomatic missions are not currently authorized to access the E-cJS system directly, but only by agreement with the Ministry of Foreign Affairs (see no. 21 in the list above) [Interview 5; Interview 8].

There are two critical differences between the procedures in the JSO and in authorized institutions, according to the law: (a) institutions are required to obtain a self-declaration from the individual about his or her judicial status (checking a box for “convicted” or “not convicted”), together with the person’s authorization for the self-declaration to be verified, and (b) institutions do not have full access to convictions history from the JSO, but only to the list of names of persons convicted; rehabilitated convictions do not appear in the list [Law 9614].

The approved form for self-declarations is shown below in Figure 3. Under the law, the self-declaration must be accompanied by identifying documents of the declarant [Law 9614: Article 2.8], but this part of the process has not been automated in the software.

Figure 3. Form for judicial status declaration and authorization

SELF-DECLARATION FORM

Information about the declarant:

Last name, First Name	
Names of father and mother	
Date of birth	
Place of birth	
Identification document (attach copy to this form)	

I declare of my own free will that I have: no criminal convictions criminal convictions

DECLARANT	RECIPIENT OF DECLARATION
_____	_____
First & Last Name/Signature	First & Last Name/Signature/Seal

Authorization: I declare that the information provided in this form is true and correct, and I authorize its accuracy to be verified by _____
Authorized person

_____	_____
Signature of authorizing declarant	Date of signature

Note: Processing of personal data for the purpose of carrying out the authorization above may be carried out only in accordance with Law No. 8517 dated 22.07.1999 “On the protection of personal data”.
Providing a false declaration carries criminal penalties under the law and will cause your exclusion from all further proceedings.

*Source: Council of Ministers Decision 825, dated 6 December 2006, Annex 1
(translation by G. Schaar)*

When an institution receives a person’s self-declaration, the authorized user for that institution logs on with fingerprint recognition, and uses the search function to find out whether the person’s name appears as convicted or not, in order to verify the declarant’s statement. The record may be printed if needed, and this is done on a form along with the statement that it is “for the internal use of _____ [institution] _____”.

For any purpose other than verifying the convicted/not-convicted status of an individual, the process of applying for a certificate at the JSO must be used. For

example, a person must apply for an official certificate from the JSO if the administrative proceeding requires detailed information about which specific offenses a person has been convicted of; or if a self-declaration is *not* verified and the person believes this is in error. This type of situation will presumably arise in only a few special cases.

9.4.2 Information flows

The E-cJS system involves the collection of a variety of personal data, which is handled in different ways. The chart in Table 1 summarizes the ways in which the various types of data are treated. The data type descriptions in the left-hand column are those processed by the E-cJS system. For each data type, reading across to the right, the table identifies how it is handled.

Table 1. E-cJS Data Flows

Description of personal information cluster	Collected by/from source	Type of media/format	Used by	Purpose of collection	Disclosed to	Storage or retention site
Outstanding criminal convictions (bulletins)	by courts/ from original case files	Paper files (organized by bulletin number)	JSO personnel	Manual issuance of certificates of judicial status; input to automated systems	Citizens (own records); public institutions, prosecutors, defense (to extent permitted by law)	JSO shelves
Rehabilitated convictions	unknown	Paper files; electronic notation in electronic database visible only to JSO users	JSO personnel	Manual issuance of certificates of judicial status; input to automated systems	Persons authorized by law	JSO shelves
Existing automated database of bulletins up to 2006	JSO/from bulletins	Oracle database	JSO personnel	Preparation of certificates of judicial status (in combination with bulletins)	none	JSO server; backup media

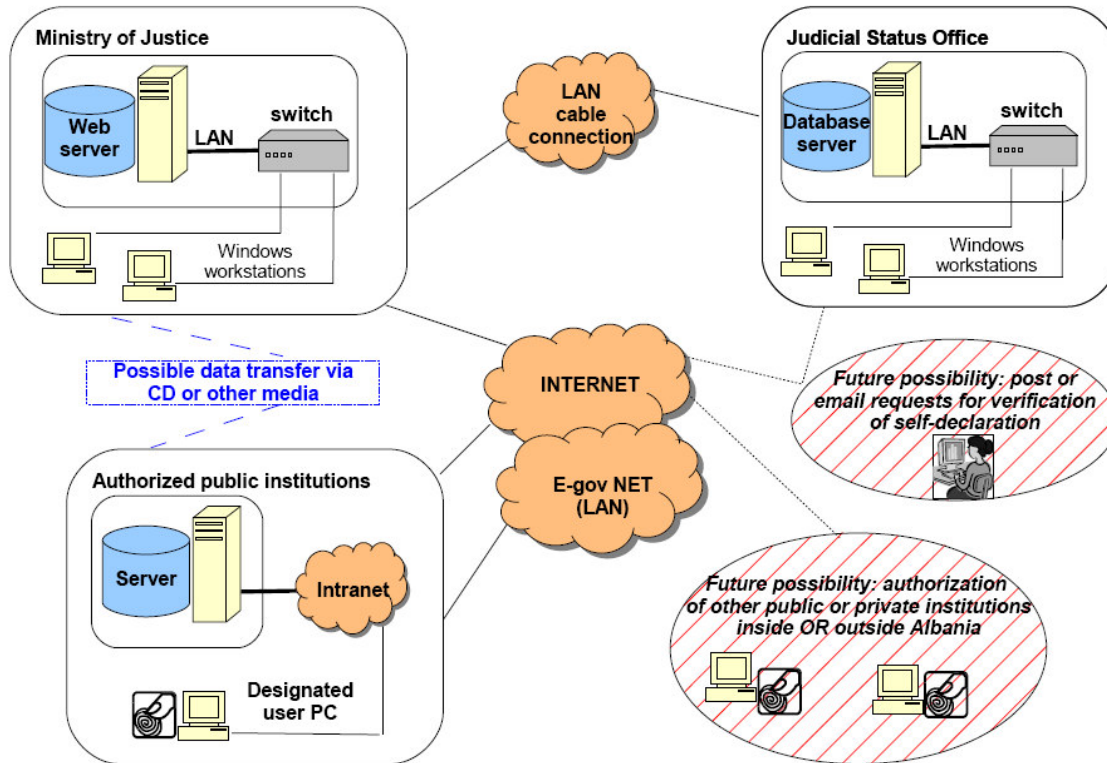
Description of personal information cluster	Collected by/from source	Type of media/format	Used by	Purpose of collection	Disclosed to	Storage or retention site
E-cJS automated database of conviction status (y/n)	by JSO staff/from paper bulletins	.net (SQL) custom application database	JSO personnel; one user in each authorized institution	Automated name search and printing of certificates of judicial status; Verification of self-declarations of judicial status	Internal use for authorized institutions	JSO server; backup media
Fingerprint data of system users	by E-cJS system administrator/ from authorized users' fingers	Electronic images	E-cJS users & administrators	Logon access to E-cJS	System administrators	User's local PC with USB reader

Source: (1) Table format, Government of Ontario 2006; (2) Content, E-cJS Law [Law No. 9614] and Interviews 3, 5, 6 and 8

9.4.3 Systems and infrastructure architecture

The systems architecture for the E-cJS is shown in Figure 4 below.

Figure 4. E-cJS System Architecture



Source: Interviews 3, 5 and 6; Cactus Albania documents; Law 9614

The computer and network infrastructure in the Albanian public sector is limited and at an early stage of development in comparison to European standards. In the public sector, the United Nations Development Program (UNDP) funded the installation of e-mail communications as well as local area network (LAN) connections between most (but not yet all) ministries and central government authorities, during the last couple of years [UNDP 2007; Interview P4]. This network is referred to as E-gov Net; the Ministry of Justice is part of this network, and it is also connected via cable LAN with the JSO [Interviews 3 and 5]. The Ministry has e-mail access, but the JSO does not [Interview 5]. Since the E-cJS is designed to be a web-based application, authorized institutions will rely on either or both the E-gov Net connections and the internet (via a virtual private network, VPN) to access the database functions. For institutions that do not have either type of connection, it might be possible to transfer data via CD or other digital media on an interim basis; presumably this would only be done for institutions which have many requests on a regular basis [Interviews 3 and 6].

There is one central server within the Ministry of Justice, which acts as a web server (the Ministry website is currently under construction) as well as the network server for the LAN inside the ministry building. The JSO has a central server used as the database server with the current Oracle database of judicial status records. This will

also be used to store the E-cJS database using the SQL platform [Interviews 3 and 6].

The enabling law for the E-cJS system allows two options which have not been operationalized within the current automation project. First, it allows the Council of Ministers to authorize fingerprint access for *any* institutions, public or private, Albanian or foreign [Law 9614: Article 8.2]. At the moment, however, there are no plans to expand access beyond the list mentioned above [Interview 8]. Second, the law provides that *any* institution, whether or not approved by the Council of Ministers, may request a verification of judicial status from the JSO via post or email, by fulfilling the necessary preconditions (self-declaration with authorization and proof of ID) [Law 9614: Article 8.4]. This option is very unlikely to occur in practice, though, because the JSO does not have e-mail access, and the private sector is hardly likely even to discover the possibility of doing so since the Ministry of Justice is not informing or promoting it to the public in any way [Interviews 3, 6 and 8].

When considering systems architecture, it should be noted that the physical setting for computerized systems is not ideal. Operating conditions are quite poor, with daily power outages and fluctuating current strength necessitating UPS battery backups and power modulators. Dust, humidity and temperature fluctuations also cause hardware maintenance problems most places, due to the poor condition of many public buildings. The Ministry of Justice premises were renovated just a few years ago, but it still suffers from these problems. The JSO premises are worse, especially in winter due to the small size of the building and poor insulation. Both the Ministry and the JSO have a generator to compensate during power outages, but these are of course expensive to run [Interviews 5 and 6].

There is also a shortage of IT personnel to perform hardware, software and system maintenance. The Ministry has two IT professionals, the director and a specialist. These two are responsible for everything related to the Ministry computers, from ordinary PC maintenance, to backups, system maintenance, website development and content management, and the like. They have also been involved in managing the E-cJS system software and infrastructure development, installation and testing from the client side. No one in the JSO has IT professional qualifications, although they have training and experience in the systems they use [Interviews 5 and 6]. The effect of such meager support can be seen in the relatively quick deterioration into disuse of the Oracle database system deployed in 2005.

As described above, bulletins are transferred from the courts as paper files. The courts are in the process of developing computerized case management and tracking systems that will generate the data currently contained in the bulletins in digital format [World Bank 2006; Schaar 2005]. However, there are no plans at the moment for automated data transfer from the courts, and it is not known whether the two systems could be made interoperable. In any event, this possibility was not considered during the application development [Interview 3].

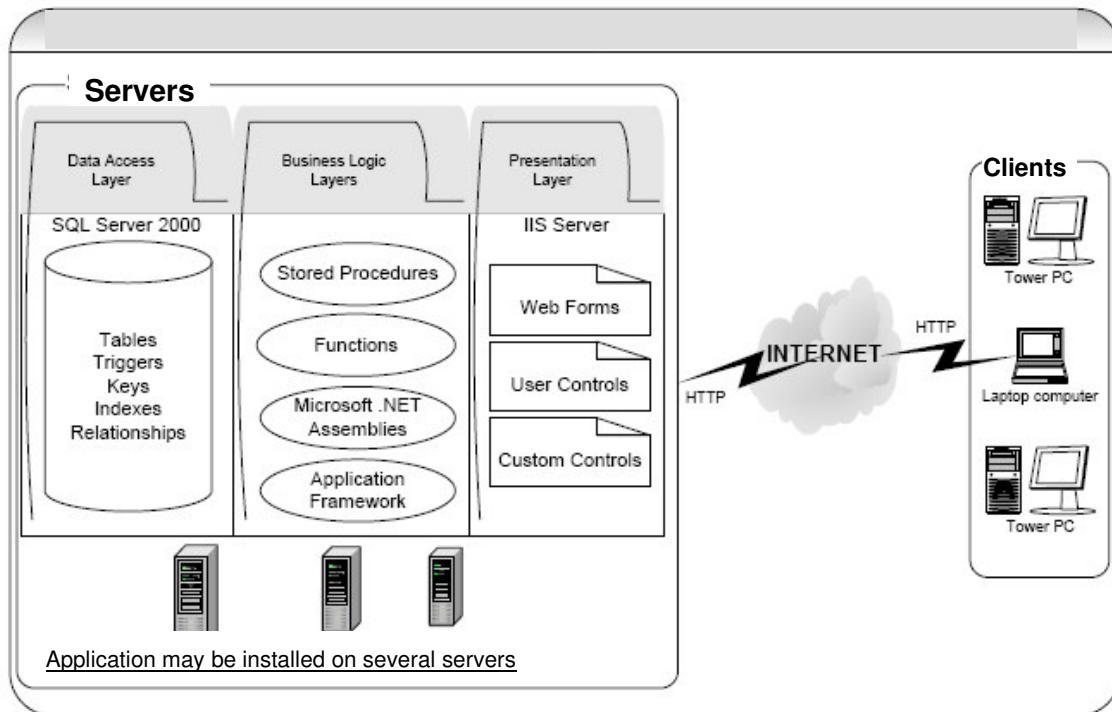
9.4.4 Application architecture

The E-cJS application was created to work with the Ministry Microsoft Windows operating system, and web functions will work with the MS Explorer browser on the client side. As shown in Figure 5, the application itself is based on Microsoft's .net platform, using SQL Server 2000 for the database functions, and IIS Server for the

web access functions. The application can run in either a client-server or stand-alone configuration, although it is being deployed in client-server mode. The application was in the testing phase in October 2007, with training of users, super-users and administrators expected to follow shortly [Interview 3].

Data migration from the existing Oracle database to the new SQL database will not be possible because the two systems are not compatible. Therefore the E-cJS system must be populated with data manually.

Figure 5. Application architecture



Source: Interview 3 (Cactus Albania document)

10 Evaluation of data protection effectiveness regarding E-cJS system

This research and analysis focuses on an assessment of the *effectiveness* of the Albanian data protection regime as exhibited through the E-cJS system.⁶

“*Effectiveness* refers to the relationship between outputs and ultimate objectives...” [Bennett 2003:194]. Put in another way, effectiveness means the relationship between the mission of an organization and the outcome of its activities [US Office of Management and Budget 2007]. In the case at hand, the evaluation of effectiveness will examine what results the privacy regime has produced for the E-cJS system, and how these compare to the defined objectives. For purposes of this analysis, the Fair Information Principles (FIPs) described earlier in section 7.2. are used as the statement of objectives for evaluation.⁷

The following sections will examine each FIP in turn, keeping in mind the elements that compose a data protection regime: national and international laws and regulations, interested institutions, self-regulation and technological measures. The evaluation must be made in light of the actual circumstances surrounding the data processing *in practice*, not only what appears from written laws and regulations [Bennett 2003: 6].

Before turning to the examination of the E-cJS system in light of the FIPs, it is necessary to examine a threshold question. The question concerns the role of the Albanian Data Protection Law in the analysis.

10.1 Applicability of Data Protection Law to E-cJS system

Besides the E-cJS Law and related provisions of the Criminal Code and Criminal Procedure Code, the question arises whether the issuance of certificates of judicial status is also covered by the provisions of the Albanian Data Protection Law.

The judicial status certificate system falls within the definition of “personal data” and “data processing” in the Data Protection Law [Law No. 8517]. Personal data is defined in Article 2(a) as “any data about an individual identified or identifiable directly or indirectly from this data.” The criminal history records do identify individuals and their criminal history directly. Similarly, collecting, checking, and using the data to produce judicial status certificates constitutes “data processing” under the very broad definition of the Data Protection Law, Article 2(c): “any act carried out with or without support of electronic equipment for the collection, registration, organisation, retention, elaboration, modification, selection, extraction,

⁶ In this section and following subsections, the analysis and observations are my own unless otherwise noted as coming from an interviewee or other source.

⁷ This type of evaluation can be problematic because there usually exist “unclear and multiple goals...” to be measured against, and because cause and effect between inputs and objectives can be difficult to establish [Bennett 2003:194]. This report does not delve into the field of performance measurement, which is an academic discipline of its own. Although the evaluation process may be problematic in some ways, approximate evaluation of effectiveness is nevertheless a useful pursuit for policy and practical reasons [*Id.*].

confrontation, use, suspension, communication, distribution, deletion, destruction, as well as any other act with regard to the data.”

Nevertheless, there is doubt about whether the Data Protection Law regulates the issuance of judicial status certificates, because Article 4(c) contains an exception for “personal data obtained in the course of investigations and proceedings in the courts”, and in Article 4(d) there is an exception for “processing of data for the purposes of national security [and] crime prevention.” Thus, it might appear that the data on criminal history and the issuance of certificates would be exempt from the protections provided by the Data Protection Law. However, there are several reasons to believe that the judicial status records maintained by the Ministry of Justice do not fall within these exemptions, and thus are covered by the provisions of the Data Protection Law.

1. *Criminal convictions data are defined as sensitive data.* The Data Protection Law specifies that personal data relating to “criminal status” are defined as “sensitive personal data” which receive special protection [Law No. 8517: Article 2(b)]. The fact that such data are included in the definition suggests that there was an intent to apply the provisions of the law to such data in at least some instances, rather than exempting them entirely under Article 4.

2. *Judicial status registry is a new act of processing.* The judicial status data, while originating from criminal proceedings in the courts, constitute a different register than those data as they exist in the files of the courts and prosecutor’s offices (see detailed explanation of the operational context in section 9.4.1). The courts’ and prosecutors’ files also contain other information about persons accused or convicted of crimes, and are maintained for a separate purpose and on the basis of different legal provisions. Thus, the judicial status files in the Ministry of Justice can be considered a new instance of processing personal data, apart from the processing done by the courts and/or prosecutors. While the latter is exempted from the law, the former is not necessarily so.

3. *An administrative body, not the courts, processes judicial status data.* The Ministry of Justice, where judicial status records are kept, is covered by the definition of “public authority” in the Data Protection Law [Law No. 8517: Article 2(f)]. Processing of data by the Ministry of Justice is therefore covered by the dispositive provisions of the Law. Since the issuance of certificates of judicial status is done by the Ministry of Justice, based on the registries it maintains separately from court files, the processing in that case is done by the Ministry of Justice, an entity obligated to follow the provisions of the Act.

4. *The processing is not only for purposes of crime prevention.* The law does not expressly state the purpose for creating criminal conviction registries or issuing judicial status certificates; but the list of those authorized to obtain certificates gives some indication of the purposes. Certificates of judicial status may be issued according to the Criminal Procedure Code to “authorities of justice, state administration and entities charged with public services” as well as prosecution and defense in certain circumstances [Law No. 7905: Article 484]. Under the E-cJS Law, E-certificates may be obtained by private entities as well as public authorities, and by foreign as well as domestic entities [Law No. 9614: Article 8]. Thus, crime prevention can indeed be considered one of the purposes for issuing certificates of criminal status, but clearly not the only one. For example, public entities must not hire a

person who has been precluded from public service by court decision. In positions where danger is involved, public safety may be an issue. Maintaining high administrative standards and efficiency might be other reasons. When private entities are considered, the purposes can be even broader, for example determining insurability or eligibility for credit, employment or recruitment, purchase of dangerous goods like firearms, and many others. Because issuance of judicial status certificates can have so many purposes, it cannot be said to be wholly exempt from the provisions of the Data Protection Act.

5. *Similar situation under data protection laws in other countries.* Data protection laws in some other countries create a situation where processing of criminal history records is covered both by a specific law tailored to such processing, as well as by the provisions of more general data protection laws. Under the laws in the U.K., individuals' access to their own criminal history data is regulated by a special police law, whose provisions are intended to be an alternative to the provisions for data subject access under the more general data protection law and regulations [Sutton 2006]. The situation in Sweden is similar, with a Police Data Act supplementing the more general Data Protection Act, and applying the principles of the general law to a specific situation and set of data [Seipel 2001: 120]. This indicates that such a legal interpretation is legally reasonable and might be the case in Albania as well.

The question of whether and to what extent the issuance of certificates of judicial status falls within the Data Protection Law's provisions has not been addressed by the Albanian courts or decided administratively. Thus, it remains an open question in Albanian law. For purposes of this research, however, the answer to the question is assumed to be positive, and the E-cJS data processing system will be treated as covered by the Data Protection Law in addition to the other relevant legal provisions. This assumption will permit a deeper analysis of data protection law and principles in Albania based on the issuance of judicial status certificates as a concrete example.

With this threshold issue established, the analysis can now turn to an examination of the data privacy regime and E-cJS system compared to the FIPs.

10.2 **Accountability principle**

- ☞ An organization must be *accountable* for all the personal information in its possession.

The principles of data privacy are not self-implementing; thus, the idea of accountability for the actions of an organization normally entails existence of a person, entity or institution with an interest in the activity in question to whom the organization responsible [Bennett 2003: 106]. This could simply be the data subjects themselves, since they arguably have the most direct and acute interest in the manner of processing their personal data. However, private individuals often lack the power, knowledge and resources (and sometimes the interest) to enforce their rights.⁸ Thus, both the EU Directive and the CoE Convention acknowledge the need for an oversight body as the key component in a data protection regime.

⁸ Regarding whether privacy rights ought to be enforced even when the individuals concerned do not do so, see the argument that society as a whole has an interest in maintaining and enforcing the individual's rights to data privacy regardless ("communitarian view") in [Bennett et al. 2003: 27, 41-43].

The EU Directive mandates that each of the member states must create and finance a data protection supervisory authority “responsible for monitoring the application within its territory” of the legal provisions for data protection, with “powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings. . .” [EU 1995: Article 28 and Recital 63]. The supervisory authority should make annual public reports on its activities and cooperate with similar authorities in other countries.

The CoE Convention contained no mention of supervisory authorities when first adopted, but the Additional Protocol directs signatory countries to establish supervisory authorities “responsible for ensuring compliance” with national data protection laws. Similar to the EU Directive, these authorities should have powers of investigation (including hearing complaints), intervention (including bringing legal proceedings or referrals to other authorities), and should cooperate with one another [CoE 2001: Article 1].

While EU member states and some other countries have established independent public supervisory authorities, in some countries oversight functions are performed by a central coordinating agency or left to passive supervision by the courts [Bennett 2003: 109]. Whatever the type of supervision, ensuring *accountability* for data privacy usually entails a variety of functions beyond those of investigation, intervention and complaint handling mentioned in the EU Directive and CoE Additional Protocol. These additional functions include consultation and advice to data processors, education and awareness-raising, and policy advice to lawmakers or self-governance bodies [Bennett 2003: 107-115].

Pressure to monitor and enforce data privacy may also come from the community of interested stakeholders—for example, NGOs with an interest in privacy issues, media, technology developers or the business community [Bennett 2003:171-83].

Accountability is a significant problem for the E-cJS system in the Albanian Ministry of Justice. Albania has not created any independent supervisory authority for data privacy issues, nor has any other government agency taken on the role in practice. In fact there is almost no awareness of the nature of data privacy rights or their application in the public or private sectors [Interviews 1, 2, 9 and 11].

There are a few authorities in Albania with the *potential* to play a supervisory role. The Albanian Data Protection Law specifies that the People’s Advocate (a parliamentary human rights ombudsman institution) is responsible for creating a registry of personal data processing, as well as hearing complaints [Law 8517: Article 15]. But the People’s Advocate institution was first opened only in 2000, and since then has struggled with establishing its existence and identity as a human rights institution in a weak state. The institution has focused on other priorities, and has not addressed its obligations under the Data Protection Law or data privacy as a human rights issue. The People’s Advocate office also has a number of drawbacks as a supervisory authority: it lacks authority over some public institutions (and the whole private sector); it has only persuasive authority and no ability to impose sanctions; and its current funding and personnel are not sufficient for additional areas of authority [Interviews 2 and 11; Agenda Institute 2007].

The Ministry of Justice is another potential supervisory authority for data protection issues. In fact, Albania’s declaration of ratification of the CoE Convention names the Ministry of Justice as the body responsible for international cooperation on data

privacy issues [CoE 2005].⁹ The Ministry's legislative department is currently drafting a new law on data protection, in line with EU standards. But the Ministry does not exercise any other functions of a supervisory authority: investigation, resolving individual complaints, intervention through sanctions, education and awareness-building, or policy advice and consultation with other public and private institutions. More importantly, it is questionable whether a ministry which itself is a significant processor of personal data is the appropriate body to act as a supervisory authority for data protection. A ministry is also directly dependent on or in close relationship with other public bodies whose data processing practices must be supervised—parliament and the Council of Ministers, for example—and thus is subject to political or other influences. For this reason, both the EU Directive and CoE Additional Protocol insist on independent supervisory authorities.

These two potential supervisory bodies also lack the necessary resources and personnel to carry out the duties of a data protection supervisory authority. This is a highly specialized field, where specialized knowledge and experience is needed, and it is advantageous to have little turnover of staff [Blume 1996: 352]. As recognized in the CoE Additional Protocol, a supervisory authority “should have the necessary technical and human resources (lawyers, computer experts)” to carry out its tasks [CoE 2001: par. 8]. Thus, additional staff, equipment and budget are needed for these public supervisory functions regardless of where they might be placed organizationally.

National non-governmental organizations (NGOs) in Albania have not yet formed a community of interest around data privacy issues. Human rights organizations have only begun to be aware of the issues, and at the moment have other pressing priorities on which to focus their resources [Interview 11]. Nor have business groups from areas such as banking or insurance taken a leadership role in focusing attention on data privacy. These groups are instead being drawn into the picture by the international actors, for example being invited to the first national conference on data privacy held by the Council of Europe in 2007 [Interview 2]. This situation may be changing, however: during this research project, one internationally funded Albanian non-profit organization published a policy paper about personal data protection [Agenda Institute 2007].

At the moment, the driving force for data protection accountability comes from international, rather than internal national sources. The main driver is the Stabilization and Association Agreement (SAA) signed between Albania and the European Commission in 2006, which requires Albania to bring its laws—and specifically data protection laws—in line with EU laws within five years. As part of the SAA, European funding is offered to help Albania comply, and the EC issues annual progress reports on the status of the SAA, thus creating considerable pressure for compliance. The new law on data protection is being drafted in order to comply with the SAA, as well as due to the realization that inadequate data protections in Albania can create an obstacle to foreign (especially European) business and investment [Interviews 2, 4 and 9].

⁹ The declarations also name INSTAT, the official statistical agency of Albania, as a responsible authority, but only for purposes of the reports and studies the agency publishes, all of which are anonymous data such as economic reports.

The Council of Europe is the other outside influence on data protection in Albania, organizing conferences and providing expertise and advice for the Albanian authorities [Interviews 2, 4, 8 and 9; see also Sutton 2006 and Patijn 2006]. This influence is based on Albania's membership in the Council and its ratification of the CoE Convention on data protection.

In the case of the E-cJS system, it is also the international actors that have had the most influence on data privacy accountability. At the recommendation of the European-financed justice sector project advisors, the Council of Europe's international experts provided a preliminary analysis and opinion of early proposals for the E-cJS. These opinions led to changes in the legislation and system design, such as not allowing full online access to criminal history records and allowing access for foreign embassies and diplomatic representations only through the Albanian Foreign Ministry [Interviews 1 and 8]. The Albanian Ministry of Justice was thus influenced by the international agencies interested in data protection to increase the level of accountability in the E-cJS system.

While the influence of international organizations on data protection issues in Albania is important, they cannot of course replace the necessary national actors. International institutions have only a persuasive and assisting role, and they naturally have less knowledge and experience with the national conditions, history and culture. National actors with legal authority, funding and resources are needed to fulfill the data protection accountability functions described above. More concretely, the influence of European organizations on the E-cJS system was a catalyst to increasing data privacy, but could not substitute for the active role and interest of the Albanian Ministry of Justice.

The Albanian data protection law and E-cJS law do contain some accountability features that could be important if there were stronger institutional forces to monitor and enforce them. The rights provided to data subjects themselves are one potential force for accountability (see sections 10.4, 10.8, and 10.11 on FIPs *knowledge and consent*, *accuracy and completeness*, and *subject access*). There is a provision for complaint handling by the office of the People's Advocate, though this office has not processed such complaints from data subjects [Office of the People's Advocate 2006: 12].¹⁰ In addition, the law contains provisions for criminal and/or administrative penalties for violations, enforced through administrative appeals or judicial proceedings. Compensation for any actual damages caused by violations can also be claimed through the courts [Law No. 8517: Articles 13, 15-19].

Likewise, the E-cJS law provides that "unlawful interventions" in the criminal records registers or in the dissemination of such data constitute a punishable criminal offense under the Criminal Code. Any event of such "unlawful intervention" must be reported immediately to the "competent organs" [Law No. 9614, Article 10].

The weaknesses of these legislative provisions is revealed by considering the possibility of a violation of data privacy in connection with the issuance of certificates

¹⁰ The People's Advocate has for several years noted the problem of names of accused persons in criminal cases being reported in the media, but this observation does not appear to result from specific complaints about personal data protection; rather it is part of the People's Advocate office general role of monitoring human rights in the public administration [Agenda Institute 2007: 6, citing People's Advocate annual reports 2001-2006].

of judicial status and electronic verification of a self-declaration under E-cJS. Several types of violations are conceivable: unintentional errors in the database, searches in the database for improper purposes, or intentional tampering with the records (such as removal of a name). For unintentional errors, an individual would have considerable difficulty getting a correction. To which entity should the person address the problem? Should he or she go to the People's Advocate Office, as the complaint handler under the Data Protection Law, or to the Ministry of Justice, as the administrative body processing the data, or to the courts, who can issue mandates to the administrative body and/or award damages? The law is ambiguous, and any of these processes would be burdensome and perhaps expensive for an individual, especially if the violation caused no actual damage, like preventing the person from getting a job or license. Moreover, an individual whose name was wrongly *absent* from the list of convicted persons would have no incentive to seek a correction; thus, societal interests are not served by relying only on individuals enforcing their rights to correct errors.

More serious violations, such as searches for improper purposes or tampering with the database, are also problematic to enforce. Lack of an independent supervisory authority means that the only "competent organs" to deal with these violations are the Office of Judicial Status itself, or somewhere higher (though unspecified) within the Ministry of Justice. The law (and the corresponding system design) gives the Head of the Office of Judicial Status great powers over the E-cJS system, including control over passwords, finalization of database entries, changes to authorized personnel, and review of system logs and reports. Yet within the institutional structure of data privacy protection, the only monitoring or supervision of this officer's activities is through the employment relationship. This is inadequate for proper enforcement of data protection interests, particularly when civil service employment systems (hiring, firing, performance review, etc.) are often politicized and lacking in management orientation [Commission of the European Communities 2007: 8].

In addition, the laws are ambiguous concerning what penalties would be applied if a serious violation of the E-cJS system would occur. The Data Protection Law states that any violation, "to the extent it does not constitute a criminal offense" is punishable under Law No. 9697 on Violations of Administrative Rules [Law No. 8517, Article 16]; but the law does not refer to specific sections of the criminal code which might cover a violation and thus is unclear.¹¹ The E-cJS law also contains a reference to violations as a "criminal offense" without specifying any particular section of the Criminal Code. This lack of clarity is an obstacle to enforcement and institutional accountability. Even assuming the Office of Judicial Status or Ministry of Justice discovered and was willing to prosecute a serious violation of the E-cJS system, prosecutors might be reluctant to act when legal ambiguities put the punishment in doubt.

¹¹ A review of the Albanian Criminal Code reveals several possibilities: Article 121, *Intruding groundlessly into someone's privacy*; Article 122, *Spreading personal secrets*; Article 248, *Abuse of office*; or Article 313/a, *Disappearance or loss of file*. But these are described in general terms, not specific to data protection, and must be interpreted by the courts in relation to the Data Protection Law. On the positive side, it should be noted that the provision of penalties for violations constitutes at least a minimum level of compliance with the CoE Convention's requirement that signatories shall establish "appropriate sanctions and remedies" in national law [CoE 1981: Article 10].

All of these problems and deficiencies in the area of accountability also affect the technological measures that might be possible to support accountability. It might be feasible, for example, to build into the system an automatic notification of any unauthorized log-ons or attempts, changes to fingerprint images, deletion of records in the database, and the like—if the “competent [national] authorities” were specified in advance. In the current system design, these logs exist but monitoring them is passive: they must be requested and checked by an administrator or user.

Moreover, the lack of oversight, monitoring and enforcement of data privacy undermines the effectiveness of all the other FIPs, no matter how correct the written regulations are or how well-designed the technology is.

10.3 *Purpose identification principle*

- ☞ An organization should *identify the purposes* for which the information is processed at or before the time of collection

The Albanian Data Protection Law provides that public sector organizations must process personal data only “with a specified, clear and legitimate purpose” [Law 8517: Article 5b]; and the data subject must be notified, before collection of the data, about “the purpose or purposes of the data processing” among other matters [Law 8517: Article 6b]. This is generally consistent with the provisions of both the EU Directive and CoE Convention.

The E-cJS law is silent about the purposes for collecting the personal data, except to refer to the provisions of the Criminal Code and Criminal Procedure Code concerning maintenance and removal of criminal convictions records. As described in sections 9.2 and 9.3 above, the Criminal Procedure Code and Criminal Code provisions mandate the maintenance of criminal convictions records in the Ministry of Justice, including rehabilitations, and describe the conditions and recipients for issuance of certificates [Law No. 7905: Articles 481-484; Law No. 7895: Article 69]. These codes require the maintenance of records for all citizens who have been convicted. The codes also describe permitted recipients of the data in very broad terms: justice authorities, state administration and entities performing public services, as well as prosecutors and defense in certain circumstances. But the only mention of the *purpose* for maintaining convictions data and issuing certificates is for the permitted recipients “to carry out their duties” [Law No. 7905: Article 484]. Such a broad purpose statement would encompass almost any official activity in any public institution, and theoretically any private companies conducting official functions under contract since these could be “entities performing public services”. As a statement of purpose for data collection, this is so broad that it is arguably not “specified” or “clear” as required by national law and international standards.

The requirement of a “specified, explicit and legitimate purpose” [EU 1995: Article 6b] applies even where the data subject’s consent is not required (see section 10.4 concerning the ‘legal duty’ exception to consent). European countries’ laws allow creation of criminal convictions registries without consent, but most of these laws specify for what purposes records checks can be made [Patijn 2006] (such as employment, insurance, or court proceedings [Sutton 2006]) rather than allowing them for any public purpose whatsoever.

It is true that individuals learn the purpose for which the data will be used when they encounter a request for a certificate or self-declaration during a particular

administrative process. However, this purpose is determined long after the data collection. International standards require purpose determination before data collection occurs.

Moreover, the data collection by the Judicial Status Office occurs without any specific notification to convicted persons about purpose or any of the other matters required by the Data Protection Law. Convicted persons may be presumed to know generally that the law that requires maintenance of a convictions registry, without special notification. But that is not the same as providing advance notice of the specific, clear and legitimate purposes for which the data will be used—employment, insurance, licenses, education or the like; and it is not the same as providing the other notifications required by the Albanian Data Protection Law, consistent with international standards—name and address of the processor, types of data processed, users of the data, possibility of transfer to third countries, and security conditions.

The fact that specific, clear and legitimate purposes for criminal convictions data processing are not specified in the Criminal and Criminal Procedure Code provisions or the E-cJS law reflects the fact that data privacy awareness is low and is not currently a factor in the legislative process. There is no oversight body, nor are there any public or private interest groups with the interest, authority and resources to press the issues into the debate about new or revised legislation. The same is true for the public institutions collecting and using the data. Thus, there has been no administrative consideration or public debate in Albania about the uses of certificates or verifications of judicial status. For instance, some societies would not consider criminal convictions relevant for admission to higher education. British law allows disclosure of rehabilitated convictions in connection with medical or other professional licenses [Sutton 2006]; Holland restricts employers' access to conviction details depending on the particular type of crime and its relevance to the particular type of employment [Patijn 2006]. An awareness of and accountability for personal data protection would encourage open, informed policy debates about the purposes for which criminal convictions history may be demanded and used.

Interestingly, the technological design of the E-cJS system actually has a positive influence on the purpose identification principle. The interface for users in authorized institutions includes a field where the user can enter a "purpose" for the records search, and this purpose will be maintained in the system logs. It is not known what was the motivation for including this field in the system, but in practice it provides some record of the reasons for data processing and focuses attention on the purpose. Of course, this technological feature does not ameliorate the purpose identification problems described above.

10.4 Knowledge and consent principle

- ☞ An organization should only collect personal information with the *knowledge and consent* of the individual (except under specified circumstances).

While this principle is stated in terms of requiring data subject consent as a general rule, in fact it is often the exceptions that are most important for data processing by public sector entities for administrative purposes. This is because in most international legal and policy instruments, one of the exceptions to the consent rule

is the exercise of a legal duty of the data controller. “Most often, in the public sector, processing will be for the purpose of exercising functions prescribed in statute or otherwise of a public interest nature” [Woulds 2004: 14], and thus exempt from the consent requirement. In fact, this principle is one of the least consistent across international instruments, sometimes being expressed only as a right for a data subject to object to processing in certain instances, or as a pre-condition for certain uses or disclosures of personal information. The CoE Convention does not mention prior consent at all.

This fair information principle is expressed in the Albanian Data Protection Law, Articles 10 and 11, in accordance with the principle of consent stated in Article 35 of the Constitution. Article 10 of the Data Protection Law states the general rule that the data subject's prior consent is required for personal data processing (and prior written consent for sensitive types of data), while Article 11 provides the exceptions to the general rule [Law No. 8517]. Article 11(b) states the exception for “when the processing of data is necessary for the fulfillment of the data subject's own legal obligation”, but this exception apparently does not cover legal obligations of public entities as does the EU Directive. Instead, the Albanian law, Article 11(c), includes an exception not found in the EU Directive or other international instruments, for data “extracted from public registries, or from lists, acts or documents publicly known to everyone”. This latter exception may apply to the E-cJS data, because the data are taken from the criminal conviction records of the courts, which are publicly accessible to everyone. Interpreted in this way, the law would permit processing of the E-cJS database without prior consent of the data subjects. Thus the Albanian legislation would reach the same result as the EU Directive or CoE Convention, but through different provisions and reasoning.

This analysis reveals an important ways in which the Albanian law is not in conformity with the EU Directive. While these differences would not cause a different result for the E-cJS system, they may have unintended effects in other situations. In particular, the lack of a consent exception for legally imposed duties of data controllers, and for activities carried out in the public interest, may mean that certain data processing activities could be unnecessarily subject to a prior consent requirement. To take just one commonplace example, the law would technically require the public administration to obtain pensioners' prior consent to process their monthly payments. Having such technicalities on the books leaves public institutions in the position of either failing to follow the letter of the law in practice—opening up the possibility of legal challenges and lack of respect for the law—or following the rules as written, with unnecessarily high expenditure of public funds. Either way, in a privacy context, the risk is a lack of trust by the public [Bennett 2003: 49-52].

Under both international standards and national data protection law, processing of the judicial status records could conceivably occur without prior consent of the data subjects.¹² Nevertheless, the E-cJS law does in fact require prior consent: under that law, a person must provide a self-declaration and must authorize the receiving entity to verify the information through an online check (see the form in Figure 3). This consent requirement is actually quite strong, since it is not subject to any

¹² For the issuance of paper certificates to a person about his or her own criminal history, there is *de facto* consent, because the person in question is requesting the processing of his or her own data.

exceptions. Furthermore, the requirement is consistent with the provision of the Data Protection Law [Law No. 8517: Article 10] that consent to processing of sensitive data must be in writing.

On the other hand, the E-cJS law does not include a provision similar to the Albanian Data Protection Law that the person's consent (i.e., the self-declaration/authorization form) "shall be valid only if given *freely* or in cases where the data subject has been notified"¹³ in advance about the nature, controllers and users, purposes, possible foreign transfer and security conditions for the data processing [Law No. 8517: Articles 10 and 6, italics added]. This omission is of concern because "the individual data subject will often have difficulty in understanding all the consequences of such consent" [Blume 2001: 20], or may be pressured into consenting [Bygrave 2002: 58-9]. Thus, the E-cJS law, while strongly mandating prior consent, still leaves open the possibility that the consent may be uninformed or coerced (concerning the latter, see further the discussion of "enforced access" in section 10.6 on the finality principle). Likewise, the EU Declaration has been criticized for the same omission, with the observation that the matter of consent deserves "careful study within data protection theory" [Blume 2001: 20].

10.5 *Limited collection principle*

- ☞ An organization should *limit the collection* of personal information to that which is necessary for pursuing the identified purposes.

The Albanian Data Protection Law states that data processing shall be conducted "making use of only such data as are relevant and necessary to achieve the purpose of processing" [Law No. 8517: Article 5(dh)¹⁴]. Both the EU Directive and the CoE Convention contain similar provisions.

Because of the uncertainty surrounding the purposes for which judicial status certificates are issued and used (see section 10.3), it is difficult to say whether the information collected and processed in the E-cJS system are relevant and necessary for these purposes. However, the information contained in the bulletins sent to the JSO for entry into the E-cJS system are "abridgements" of the original court conviction records [Law No. 7895: Art. 481]. Considering the ordinary purposes of a criminal convictions registry in the public sector, like employment or licensing, the types of data collected (see section 9.3) do not seem excessive.

However, the bounds of what is or is not excessive data processing in relation to the particular purposes can change with time and technology. For example, the E-cJS system currently is designed to collect and process data about a person's date and place of birth, as well as mother's and father's name. This is used as a control on identity where there are multiple persons with the same name. But Albania is now working on a system for national identity cards, which will provide unique identifiers (numbers or biometrics, for example) for each citizen. When that system is

¹³ Although worded awkwardly, this provision can most reasonably be interpreted to mean that a person's consent can be presumed to be freely given if the person has received the prior notification information specified by the law.

¹⁴ In Albanian language, *dh* is a separate letter of the alphabet, representing a distinct sound. It comes after the letter *d* in the alphabet. Therefore, it is used as a separate subsection designation in the Albanian laws.

implemented, it might be considered excessive to collect and retain data about a person's birthplace and parentage, or even birth date, because the unique identifier should be sufficient.

Another evolution might be caused by the technology improvements being made in the courts, which are implementing case management software. At some stage, the two computer systems might be integrated or connected, so that two databases would in fact be unnecessary; rather, certificates of judicial status could be created directly from the integrated database. In that situation, it might be considered irrelevant and unnecessary for the JSO to keep any records or databases at all, and the only personal data processing it performs would be creation of certificates.

The changing nature of this standard means that organizational awareness of information privacy issues is required within the Ministry of Justice and other public institutions. Those who design, work with and control systems such as the E-cJS must continually revisit the issues as conditions change.

10.6 *Finality principle*

- ♣ An organization should not use or disclose personal information for purposes other than those identified, except with the consent of the individual.

The principle that data processing should not occur beyond the original specified purposes, appears in both the EU Directive [EU 1995: Article 6(b)] and the CoE convention [CoE 1981: Article 5(b)]. In the Albanian Data Protection Law, it is expressed in Article 5(ç),¹⁵ stating that personal data must be processed "without exceeding the purpose for which they are processed..." [Law No. 8517].

As with the *limited collection* principle, it is difficult to assess this principle as exhibited in the E-cJS system, due to the lack of clarity about the purposes of data processing. However, the E-cJS legislation has enlarged the potential purposes for use of judicial status certificates to include both private companies and foreign users, without full consideration for the implications for this principle of *finality*.

The Council of Ministers order listing the institutions authorized for fingerprint access includes some institutions that could be outside the original purposes envisioned by the Criminal Procedure Code. The list includes foreign diplomatic representations (via the Ministry of Foreign Affairs), as well as the representation offices of the European Union, Council of Europe and NATO in Albania [Council of Ministers 2006]. While these institutions could be considered "entities charged with public services", which may receive judicial status certificates according to the Criminal Procedure Code, they are nevertheless foreign entities. Foreign entities are probably not within the scope intended by the Criminal Procedure Code provision, nor within the usual expectations about who would use the information.

Additionally, although it has not happened yet in actual practice, the E-cJS law permits the Council of Ministers to authorize private companies, including foreign companies, to have fingerprint access to the online e-certificate system [Law No. 9614: Article 8.2 and 8.3]. Private companies that do not have fingerprint access

¹⁵ The letter ç is a separate letter in the Albanian alphabet. See footnote 14.

could request e-certificates by e-mail or post [Law No. 9614: Article 8.4]. (E-mail or postal requests are not a current reality, partly because the JSO does not have e-mail access and partly because the law is not generally known by those companies who might be interested in doing so.) Issuing e-certificates to private companies significantly expands the possible uses of personal information, since the Criminal Procedure Code contemplates their use only by state and public institutions, not private companies [Law No. 7905: Article 484]. Under the new law, banks, insurance companies, private employers, private educational institutions, and even private individuals could (in theory) obtain judicial status certificates about other individuals, if they obtain a self-declaration and search authorization form (Figure 3) from the person. For fingerprint access, the Council of Ministers authorization places limits and controls on the data processing; but e-mail or postal requests have no such restrictions and there is no requirement to state a purpose in the request. Thus, the law creates the potential for “so-called ‘enforced access’ whereby persons are pushed into utilising their access rights in order to provide a body on which they are dependent (e.g., employer or insurance company) with personal information normally unavailable to it” [Bygrave 2002: 65; Patijn 2006]. The problem of “enforced access” has been of concern in the UK, Holland, Denmark and the drafts leading up to the EU Directive [*id.*; Bennett 2003: 54; Blume 2001: 20].

Furthermore, the E-cJS law permits expanded access for foreign entities, public or private, without an analysis of the level of data protection present in the foreign countries as envisioned by the CoE Convention [CoE 1981: Article 12], the CoE Additional Protocol [CoE 2001: Article 2] and the Albanian Data Protection Law [Law No. 8517: Article 14]. The fact that the E-cJS law potentially permits sensitive personal data to be transmitted to *any* entity in *any* other country, and the practical impossibility of assessing the levels of data protection in all countries, demonstrates the breadth of the data processing permitted under the law.

The expanded fingerprint access for foreign public entities authorized by the Council of Ministers, and the potential for “enforced access” created by the Albanian E-cJS law, and the potential for cross-border data transfers illustrate a problem pointed out by some in connection with implementation of the EU Directive in national laws—that is, its wording “could lead to data processing being authorised by laws which have not given due consideration to data protection issues” [Blume 2001: 21]. The EU Directive allows personal data processing when it is done “in the public interest or in the exercise of official authority” [EU 1995: Article 7(c)], which should be interpreted as allowing processing by public authorities under statutory law. But this creates a danger of undermining personal data protection when the legislative body does not pay proper attention to data protection principles when shaping the statutory law. Personal data protection requires thorough, careful consideration of data protection principles when crafting any legislation that implicates personal data processing.¹⁶ One role of a national data protection authority is to ensure such principles are

¹⁶ This is not to say that data protection principles were not considered at all when drafting the E-cJS legislation; to the contrary, preliminary opinions were provided by two European experts [Sutton 2006; Patijn 2006] and the Ministry of Justice made changes in the legislation because of them [Interviews 1 and 8]. But data protection is a novel concept in Albania, there is no experience with its principles in practice, and there is no supervisory authority to provide specialized advice. Under these circumstances, gaps are understandably bound to arise.

considered during the legislative process [Blume 2001: 21], but this authority is missing in the Albanian state.

10.7 Limited retention principle

☞ An organization should *retain* information only as long as necessary.

International legal instruments express the principle that personal data processing should be done so that it “permits identification of the data subjects for no longer than is required for the purposes” for which those data are collected, stored or further processed [EU 1995: Article 6(e); CoE 1981: Article 5(e)]. In accordance with these instruments, the *limited retention* principle is also present in the general Albanian Data Protection Law [Law No. 8517: Article 5(ç)], which states that data processing should take place “for a period no longer than necessary to achieve the purpose of processing.”

The quoted statutory language makes clear that this principle, like the principles of limited collection and finality, is closely linked to the defined purposes for which the personal data is used. As discussed above, the purposes for which the E-cJS system processes personal information are not clearly defined; but the system does include specific limitations on the retention of personal data by virtue of the applicable Criminal Procedure and Criminal Code provisions. These provisions specify that certain convictions records are cancelled or registered as rehabilitated upon certain events or after a certain amount of time (see section 9.3). The practice of the JSO includes at least registering rehabilitated convictions in accordance with these legal provisions [Interview 3].

In this respect, the technology design has the potential to promote the privacy principle more than it does currently. For example, the system could build in automatic review dates for conviction records that should be deleted. For example, the Criminal Procedure Code provides that

There shall also be cancelled the notes related to:
...b) the decisions of acquittal or dismissal on expiry of ten years from the date on which the decision has become final;
c) decisions of punishment for contraventions when a fine penalty is involved, on expiry of ten years from the day when the decision has been executed [Law No. 7905: Article 483].

The technology could assist the JSO in carrying out these legal rules by automatically creating messages for the Super-user noting that ten years had expired from the date of a decision of acquittal, dismissal or execution of a fine, and giving the option to delete the record (naturally, with error prevention and security features). This is another example of the interaction of technology design as part of the privacy regime.

10.8 Accuracy and completeness principle

☞ An organization should ensure that personal information is kept *accurate, complete and up-to date*.

The Albanian Data Protection Law includes a clear statement that personal data must be processed “in an accurate way and on the basis of updated data” [Article 5(c)], in keeping with similar provisions in the EU Directive [EU 1995: Article 6(d)]

and CoE Convention [CoE 1981: Article 5(d)]. While the Albanian Criminal and Criminal Procedure Codes do not specifically mention accuracy and completeness of data, the E-cJS law mandates that “the Head [of the JSO] takes measures for the electronic register to be updated every 24 hours” [Law No. 9614: Article 5.3].

The legal provision for daily updating of data seems admirable from the standpoint of accuracy and currency; but it may be over-ambitious in practice. The current practice of the JSO is to update the database on an ongoing basis as bulletins are delivered by the courts, but the office does not now impose a 24-hour data input deadline. [Interviews 3, 5 and 6]. This is also reflected in the design of the database system, which incorporates a weekly check of records input before they are finalized (see section 9.4.1). Since the new E-cJS system was in the pilot testing phases at the time of this research, it was impossible to tell whether the JSO would be able to meet the daily updating standard in practice after full implementation.

Another practical problem with the accuracy and completeness of the E-cJS system is the search functionality. The Albanian alphabet contains special characters (*ç* and *ë*) and combination letters (*dh, gj, ll, nj, sh, rr, th, zh*) which can create difficulties in designing a search system and using it successfully. In addition, electronic search functionalities are often imperfect and require user finesse in order to return accurate results, as any user of Google's internet search or Microsoft Outlook's address book can attest. Furthermore, the system for registering name changes in the courts and reporting them to other authorities may not always function optimally, thus compounding the difficulties with name searches. Some problems with inaccurate results on judicial status certificates have been reported with the current electronic database system¹⁷, and similar problems can be anticipated with the new one. These problems apparently arise due to typing errors in search requests and misspellings of names either in records or in search requests, or from unrecorded name changes.

The technological design of the E-cJS system includes a number of measures designed to increase accuracy in data input, such as double data entry and verification by a supervisor before records are finalized (see section 9.4.1). The search function has also been designed to increase user friendliness, by including automatic partial word searches and alternative spellings [Interview 3]. However, human error probably cannot be eliminated 100%; and error can also be introduced in the creation and transmission of bulletins by the courts, and by user error when conducting searches.

Whatever their cause, and despite the technological measures in place to avoid them, errors in the E-cJS system may be difficult to detect and correct. The only time they might be discovered is when requests for certificates or verification of self-declarations are made. Individuals with a clean criminal history whose records incorrectly show the presence of convictions will have adequate motivation to complain and have the records corrected; but those whose convictions inaccurately are missing from the records have little incentive to ask for correction. Furthermore, when third parties, such as prosecutors or the institutions authorized by the Council of Ministers, request judicial status verification directly, they are not in the same

¹⁷ Based on a conversation between the author and a member of the General Prosecutor's office, which frequently requests such certificates.

position as the individual to recognize a false negative result. To put it more concretely, if the ministry official performs a search of the E-cJS system and it returns a result of "no convictions" for a person, the ministry official has no way of knowing whether this may be the result of an incorrectly typed search term, and the individual is very unlikely to point out the inaccuracy. The number of occasions when this problem occurs may be infrequent, but they could lead to some quite unfortunate consequences when important official decisions are based on the results. Such a situation indicates the desirability of having an independent supervisory authority which could perform random checks and inspections to detect potential errors and assess the adequacy of measures to prevent them.

10.9 Security principle

- ☞ An organization should protect personal information with appropriate *security safeguards*.

Security of personal data is a clear principle running through all international policy and legal instruments, as well as the Albanian national laws for data protection and the E-cJS system. The notion of *data security* in relation to data privacy has "caused considerable confusion" and the two concepts have sometimes (mistakenly) been used interchangeably [Bennett 2003: 18]. Used correctly, personal data *security* refers to protecting data against various risks, such as unwanted loss or destruction, unauthorized access or improper disclosure; while data privacy encompasses a much broader field of personal rights and principles.

In other words, data security is a necessary but not a sufficient condition for information privacy. An organization might keep the personal information it collects highly secure, but if it should not be collecting that information in the first place, the individual's privacy rights are clearly violated [*id.*].

So the principle of data security is a subset of the various principles and rights encompassed by information privacy. The EU Directive [EU 1995: Article 17] expresses the principle as a requirement that a personal data

...controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Thus, the European policy standard specifies the risks which must be protected against, and provides flexible parameters for the specific security measures that must be taken. Notably, this standard identifies both technological and organizational measures as necessary to a sufficient level of data security. By expressly requiring a balance between the nature of the risks and the level of security measures, the Directive implicitly requires a greater level of security for data of a *sensitive* nature.

The CoE Convention is less specific about both the risks and the measures: "Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination" [CoE 1981: Article 7].

The Albanian Data Protection Law and the E-cJS law also include provisions about data security. The Data Protection Law's main clause relevant to security, titled "Security of data processing", requires that

The person in charge of the personal data must implement all technical and organisational measures to protect these data against any damage or loss, whether accidental or unlawful, against any unauthorised alteration, disclosure or access, in particular where the processing involves networked information technology, and against all other unlawful forms of processing. In the case of sensitive data, such measures shall ensure a level of security proportional to the risk posed by the processing and the specific nature of these data. [Law No. 8517: Article 9]

While this language is almost the same as the EU Directive's, and more explicit than the CoE Convention provision, it leaves some potential gaps in legal interpretation. The literal language mandates implementation of "all" security measures, but it is not clear whether this means all *reasonable* measures or all *possible* measures. The latter interpretation would be costly and difficult to implement, since technical and organizational measures can be costly, especially for early technologies. It could be that a court would interpret the law to mean only reasonable measures must be implemented, but the formulation above leaves the issue open to interpretation.

Admirably, the Albanian law also recognizes the need for particular security concern where personal data are transmitted over a network, as does the EU Directive. This type of provision acknowledges the risks of network transmission, such as interception or corruption of data. In the E-cJS system, network security is provided by using the E-gov Net dedicated cable connections or a VPN where transmission is done over the internet. It is not known whether a firewall is in place, but if not this could easily be accomplished.

Unlike the international instruments, the Albanian law also specifies the personal and professional qualifications of data processors, apparently as a security measure: "the person in charge of data processing and any other person involved with the data processing shall be a person with experience in data processing, with a high level of moral integrity and with technical aptitude, in order to guarantee the security of the data" [Law No. 8517: Article 7]. Since this standard is applicable for the entire public sector, it is difficult to see how it could be fully implemented in practice, since the definition of data processing is so broad as to include tasks that would often be carried out at lower functionary levels. Again, a proportionality requirement would be desirable, to balance the level of experience and competence against the nature of the data processing performed. A ministry clerk who performs data input does not need a degree in computer science, but should be trustworthy and trained, whereas higher officials deciding the design and implementation of whole data processing systems must have education, training and experience in records management, computer technology, organizational management and legal requirements.

The E-cJS law also treats data security as an important principle, with the emphasis on organizational measures of security. Article 4 of the law limits processing of convictions data in the E-cJS system to persons authorized by the Head of the JSO, and mandates that all actions with respect to E-cJS data “shall be done through the levels of security determined by a person licensed in this field, and through entry codes that are administered only by the head of the [Judicial Status] Office.” The article also prohibits the Head of the JSO “from giving data to third persons about the level of security.” For access by authorized persons outside the JSO, the law mandates “several levels of security according to Article 4”, as well as specifically mandating fingerprint access control [Law No. 9614: Article 8].

In addition to mandating fingerprint access for online verifications, the E-cJS Law mandates that the “levels of security” needed to perform “entry of data, their preservation, the performance of logical actions on these data, their protection from changes, their receipt and their dissemination” should be determined by a licensed person [Law No. 8517: Article 4.2]. It is not clear what is meant by “licensed” since there is no licensing scheme for computer professionals in Albania.

Another organizational security measure mandated by the E-cJS law is that “when an unlawful intervention is found in the register of judicial status, the competent organs must be notified immediately” [Law No. 9614: Article 10.1]. The law does not specify which organs are the competent ones, however, or the manner or time in which they should be notified. The consequences of unlawful intervention are specified as carrying criminal penalties under the Criminal Code, but without specifying which specific Code sections or penalties (a number of which could conceivably apply).

A reasonable degree of security measures exists in the E-cJS technology. As required by the law, users must access the system by fingerprint scan. Fingerprint technology can be a relatively secure means of controlling access to a computer system; it is highly difficult, though not impossible, to spoof [OECD 2004: 13]. It can provide one factor in a multi-factor identification system, along with other factors such as a card-key, token or password. The more factors required for identification, the more secure the access method [*id.*]. The fingerprint image is one strong factor for identification of users of the E-cJS system, but the system design will not require the user to enter a password together with the fingerprint for logon (though the capacity does exist in the software) [Interviews 3 and 6]. In addition, the system stores fingerprint scans in the authorized user's PC, rather than in a central server, and requires use of that particular PC in order to access the system, so that the IP address of that PC constitutes a second factor for authentication. As mentioned above, VPN technology and presumably a firewall will be used for internet connections. Other physical security measures, like fire- and water-proofing may be more difficult to achieve, given the state of the existing facilities.

Organizational security measures are also present in the Ministry of Justice and JSO, such as creating database backups, performing system maintenance, locking server cabinets, and monitoring system tracking logs, and instructing users to restrict access to their PCs and fingerprint scanners and to log off the system immediately after each use [Interviews 3 and 6]. These measures could be made stronger by having written policies and procedures that can be used as reference by the current personnel and passed along to others in the future.

Another organizational measure relates to the Head of the JSO, who has the sole authority under the E-cJS law and software to perform a number of system functions, like activating authorized users or final approval of database entries [Interview 3]. Limiting authority over certain system functions to one person has the security advantage of restricting the possibilities for error or abuse; however, it must be balanced against the risks and consequences if there is error or abuse by that one person. No supervisory authority inspects the actions of the JSO concerning privacy and security of data, and organizational controls such as performance evaluations and management accountability are weak in most Albanian ministries. Technological means such as system logs have a regulatory effect on the JSO Head as Super-user, but the Super-user also has a good deal of authority within the software application.

Despite technical and organizational security measures, the risk of human error and abuse cannot be eliminated fully. Criminal records data is essential for a number of important public functions, and can affect individuals in quite significant ways. The pressure and temptations to breach security could be severe, given the critical nature of these data. There are several points in the business processes where security weaknesses could arise in the E-cJS system, entirely aside from the question of fingerprint access: for example, network connections, paper data transmissions, data entry, presentation of ID by requesters, and creating backups are some points where the system could be vulnerable to risks of error, attack, interference, or falsification.

The E-cJS Law suggests that organizational and technical system security should be based on an overall plan developed under the direction of one responsible person, who is a trained, educated and experienced professional [Law No. 9614: Article 4.2]. However, instead of this type of overall planned vision, security in the E-cJS system appears to be occurring on an *ad hoc* basis, with divided responsibilities. The drafters of the law obviously considered security important, but they could not foresee the specific technological and organizational security needs of the system before it was developed or as it could be modified in the future. The software designers have built many security features into the software application, but they are not responsible for the networks, servers and client computers on which it operates [Interviews 3 and 6], nor are they responsible for organizational policies. The ministry staff, such as the Head of the JSO and the IT director, have the organizational knowledge to develop security standards and policies, but not the technical help and support they would need to implement a comprehensive security plan, due to budget constraints, understaffing and poor physical conditions. Written policy or procedures about system security do not exist, other than what is written in the law itself. Thus, a number of people have contributed piecemeal to the security picture of the E-cJS system, but without an overall evaluation and comprehensive plan.

10.10 Openness principle

- ☞ An organization should be *open* about its policies and practices and maintain no secret information system.

The principle of *openness* with regard to personal data processing is closely connected with the principle of *subject access* (below). The idea behind the principle is that there should be no organized system for collecting or utilizing data related to

individual persons, of which those persons are unaware. Many of the international instruments treat subject access rights as concurrent with openness of data processing, meaning that data files must be opened to individuals if they ask. This is the case under the CoE Convention, which mandates that “any person shall be enabled...to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file” [CoE 1981: Article 8a]. The Convention does not impose positive obligations of data controllers towards data subjects or a supervisory authority to notify or register their processing activities.

The EU Directive goes further, based on the idea that the existence of data files should be publicized independently of individuals' rights of access to that data, because knowledge is a prerequisite for exercising those rights [Bygrave 2002: 75-77]. Thus, the EU Directive dictates that data controllers must notify individuals from or about whom they collect data—without a request from the individual—concerning the identity of the controller and purposes of processing [EU 1995: Articles 10-11]. In addition, data controllers must notify the supervisory authority of their personal data processing activities prior to undertaking them, with a number of permissible exceptions; supervisory authorities must maintain registers of these notifications. [EU 1995: Articles 18-21].

The European member countries have enacted national legislation implementing these principles, with varying approaches and significant exceptions for a large number of data processing types. European countries use a number of regulatory approaches, combining prior registration with supervisory authorities, prior licensing of data processing, and notification of data subjects in various ways for various types of data. Often, sensitive data is treated exceptionally [Kuner 2007: 248-59, 471, Appendix 11]. Norway is an example of a country that requires issuance of a license before data processing can be carried out, including on some sensitive data, but Norway exempts processing by public entities when it is required by law [Schartum 2001: 101].

The Albanian data protection legislation takes an approach somewhere between the CoE Convention's passive openness principle, and the EU Directive's extensive active reporting requirements. The Albanian Data Protection Law requires prior notification to individuals from whom personal data is collected [Law 8517: Article 6]. The notification must include an extensive set of information:

- a) the name and address of the person in charge of data processing, as well as that of other persons who will process the data;
- b) the purpose or purposes of the data processing;
- c) the category or categories of personal data to be processed;
- ç) the persons or categories of persons who will use the data;
- d) the possibility of transfer of these data to third countries;
- dh) the fulfillment of conditions for the security of data processing [*id.*].

The requirement for prior notice, as well as the types of information required to be notified, are more comprehensive than the CoE Convention; and the Albanian law does not provide for the large number of exceptions as does the EU Directive. While this could be considered as a positive factor for strong personal data protection, it would likely cause a number of practical difficulties and unintended consequences. For example, the law would technically require all tax authorities to provide this

notification prior to collecting tax data; all public entities to notify their employees before processing personnel files; and all educational institutions to notify their students before compiling class rosters and course registrations.¹⁸ This type of activity is so pervasive, is so unlikely to damage the personal data interests of individuals, and would involve so much administrative bureaucracy on the part of the state, that good personal data protection principles and standards would permit exceptions. Thus, the Albanian law can be considered over-inclusive in this regard.

Neither the E-cJS law nor the relevant Criminal and Criminal Procedure Code provisions mention data subject notification in any particular way. However, the judicial status records and certification/verification system cannot be considered secret or undisclosed data processing, because they are declared by law to exist. Moreover, persons who provide a self-declaration and authorization for their records to be checked will thereby be informed that the files exist and that their personal data will be processed. This may not suffice to create the conditions for informed consent to the processing (as discussed in section 10.4 on the *knowledge and consent* principle) but it is enough to satisfy the principle of *openness*.

10.11 **Subject access principle**

- ☞ An organization should allow data *subjects access* to their personal information, with an ability to amend it if it is inaccurate, incomplete or obsolete.

Albania is one of only a few countries to mention personal data privacy rights in its constitution [CoE 1981: Explanatory Note, par. 5]. The constitutional provisions specifically address the *subject access* principle:

3. Everyone has the right to become acquainted with data collected about him, except for the cases provided by law.
4. Everyone has the right to request the correction or deletion of untrue or incomplete data or data collected in violation of law [Republic of Albania 1998: Article 35].

The Data Protection Law transfers these constitutional principles into law, by giving every person “the right to be informed at any time about the procedure of processing of his/her personal data,” and to receive a response within 10 days [Law No. 8517: Article 12]. Furthermore, data subjects are “entitled to request the correction or deletion of data that are false, incomplete or that are collected in violation of the law” and to receive a written response within 15 days [Law No. 8517: Article 13]. A special remedy is provided in the event that the request for correction or deletion is denied: the request continues to accompany the original data for as long as they are used or kept [*id.*].

Similar provisions are contained in the EU Directive [EU 1995: Article 12] and the CoE Convention [CoE 1981: Article 8].

¹⁸ Based on the author's own personal observations of public authorities in Albania, such notifications are not occurring in actual practice anywhere in the public sector. This observation is in line with the reported low level of awareness about personal data protection in Albania in both public and private sectors.

Further, the Criminal Procedure Code of Albania expressly gives data subjects access to their own data about criminal convictions history [Law No. 7905: Article 484.3], and this is widely practiced in Albania as demonstrated by the long queues at the JSO. The E-cJS law preserves this right for printed certificates of judicial status, but does not extend it to obtaining electronic verifications or certificates [Law No. 9614: Article 6.2]. However, the right to obtain correction or deletion of errors is not expressly addressed in either of these laws. In the event that a citizen discovered and was interested in correcting an error in the judicial status records about himself, the procedures for doing so are unclear and enforcement would be difficult (see earlier discussion in section 10.2 on accountability).

Nevertheless, it can be said that Albania is complying at a basic level with national laws and international standards for *subject access* with respect to the judicial status database and certificates system.

10.12 *Sensitivity principle*

- ☞ Processing of certain types of data regarded as especially *sensitive* should be subject to more stringent controls.

The principle recognizing the need for special treatment of sensitive data is embodied in a number of international instruments (see Attachment 5). Both the CoE Convention and the EU Directive, as well as Albanian law, include it.

The CoE Convention concerns “special categories of data,” defined as “personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life...[and] personal data relating to criminal convictions” [CoE 1981: Article 6] These types of data “may not be processed automatically unless domestic law provides appropriate safeguards.” The Convention does not indicate what is “appropriate,” leaving it up to national law; but presumably the level of protection ought to be greater than the other provisions of the Convention for ordinary personal data types. Nor does the Convention specify when or how exceptions may be allowed to this general rule.

The EU Convention defines the categories of sensitive personal data similarly [EU 1995: Article 8.1], but conspicuously adds “personal data revealing...trade union membership” to the list¹⁹ and omitting criminal convictions data. The latter are dealt with separately; “processing of personal data relating to offences, criminal convictions or [court-imposed penal] security measures may be carried out only under the control of official authority,” but national law may provide exceptions if it also provides “suitable specific safeguards.” Moreover, “a complete register of criminal convictions may be kept only under the control of official authority” [EU 1995: Article 8.5].

¹⁹ There is some debate about whether the list of sensitive data categories in the EU Directive are meant to be exhaustive, or whether Member States may add others, particularly in order to preserve protections existing in prior law [Bygrave 2002: 68-69; Blume 2001: 23; Saarenpää 2001: 55]. For example, information about membership in associations other than trade unions may be considered sensitive; and it can be argued that the notion of sensitivity should change with time, culture, social values and processing context [Bygrave 2002: 68-69].

As with the CoE Convention, the Directive does not specify what type of safeguards are suitable to criminal convictions data. However, it does specify safeguards for other types of sensitive data. Processing is permitted only in certain enumerated instances [EU 1995: Article 8.2], and when (and if) processing is based on the subject's consent, the consent must be "explicit."

Member States have handled the permitted exceptions to the *sensitivity* principle, and the processing of criminal convictions data, in various ways [Kuner 2007: 101-107]. In particular, some countries have restricted processing of data relating to criminal matters in ways that limit the extent to which companies can screen potential employees' criminal history [Kuner 2007: 103; Saarenpää 2001: 55 (concerning Finland)]. What is important for this analysis is that both the EU Directive and the CoE Convention indicate that criminal convictions data, particularly when it is kept in a comprehensive register system, deserves special treatment due to the risks it presents for information privacy.

The Albanian legislation follows the pattern envisioned by the EU Directive, defining similar types of sensitive data in the general Data Protection Law, while regulating the criminal convictions register in special statute (the Criminal Procedure Code and E-cJS Law). Some confusion is caused by the fact that the Data Protection Law defines "sensitive personal data" to include "data such as...criminal status," [Law No. 8517: Article 2b], while the same data is also governed by the specific legislation (this is fully discussed in section 10.1 with respect to applicability of the Data Protection Law to the judicial status register system). Like the EU Directive, the Albanian Data Protection Law requires that consent to processing of sensitive data must be given in writing by the data subject; but it does not prohibit or provide exceptions for processing of sensitive data otherwise.

Considering the widespread nature of the demand for and issuance of judicial status certificates, as has been the practice in Albania, one might question whether the prevailing legal and administrative culture considers this information to be of a sensitive nature. Early proposals for the E-cJS system contemplated an online database that would potentially be open to all, at least to verify whether a person did or did not have criminal convictions [Sutton 2006; Patijn 2006; Interview 1], but this idea was quickly abandoned once the privacy concerns were pointed out [Interviews 1 and 8]. These early proposals may have been shaped by the influence of American laws and standards, on which the self-declaration was based [Interview 8].

The original E-cJS proposals for open online access were based on the idea that criminal convictions history should be publicly available, because all criminal convictions are already public court records [Patijn 2006], under the constitutionally protected right to a "fair and public trial" [Republic of Albania 1998: Article 42.2]. These proposals ran contrary to European information privacy standards, which consider criminal history records to be sensitive data, and require data registries to be administered only by official authority [EU 1995: Article 8] and criminal court decisions to be published anonymously using only the offender's initials [Patijn 2006]. But other countries (notably the USA) follow the opposite approach, similar to the original Albanian proposals, and based on similar constitutional logic. A number of states in the USA allow public criminal records searches online or by mail (see, for example, [Virginia Dept. of State Police 2007; State of Colorado 2007]), and there are myriad commercial firms that offer consolidated criminal records searches of all 50 states and federal levels for a fee (see, for example, [SearchMyRecords.com

2007; Dehnel & Associates 2007]). These are often used for hiring purposes by private employers. Even the Electronic Privacy Information Center (EPIC)—an American non-governmental advocacy group which seeks to limit publication of personal information from all types of public records in electronic form—recognizes “the strong interests of the public in having access to all aspects of criminal prosecutions” [EPIC 2001]. In the case of electronic court records of criminal cases, EPIC proposes restricted access only to “sensitive information such as pre-indictment documents, pre-sentence reports, plea agreements, and unexecuted warrants” whereas “the public would still have access to the indictment and the final decision of the court” [*id.*].

The stark contrast between the American and European approaches may be due to societal differences in the way criminality and criminal rehabilitation are viewed. The European approach is based on the view that a person may be rehabilitated into orderly society after undergoing criminal punishment, and that his or her privacy should be protected in order to encourage this [Patijn 2006]. The American view is otherwise, emphasizing punishment more than rehabilitation and promoting the public's right to know the names of convicted criminals in order to protect themselves and their families.²⁰

The dramatic contrast between these attitudes towards publication of personal data about criminal convictions illustrates that social values and attitudes towards information privacy do differ quite drastically on the matter, and can strongly affect public policy, laws and regulations. It also illustrates the strong influence that European international organizations have had on the privacy debate and the regulatory regime in Albania. Furthermore, it is an example of the role that the community of interested actors—public entities, private persons and interest groups, academics—can play in the information privacy arena.

²⁰ This attitude can be seen in the so-called “Megan’s laws” which mandate the publication of lists of names and addresses of sex offenders to make communities aware of their presence. These were upheld by the Supreme Court, which remarked that “the purpose and the principal effect of notification are to inform the public for its own safety, not to humiliate the offender” [CBS News 2003].

11 Conclusions and recommendations

At the outset, this research project proposed to explore four topics: (1) to identify criteria for evaluation of personal data privacy issues, (2) to describe the regulatory environment for information privacy, (3) to describe the E-cJS system, and (4) to compare the evaluation criteria to the E-cJS data processing system in its regulatory context.

The methodology involved the investigation of theory to identify privacy principles, and collection of interview data and interpretation of laws to describe the regulatory context and the E-cJS data processing system. Comparison of the principles to the E-cJS system in the regulatory context yielded a view of the effectiveness of Albania's data privacy regime in operation. The comparison revealed a number of ways in which the privacy regime falls short of the aspirations embodied by the FIPs, and a number of ways in which it is fulfilling them. That Albania's privacy regime is not as effective as it could be, given the country's situation as a developing economy emerging from the effects of dictatorship, is almost a foregone conclusion that hardly needs an entire research project to reach. The same goes for the conclusion that Albania's legislation needs revision. But the foregoing research topics aimed at examining in specific instances *how* Albania's privacy regime differs or corresponds to international standards, and based on that examination, a number of conclusions and recommendations can be proposed regarding increasing the effectiveness of information privacy in Albania.

11.1 *Outlining a set of data privacy principles aids research, communication and debate.*

The first topic concerned mainly an academic study of theories on personal data protection, and resulted in identification of FIPs. The analysis reveals something about the identified criteria themselves. It shows that they can indeed be applied concretely to evaluate the data protection effectiveness of particular IT projects, in a way that reveals information useful for legal reasoning, technological adaptations and policy debates. The FIPs serve as a useful framework that could potentially also be applied in other ways, to evaluate the effectiveness of a country's overall data privacy regime, or to evaluate the performance of data controllers or data subjects [Bennett 2003: 200-207]. In Albania, the FIPs could serve as a useful reference point for policy debate, legislative drafting, media attention or community awareness and education.

In the evaluation of the E-cJS system with respect to several of the FIPs, it appeared that there is variation among countries as to how they are enacted into law, and variation over time and across cultures as to how the principles should be carried out in practice. Yet without a set of principles to serve as a framework, these legal, temporal and cultural differences are very difficult to identify and talk about.

In addition, it is an old adage that having a goal is necessary for making progress, even if the specified goal is not ultimately reached. Without goals, effort is often expended aimlessly, and progress is difficult to measure or perceive. The FIPs serve as a ready-made set of goals for information privacy, based on international standards and practical experience. Especially for a country such as Albania where

consciousness of information privacy issues is just beginning, it can be helpful to have a starting point for further study and reflection in the national context.

The descriptive portions of the research, concerning the regulatory environment and the E-cJS system, compile the results of both desk work and field research. As far as could be discovered, no such catalog about Albanian laws on data protection has been made before, nor any similar comparison with the provisions of international law, at least in an academic document. Likewise, there has been little if any examination of public sector information processing systems like the E-cJS other than by those designing and using them. It is hoped that these descriptions can provide a more thorough understanding of the legal field, form the basis for discussions about this and similar information processing systems, and contribute to an increased level of openness about information processing in Albania.

11.2 *Mechanisms are needed to introduce personal data protection concepts into legislative and administrative processes.*

There are many new data processing systems being developed in the Albanian public sector, some adopted by administrative decisions in the ordinary course of business, and some introduced by specialized legislation, like the systems for national ID cards or business registration. It is encouraging that the analysis of the E-cJS legislation and the resulting data processing system showed the existence of information privacy measures. Yet these measures were incorporated without a formal process that would ensure that privacy concerns are addressed every time new data processing systems are created.

The E-cJS legislation was modified considerably from the original proposals, to restrict online access to the data only for specified persons in authorized institutions. This change was made at the recommendation of international experts, whose involvement occurred coincidentally due to the fact that the Council of Europe was beginning its data privacy activities at the same time as the legislation was adopted. The E-cJS data processing software includes a number of data security and privacy features as well. These were incorporated in the system design because of the experience and attention of the particular software firm that designed the system. But the privacy measures in both the legislation and the technology design are there more because of fortunate circumstances rather than formal mechanisms.

Formal mechanisms could be developed and implemented to assure data privacy rules and principles are respected whenever a data processing system is created in the public sector. For example, institutions creating or upgrading data processing systems could be required to clear them with the data privacy supervisory authority before proceeding. The supervisory authority could also be a required point of review for draft legislation, similar to the way draft legislation is routinely reviewed for compatibility with other legislation. For technology design, public authorities could be required to use a standard clause in tender documents for new data processing systems that instructs technology firms to address privacy matters in their proposals.

Having formal mechanisms to assure consideration of privacy issues is particularly important where, as in the EU Directive, data processing conducted by authority of law is exempted from the normal personal data protection rules. The analysis of the purpose finality principle showed that this exemption has the potential to open the door to large amounts of personal data processing by public institutions without the

same regard for privacy principles, and this can occur just because of lack of attention in the legislative process. Had the E-cJS legislation not received the data privacy analysis it did, the original proposal might have been passed into law authorizing open public online access to criminal history records of all citizens. In a country with data protection laws corresponding to the EU Directive—which Albania is expected to be in the near future—such a result would undermine the principles of personal data protection.

11.3 *An independent supervisory authority for data privacy is advisable in Albania.*

Albania is obligated by its Stabilization and Association Agreement with the EU Commission to create, staff and finance an independent supervisory authority for data privacy. But beyond simply being a requirement for advancement towards EU membership, a supervisory authority is advisable for substantive reasons.

One reason is the complexity and specialized nature of personal data protection issues. The analysis in this research paper shows that understanding and applying information privacy principles in concrete cases requires knowledge of background theory and careful study of the specific features of a data processing system. Experience and accumulated knowledge in personal data protection must be built up over time and repeated application. The staff of a data protection authority can most effectively build the required skills and knowledge.

Moreover, combination of skills and knowledge needed for data protection, as well as the combination of legal, policy, educational and technical roles involved in personal data protection, are not found in other public institutions. The Ministry of Justice or other ministries are political organizations, not so well suited for the technical, awareness-raising and industry-relations aspects of information privacy. The Albanian ombudsman does not have the necessary scope of jurisdiction or extent of powers to handle administrative decision making and enforcement in all parts of the public sector (or private sector, when that is covered in the future). A new, independent authority can be structured and organized in a way that is tailored to the needs of personal data protection.

Some non-European countries (most notably the USA) have adopted a passive, self-regulatory approach that relies heavily on citizens to actively monitor and pursue their own rights with regard to personal data protection. Such an approach is not advisable in Albania, where the public is not aware of the issues, civil society is not active on behalf of the institutions, and public authorities cannot be relied on to apply data protection principles consistently.

11.4 *Attention to data protection matters must occur very early in the process of developing data processing systems.*

The evaluation of effectiveness highlights the need for awareness and early involvement of privacy issues in both legislation and system design—in other words, privacy protections are more effective if they are “*built in*” at the outset, rather than “*bolted on*” afterward [Bennett 2003: 110]. The privacy protections that do exist in the E-cJS legislation are there in large part because of the influence of experts specialized in data protection, and because this influence was exercised at an early stage in the process of legislative drafting and system design. In this case, the

detailed nature of the legislation largely dictated the technological privacy measures (such as fingerprint authentication and limited access authorizations). In other cases, IT system designers might play a more influential role. But it is clear that the outcome for data protection is already largely determined once enabling legislation and system designs have been made. Thus, in order to be effective, steps towards personal data protection must be taken at the earliest possible stage in the process.

With respect to legislation in particular, this means that the mechanisms designed to introduce data privacy issues into the drafting process must occur when laws are still within the originating ministry, when their privacy impacts can be assessed and taken account of. The stage of parliamentary debate is too late, since these are the type of issues that require careful and detailed analysis, as can be seen from the comparison of FIPs to the E-cJS legislation. This type of analytical process is not suited to the parliamentary setting.

Likewise, technology can assist in protecting personal data and proper data handling, as seen in several instances in the analysis above, but it can best do this if measures are designed into the systems. It is difficult and often expensive to add or subtract features from a system that is already operational. In order to introduce privacy features in personal data processing technology design, IT staffs in public institutions as well as private technology firms must be educated about information privacy concerns.

11.5 *Information privacy cannot be created by legislation alone—a policy community of interested actors is needed.*

From the comparison of FIPs to the E-cJS, a number of instances can be seen where legislation is insufficient to create privacy protection in actual practice. In addition to legislation, privacy must be built and maintained by the type of community of interested actors that is currently lacking in Albania, such as a governmental supervisory authority, business groups and NGOs, technology firms and professionals, active citizens and public officials who are informed about data privacy. Bennett and Raab call this group of interested actors a *policy community* [Bennett 2003: 171-183].

This research analysis shows several ways in which a policy community is necessary to create privacy protections in practice, in addition to legislation. For example, the analysis of the purpose limitation principle revealed that public institutions demand judicial status certificates often and for a wide variety of purposes. The level of demand for these certificates is beyond the scope of E-cJS legislation. Rather, the interested actors must solve the policy problem of whether and in what instances the use of judicial status certificates should be reduced; the resulting policy decisions can be enacted into law. Demand for use of personal data for other purposes by the public sector must be addressed in the same way.

Similarly, a number of the FIPs can be applied in different ways depending on the culture of privacy in a country. For example, Albania may have culturally less resistance to revealing criminal history data than other European countries; its culture may consider certain types of data as sensitive and not others; people's attitudes towards educational or journalistic use of personal data will be culturally determined. Cultural attitudes towards commercial use of personal data will be important when the private sector is covered by data protection rules. All of these

issues must be resolved by policy decisions, which are best reached by debate among a community of interested actors from various spheres of society.

As noted in the theoretical portion of the analysis, the notion of privacy rights is a relative one: it can come into conflict with, and must be balanced against, other rights and principles. Rights and societal interests such as journalistic freedom, educational and research needs, religious and labor organization freedoms, open access to government documents, public safety and national security can all come into conflict with personal data protection interests [EU 1995: Recitals 13, 34-38, 43-44; CoE 1981: Article 9.2; CoE 1950: Article 8.2]. In addition, the goals of increased efficiency, economy and service levels—all drivers of computerization and automated data processing—are the trends that originated concern for information privacy, because they often tend to include features that are perceived to threaten privacy [Bennett 2003: 23-25, 47-49]. These conflicting rights and interests must also be debated and balanced within a national, historical and cultural context to reach policy decisions, whether in legislation, administrative practice or private commerce.

International organizations have been the main actors in the policy community in Albania to date. These organizations can highlight the need for awareness, interest and action on privacy issues, and they can help create the necessary understanding and structures, but they cannot comprise a sustainable national policy community from the outside. A national supervisory authority would be a natural focal point around which to develop a national policy community: citizens would have a place to bring their concerns and complaints; business organizations would have an advisor for their own self-regulatory efforts; NGOs would have a liaison to public and private data processors; and public authorities would have an ally and sounding board.

11.6 *Personal data protection should be approached as a good governance issue.*

Protection of personal data is not likely to rise to the top of the political agenda or the public consciousness anytime soon. The reality is that Albania faces more urgent and economically important problems in the immediate future that will take up political time and attention; and the automation of personal data processing that usually sparks interest in protection of personal data is only now beginning.

Nevertheless, personal data protection will be on the agenda at some level, if for no other reason than that the country's agreement with the EU mandates it. Therefore, as was the case with the E-cJS, the community of interest that arises around this issue initially is likely to be one centered on public administrators and those involved in European integration, rather than civil society organizations or consumer groups, and the attention given to it is likely to be done in the context of fulfilling obligations to the EU.

But improving the effectiveness of personal data protection has side benefits that implicate the more general goals of improving governance in the public or private sector. The steps necessary to achieve data protection are generally also steps towards good computing practice generally, or good records management practice, or transparency of public institutions [Bennett 2003: 192-193]. Developing security measures designed to protect personal data, for example, would naturally cause an institution to improve the security of its computer systems in general. The need to

assure that personal data records are accurate, complete, up to date and destroyed when no longer needed is part of the larger goal of managing all of the institution's records properly. And allowing citizens access and the ability to correct their own records, as well as procedures to complain about improper handling, improves the openness of government institutions towards the citizens.

Thus, even though information privacy may not be a hot political issue in Albania (as indeed in many countries), it can still be addressed within the context of general good governance. And the general improvement of government performance *is* a top political issue, with reforms in civil service structures, anti-corruption measures, and modernization as examples.

11.7 *Technology can promote data protection, but beware of over-reliance.*

As noted in the discussion of almost all the FIPs, technological features have an important impact on the level of information privacy exhibited by data processing systems. Data security is probably the area where it has the greatest visibility, but technological measures can also affect information privacy in the areas of limited collection and retention of data, finality of purpose and recipients, and data accuracy.

However, there may sometimes be a tendency to rely too much on technology to implement personal data protections. Particularly in a country such as Albania, where widespread computerization of public functions is just beginning and experience is short, responsible officials may believe that the computer hardware and software itself encompasses all necessary privacy protections. But organizational and policy measures are equally if not more important than technological ones in protecting privacy, since it is individuals in institutions who are responsible for designing, using, maintaining and modifying data processing systems. Officials may rely on technology to the detriment of organizational measures and policy decisions because technology is more visible and easier to implement.

The E-cJS system is a good example of this. The hardware and software design contains or could easily include features that promote the privacy principles of accountability, purpose identification, limited collection and retention, finality, accuracy, and security. Yet human error cannot be eliminated fully, and organizational measures are needed to address this. Furthermore, sound policy decisions must be made about structures and procedures to ensure accountability, the purposes for which personal data may be used, the institutions which may receive and use the data, how to avoid uninformed consent or enforced consent, how to handle transfers to foreign countries, in what cases exceptions should be allowed, and many other issues. These organizational and policy matters are more difficult to design, harder to implement in practice, and more difficult to display than a high-tech fingerprint reader or a secure network. With the pressure to reassure the public and international observers that information privacy is being protected, there is a risk of placing too much reliance on technological solutions and neglecting organizational and policy requirements.

12 Critical perspectives on the research

12.1 *Critiques of theory and methodology*

This research project relied mainly on theoretical models developed and described by Bennett and Raab, which “take privacy as the goal against which to evaluate data protection” [Bennett 2003:192]. These authors acknowledge that evaluation models are problematic because of “the vagueness and contestability of the definition of privacy” as well as subjective attitudes towards privacy, and difficulty of measuring degrees of progress along a scale [*Id.*]. Other approaches might have been equally valid or useful for the task.

One such alternative approach is that of examining constellations of the values and interests protected by privacy laws [Bygrave 2002:125-169]. Bygrave takes a somewhat broader context for analysis than do Bennett and Raab, attempting to catalog not only the current state of data protection but also future policy directions. Building upon concepts developed largely in Norwegian information privacy theory, Bygrave develops and describes a typology of interests held by data subjects and data controllers. His catalog includes interests and values in two areas: “Group 1” having to do with the quality of personal information and information systems, and “Group 2” having to do “with the condition of persons as data subjects and with the quality of society generally” [Bygrave 2002:144]. The catalog of privacy interests breaks down as follows:

Group 1—quality of data and information systems

- A. Validity interests—related to content of personal data
 - A1. Precision of data
 - A2. Comprehensiveness of data, including its identifiability
 - A3. Correctness of data, including its currency, actuality and up-to-dateness
- B. Utility interests—related to uses to which data are put
 - B1. Relevance of information, including logical and legal/moral relevance
 - B2. Completeness of information
- C. System quality interests—related to information processing systems
 - C1. Manageability (organizational and administrative)
 - C2. Robustness (vulnerability to external interference)
 - C3. Accessibility (ability to locate and retrieve data)
 - C4. Reliability (desired, error-free functioning)
 - C5. Comprehensibility (transparency of functioning and facilitation of error identification)
 - C6. Integrity of data during processing
 - C7. Interpretability of data (in presentation and form)
 - C8. Predictability of means and outcome of processing
 - C9. Registration quality, including completeness and correctness of data recording

Group 2—individual persons as data subjects and in society

- A. Privacy, including non-transparency (anonymity) to, and non-interference by, others

- B. Autonomy (informational self- or co-determination), including insight into data processing, controlling outflows of own data and controlling inflows of others' data
- C. Civility (promoting attitudes of mutual respect among persons)
- D. Pluralism (encouraging diversity and equality)
- E. Democracy (active participation of citizens in government)
- F. Rule of law (subjecting activities to legal control)
- G. Balanced control (achieving proportionality of governmental efforts)

While Bygrave's taxonomy has the advantage of being wide-ranging and of bringing out a number of technological aspects, it was not chosen for this research for a number of reasons, which the author himself acknowledges [Bygrave 2002:157-60]. The values and interests catalogued are difficult to apply in concrete terms; they contain a good deal of overlap and interrelationships that could be collapsed into fewer categories. Moreover, they include a range of philosophical and societal issues that would take the research into a vague and subjective direction. They also include interests that apply not only to personal data protection, but also to other areas of law and society. Furthermore, Bygrave's catalog does encompass all or most of the Fair Information Principles outlined by himself and others. Thus, the FIPs were considered the most practicable and relevant framework for the research task undertaken here. In addition, the privacy regime concept proposed by Bennett and Raab provides a useful framework for evaluating the various actors involved in information privacy not afforded by Bygrave's interest catalog.

The analysis presented here may be criticized as being Euro-centric. This is partly the natural result of the choice of methodology (drawing heavily on the EU adequacy assessment methodology [Raab 1998]), and partly the result of selecting two European policy instruments as points of reference (the EU Directive and CoE Convention). While both the methodology and policy references were chosen for their relevance to the Albanian situation, the result is that the analysis fails to consider alternative policy and legislative choices reached in non-European countries. For example, the US and Japanese models are much more heavily weighted toward private self-regulation and technology solutions [Bennett 1992: 170-179; Bennett 2003: 105-107; Bygrave 2002: 70] than the European one, and without a one-issue supervisory authority. Nevertheless, the research project was not intended as an overall evaluation of the political and policy processes (see delimitations in section 3.2), nor as a transnational comparative study. Furthermore, Euro-centrism is a fact of life in Albania, which has made the policy choice to commit itself to the EU accession process. A similar analysis of a developing country in, for instance, Asia would probably produce markedly different results.

12.2 *Other critiques*

Beyond questions of methodology and theory, one might also raise the criticism that the study of information privacy is an impractical, academic luxury for a country like Albania. So many other pressing problems face the nation at present—problems such as organized crime, poverty, corruption, lack of power and transportation infrastructure, environmental pollution—that fair treatment of personal data privacy seems almost trivial in comparison. This point has appeal especially from the point of view of the limited financial and human resources available to the Albanian state. Why should the state (or researchers, for that matter) devote time, attention and

money to this issue now? And why should Albanians be concerned about how their personal data is being handled?

There are a number of responses to these criticisms. First, the financial and human resources are indeed limited when considering only the public budget. However, considerable money and expertise are being provided by international donors to assist not only in priority areas like crime and infrastructure, but also in areas lower in profile and priority, yet important to economic and social progress. And information privacy, while it may not be top priority, is nevertheless important to Albania's development. Partly, the aspirations towards EU membership force it to be so, since the EU demands harmonization of laws and the policies underlying them. But also, information privacy cuts to the heart of what the process of democratization is about, because it concerns the relationship between government and citizen [Bennett 2003: 14-15]. The history of state surveillance of private individuals in former dictatorships or authoritarian states has brought privacy interests to the forefront in those countries [Bennett 2003: 25, 60]. Albania's history includes chapters of harsh repression based on personal information gathered by informants, maintained in secret and used by the state for political ends. Protecting interests in information privacy can thus be seen as a step towards democratization and a remedy for the authoritarian practices of the past.

Yet despite their rejection of an authoritarian past, information privacy has not become a political issue for citizens, media or civil society in Albania to date. A number of explanations can be offered for this. First, until now the government has been almost completely inactive in the area, so there has been no event or action to focus public attention on the issue. Second, computerization of public and private services, which has heightened privacy concerns in other countries, is in the beginning phases in Albania. Another explanation might be the one offered by a survey of Hungarian attitudes towards data protection in 1991, which showed that less educated, older and lower income segments of the population generally had fewer concerns about their personal data; the researchers concluded that people who must depend on the help and assistance of others, in particular on government agencies, are willing and accustomed to revealing more about themselves and their personal circumstances in order to receive the help they need [Bennett 2003: 59-60]. In Albania, people may be willing to relinquish their privacy interests if it means improving their level of public or private benefits, like health care, electricity service, transportation, or access to communications technologies.

Finally, it may seem unfortunate to base the analysis of Albanian national law on the existing Data Protection Law, while a new draft is in process that is expected to incorporate the EU Directive's provisions. The existing law will soon be replaced and has never been applied or enforced, so it could be questioned whether there any point in examining its provisions as part of the analysis. Yet the analysis did produce some useful results, even considering the new law on the horizon.

Considering the existing legislation within the FIP framework resulted in identifying certain jurisprudential ambiguities and conflicts in the existing data protection legislation. Identifying specific examples where the differences in laws have practical effects can help with the process of improving the legislation. This process is still ongoing, so the analysis may offer certain relevant points.

The threshold evaluation of whether the data protection law covered the E-cJS data processing system at all raises a policy issue that must be addressed in the new legislation as well. What will its scope be in terms of types of data processing? To what extent will it leave room for specialized laws covering particular sectors of data processing?

Additionally, the analysis of the existing law identified jurisprudential issues with respect to the need for balance and flexibility in the wording of the law, reasonableness and proportionality standards, and careful consideration of exceptions and exemptions. These issues arose concerning the principles of knowledge and consent, security, openness and subject access. Such jurisprudential issues were identified in connection with the E-cJS system, but would also affect other data processing systems covered by the law. The drafters of new legislation must also consider these issues, in the context of many different types of data processing systems, in order to avoid unintended and undesired consequences for public sector data processing, such as gaps in protection, unnecessary expenditures on compliance or limited enforceability.

Likewise, the choice to examine the E-cJS system may seem curious in light of the fact that other larger, more visible and more controversial public computerization efforts are ongoing, such as the system for national ID cards or one-stop business registration. Yet this lack of visibility is precisely why it is important to examine data protection principles in the context of data processing systems like the E-cJS. To date, no catalog exists of public data processing systems. Those who are interested in data protection, who are drafting the laws or must apply them, have little knowledge of the concrete situations where FIPs are relevant. More knowledge about all the ways in which data processing is occurring in Albania, and how data protection principles apply to them, will contribute to a culture of careful handling of personal data.

13 References

All internet addresses for documents available online were accessed on 16 December 2007.

13.1 *International treaties and conventions*

Council of Europe (1950), *Convention on the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol No. 11*, Nov. 4, 1950, European Treaty Series No. 5; 213 United Nations Treaty Series 221; available online at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=005&CM=8&DF=4/25/2006&CL=ENG>

Council of Europe (CoE) (1981), *Convention [No. 108] on the Protection of Individuals with Regard to Automatic Processing of Personal Data* (28 January 1981), available online at <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm> [referred to in the text as "CoE Convention"]

Council of Europe (CoE) (1981a), *Explanatory Report to Convention [No. 108] on the Protection of Individuals with Regard to Automatic Processing of Personal Data* (28 January 1981), available online at <http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm> [referred to in the text as "CoE Explanatory Report"]

Council of Europe (CoE) (2001), *Additional Protocol [No. 181] Regarding Supervisory Authorities and Transborder Data Flows* (8 November 2001), available online at <http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm> [referred to in the text as "CoE Additional Protocol"]

Council of Europe (CoE) (2005), *Albania declarations contained in the instrument of ratification deposited on 14 February 2005*, document available online at <http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=108&CM=1&DF=12/16/2007&CL=ENG&VL=1>

Council of the European Union (2006), *Stabilisation and Association Agreement between the European Communities and their Member States, of the one part, and the Republic of Albania, of the other part*, document no. 8164/06 (22 May 2006), available online at <http://www.delalb.ec.europa.eu/en/documents/st08164.en06.pdf> [referred to in the text as "Stabilization and Association Agreement"]

European Union (EU) (1995), *Directive 95/46/EC on the Protection of Individuals with Regard to Processing of Personal Data, and on the Free Movement of Such Data* (24 October 1995), Official Journal L 281 , 23/11/1995 pp. 31–50, available online at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML> [referred to in the text as "EU Directive"]

Organization for Economic Cooperation and Development (OECD) (1980), *Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data, with Explanatory Memorandum*, Council recommendation (23 September 1980), available online at http://www.oecd.org/document/18/0,3343,en_2649_201185_1815186_1_1_1_1,00.html

United Nations (UN) (1990), *Guidelines Concerning Computerized Personal Data Files*, General Assembly Resolution 45/95 (14 December 1990), available online at <http://www.unhchr.ch/html/menu3/b/71.htm>

13.2 Albanian laws

Law No. 7895, *Criminal Code of the Republic of Albania*, dated 27 January 1995, as amended (Consolidated version October 2004); Albanian language version available online at <http://www.qpz.gov.al/doc.jsp?doc=docs/Liqj%20Nr%207895%20Dat%C3%AB%207-01-1995.htm>; unofficial English translation available online at <http://www.legislationline.org/upload/legislations/0f/55/d46a10bcf55b80aae189eb6840b4.htm>

Law No. 7905 *Criminal Procedure Code of the Republic of Albania*, dated 21 March 1995, as amended (Consolidated version October 2004); Albanian language version available online at <http://www.qpz.gov.al/doc.jsp?doc=docs/Liqj%20Nr%207905%20Dat%C3%AB%201-03-1995.htm>; unofficial English translation available online at <http://www.legislationline.org/upload/legislations/ba/fb/3e7ef0be7ad60ee6e16cbd8b63db.htm>

Law No. 8485 *Code of Administrative Procedures*, dated 12 May 1999; Albanian language version available online at

<http://www.qpz.gov.al/doc.jsp?doc=docs/Liqj%20Nr%208485%20Dat%C3%AB%2012-05-1999.htm>; unofficial English translation available online at http://hidaa.gov.al/english/pub/l_8485.htm

Law No. 8503 *On the Right to Information Over Official Documents*, dated 30 June 1999; Albanian language version available online at <http://www.qpz.gov.al/doc.jsp?doc=docs/Liqj%20Nr%208503%20Dat%C3%AB%2030-06-1999.htm>; unofficial English translation available online at http://hidaa.gov.al/english/pub/l_8503.htm

Law No. 8517 *On the Protection of Personal Data*, dated 22 July 1999; Albanian language version available online at <http://www.qpz.gov.al/doc.jsp?doc=docs/Liqj%20Nr%208517%20Dat%C3%AB%2022-07-1999.htm>; unofficial English translation available online at http://hidaa.gov.al/english/pub/l_8517.htm; edited English translation in Attachment 6

Law No. 9131 *On the Rules of Ethics in the Public Administration*, dated 8 September 2003; Albanian language version available online at <http://www.qpz.gov.al/doc.jsp?doc=docs/Liqj%20Nr%209131%20Dat%C3%AB%2008-09-2003.htm>; unofficial English translation available online at http://hidaa.gov.al/english/pub/l_9131.htm

Law No. 9614 *On Electronic Certificates of Judicial Status*, dated 21 September 2006, Albanian language version available online at <http://www.qpz.gov.al/doc.jsp?doc=docs/Liqj%20Nr%209614%20Dat%C3%AB%2021-09-2006.htm>; English translation in **

Council of Ministers (2006), Decision No. 825, dated 06 December 2006; Albanian language version obtained from Interview 5.

Republic of Albania (2007), "*Constitution of the Republic of Albania*", ratified 22 November 1998, amended 13 January 2007; Albanian language version available online at http://www.osce.org/documents/pia/1998/11/4321_sq.pdf; unofficial English translation available online at http://www.osce.org/documents/pia/1998/11/4321_en.pdf

13.3 Books, articles and other publications

Agenda Institute (2007), "*Policy Brief: Albania's Experience in Harmonization with European Standards on Data Protection*", October 2007, online article available at **

Andersen, Ib (2006), "*Den skinbarlige virkelighed*", 3rd ed. (Copenhagen, Denmark: Forlaget Samfundslitteratur)

Bennett, Colin J. and Raab, Charles D. (2003), "*The Governance of Privacy: Policy Instruments in a Global Perspective*" (Aldershot, Hampshire, England: Ashgate Publishing Limited)

Bennett, Colin J. (1992), "*Regulating Privacy: Data Protection and Public Policy in Europe and the United States*" (Ithaca, New York: Cornell University Press)

Blume, Peter (2001), "*Denmark*", in "*Nordic Data Protection Law*", P. Blume ed. (Copenhagen, Denmark: DJØF Publishing)

Blume, Peter (1996), "*Personregistrering*" (Copenhagen, Denmark: Akademisk Forlag)

Bygrave, Lee A. (2002), *"Data Protection Law: Approaching its Rationale, Logic and Limits"* (The Hague, Netherlands: Kluwer Law International)

Chaffey, Dave (2004), *"E-business and E-commerce Management"*, 2nd ed. (Harlow, Essex, England: Pearson Education Limited)

Carey, P.W. (2004), *"Data Protection—a Practical Guide to UK and EU Law"* (Oxford, England: Oxford University Press)

Commission of the European Communities (2006), *"Albania 2006 Progress Report"*, staff working document SEC (2006) 1383, 8 November 2006, available online at http://www.delalb.ec.europa.eu/en/news/al_sec_1383_en.pdf

Council of Europe (no date), *Joint Programmes—Logframes and Activities*, website located at <http://www.jp.coe.int/CEAD/JP/Default.asp?TransID=112>

Dehnel & Associates, Inc. (2007), *"CRC"*, website located at www.criminalrecordcheck.com

EPIC (Electronic Privacy Information Center) (2001), *"Public Comment on Privacy and Public Access to Electronic Case Files"*, 26 January 2001, document available online at http://www.epic.org/open_gov/ecfcomments.html

Government of Ontario, Access and Privacy Office (2007), *"Privacy Impact Assessment Guidelines"* (Ontario, Canada: Queen's Printer for Ontario), document available online at <http://www.accessandprivacy.gov.on.ca/english/pia/pia.pdf> [referred to in the text as "Ontario impact assessment methodology"]

Kuner, Christopher (2007), *"European Data Protection Law: Corporate Compliance and Regulation"*, 2nd ed. (Oxford, England: Oxford University Press)

National Registration Center Albania (2007), webpage located at http://www.gkr.gov.al/nrc/About_us.aspx

Organization for Economic Cooperation and Development (OECD) (2004), Working Group on Information Security and Privacy, *"Biometric Based Technologies"*, 30 June 2004, No. DSTI/ICCP/REG(2003)2/FINAL, document available online at [http://www.oilis.oecd.org/oilis/2003doc.nsf/LinkTo/NT000070D6/\\$FILE/JT00166988.PDF](http://www.oilis.oecd.org/oilis/2003doc.nsf/LinkTo/NT000070D6/$FILE/JT00166988.PDF)

Office of the People's Advocate (2006), *"Annual Report on the Activity of the People's Advocate: January 1—December 31, 2006"*, document available online at <http://www.avokatipopullit.gov.al/English/Reports/Report%202006.pdf>

OSCE (Organization for Security and Cooperation in Europe) (2007), *"Press release: Albania modernizes address and civil registration systems with support from the OSCE Presence"*, 15 November 2007, online article located at http://www.osce.org/albania/item_1_27956.html

Raab, Charles D., et al. (1998), *"Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals With Regard to Processing Personal Data: Test of The Method on Several Categories of Transfer—Final Report"*, September 1998, document available online at http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/adequat_en.pdf [referred to in the text as the "EU adequacy assessment methodology"]

Saarenpää, Ahti (2001) "*Finland*", in "*Nordic Data Protection Law*", P. Blume ed. (Copenhagen, Denmark: DJØF Publishing)

Schartum, Dag W. (2001), "*Norway*", in "*Nordic Data Protection Law*", P. Blume ed. (Copenhagen, Denmark: DJØF Publishing)

SearchMyRecords.com (2007), website located at www.searchmyrecords.com

Seipel, Peter (2001), "*Sweden*", in "*Nordic Data Protection Law*", P. Blume ed. (Copenhagen, Denmark: DJØF Publishing)

State of Colorado (2002), "*Colorado Bureau of Investigation Records Check*", website located at <https://www.cbirecordscheck.com/Index.asp>

Tirana Times (2007), "*Albtelecom Sale to Calik is Finalized*," 19 June 2007, online article located at <http://www.tiranatimes.com/index.php?id=75>

United Nations Development Programme (UNDP) (2007), "*Implementation of Government Network (GovNet) Phase II*", document available online at <http://intra.undp.org.al/ext/elib/download/?id=924&name=GovNet%5FAgreement%5FProDoc%5Fweb%2Epdf>

USAID (United States Agency for International Development (2004), "*Mini-Revolution in Health Care: New information systems for primary health care*," 26 October 2004, online article located at http://albania.usaid.gov/shfaqart/143/49/Success_Story.htm

United States Department of Justice (2007), "*International Criminal Training and Assistance Program (ICITAP), Albania Program Overview*", webpage located at <http://www.usdoj.gov/criminal/icitap/albania.html>

United States Department of State, Bureau of Consular Affairs (no date), "*Criminal Records Checks*", webpage located at http://travel.state.gov/travel/tips/emergencies/emergencies_1201.html

United States Office of Management and Budget (2007), "*What do we mean by 'Effective'?*", webpage at <http://www.whitehouse.gov/results/agenda/effective.html>

Virginia Department of State Police (2007), "*Criminal Record Check*", webpage located at http://www.vsp.state.va.us/CJIS_Criminal_Record_Check.shtm

World Bank (2005), "*ICT at a Glance: Albania*", document available online at http://devdata.worldbank.org/ict/alb_ict.pdf

World Bank (2006), "*Implementation completion and results report (IDA-33270) on a credit in the amount of \$ 9 million USD for a legal and judicial reform project*", World Bank Report Number 35351-AL, 12 June 2006, available online at http://www-wds.worldbank.org/external/default/main?pagePK=64193027&piPK=64187937&theSitePK=523679&menuPK=64187510&searchMenuPK=64187283&theSitePK=523679&entityID=000090341_20060725100911&searchMenuPK=64187283&theSitePK=523679

Woulds, John (2004), "*A Practical Guide to the Data Protection Act*" (London, England: The Constitution Unit, School of Public Policy, University College London)

13.4 Unpublished papers

Patijn, Alexander (2006), "*Opinion on the Proposal to Offer Online Access for Judicial Status*", prepared for the Data Protection Unit, Council of Europe

Prelec, Dubravka (September 2006), "*The Role of Line Managers in the New Model of Human Resource Development in the Croatian Civil Service*", Masters dissertation in National School of Government, Kingston (UK) University School of Business

Schaar, G., et al. (2006), "*Preliminary Study of ICT in Developing Countries*", IT University of Copenhagen M.Sc. student project paper, available online at https://mit.itu.dk/ucs/pb/download/Report%20ICT4D.pdf?file_id=304912 (requires login)

Schaar, G. (2006a), "*Information Technology for Court Case Management*", IT University of Copenhagen M.Sc. student paper available online at https://mit.itu.dk/ucs/pb/download/Project%20report%20Summer2006.pdf?file_id=342395 (requires login)

Schaar, G. (2006b) "*Organizational Theories and IT Realities: Database System Development at an International Consulting Firm*", IT University of Copenhagen M.Sc. student project paper, December 2006

Schaar, G. (2005), "*IT-enabled reforms in the legal and judicial sector in Albania: a case study*", IT University of Copenhagen M.Sc. student paper, May 2005 (not publicly available due to confidentiality)

Sutton, Graham (2006), "*Opinion on the Proposal to Offer Online Access for Judicial Status*", prepared for the Data Protection Unit, Council of Europe

14 Attachments

Attachment 1. Data needs and analysis matrix.....Page 73

Attachment 2. Table of Interviewees.....Page 74

Attachment 3. List of preliminary interviewees.....Page 75

Attachment 4 Semi-structured interview questions.....Page 76

Attachment 5. Comparison of sources of Fair Information Principles (FIPs).....Page 78

Attachment 6. Albanian Law No. 8517 On the Protection of Personal Data.....Page 80

Attachment 7. Law No. 9614 On Electronic Certificates of Judicial Status.....Page 84

Attachment 8. Provisions of Criminal Code / Criminal Procedure Code referenced in E-cJS Law.....Page 88

Attachment 1. Data needs and analysis matrix

Question	What theory supports?	Data requirements	Data sources	Practical collection issues	Ethical concerns	Method of analysis	Analysis concerns
<i>What is the nature and structure of the E-certificate system?</i>	Business process modeling; data flow analysis; system architecture modeling	Description of business purposes, data flows and IT design and architecture	E-certificates law; Semi-structured interviews	Confidential, sensitive nature of system; Access to responsible officials; Limited time to collect	Compromising security of system; Causing breach of official duties	Compile interview notes, Desk study of law	Faulty recollection of interviews; subjective interpretation of data; translation errors
<i>What is the nature of the relevant regulatory environment for data protection?</i>	Privacy and data protection legal, social, political theory Bennett 2003 Bygrave 2002	Contents of relevant regulatory and policy instruments; Information about practices and actors in Albania	Academic literature on privacy and data protection; Semi-structured interviews	Access to knowledgeable individuals; Diffuse nature of information; Limited time to collect	None	Compile interview notes, Desk study of law	Selection of proper references; Scope limitation Faulty recollection of interviews; subjective interpretation of data; translation errors
<i>How does the E-certificate system compare to principles and standards within the regulatory environment?</i>	Ontario privacy impact assessment; EU Commission Working Group Assessment Methodology	Results of data collection and analysis for above questions	See above	Willingness of subjects to speak honestly and critically; scope of analysis	None	Compile interview notes, Desk study of law	Limited nature of test case; comparison across legal/ regulatory/ socio-political frameworks

Source for table framework: [Prelec 2006]

Attachment 2. Table of Interviewees

Interview Reference	Organization	Position	Area of knowledge
Interview 1	EURALIUS (European Assistance Mission to Albanian Justice System)	Expert on Case Management and Court Administration	General status of IT developments in courts and ministry of justice; history of E-cJS project; European standards and practices
Interview 2	Council of Europe Information Office in Albania	Project Officer	Council of Europe assistance to data protection in Albania; interested actors and stakeholders; Albanian conference on data protection; European standards
Interview 3	Cactus Albania	Project Manager	Development, architecture and operation of E-cJS system
Interview 4	Ministry of Justice, Legislative Drafting Department	Head of Data Protection Working Group	Legislative process; data protection in Albania
Interview 5	Ministry of Justice, Judicial Status Office	Head of Office	Operating context and practices of JSO; development of E-cJS
Interview 6	Ministry of Justice	Head of IT	Development and operation of E-cJS system
Interview 7	Ministry of Justice	Specialist (former Head of Judicial Status Office)	History and development of E-cJS system; operating context and practices of JSO
Interview 8	Ministry of Justice	Vice-minister	Legislative and political process; history and development of E-cJS system
Interview 9	Ministry of Justice	Minister of Justice	Legislative and political process and context
Interview 10	Council of Ministers	Information Society Counsellor to Prime Minister	General status of IT development in Albanian public sector; role of public institutions in data protection
Interview 11	Albanian Center for Human Rights	Director	Legislative process; role of NGOs; data protection in Albanian society

Attachment 3. List of preliminary interviewees

Interview Reference	Organization	Position	Area of knowledge
Interview P1	EURALIUS (European Assistance Mission to Albanian Justice System)	Expert on Legislative Drafting and Approximation of Laws	General status of IT developments in courts and ministry of justice; current issues in Albanian legal sector
Interview P2	EURALIUS (European Assistance Mission to Albanian Justice System)	Expert on Case Management and Court Administration	General status of IT developments in courts and ministry of justice; history of E-cJS project; European standards and practices
Interview P3	Council of Europe Information Office in Albania	Project Officer	Council of Europe assistance to data protection in Albania; interested actors and stakeholders; Albanian conference on data protection; European standards
Interview P4	UNDP Albania (United Nations Development Programme)	Manager, Democratic Governance Programme Cluster	UNDP E-government projects in Albania
Interview P5	US DoJ OPDAT (Dept. of Justice Office of Overseas Prosecutorial Development, Assistance and Training)	Legal Advisor	Case management software in Albanian prosecutors office; integration of legal sector institutions
Interview P6	Council of Ministers	Information Society Counsellor to Prime Minister	General status of IT development in Albanian public sector; role of public institutions in data protection

Attachment 4 Semi-structured interview questions

- 1) Nature of the e-certificates system
 - a) What is the purpose of the creating the new online system? What country or countries' laws/practices were the model for the technical and legal aspects?
 - b) What types of personal data are collected and by what means are they processed? How and where are the data stored? What are the data sources?
 - c) What hardware and software are used in the system and how is it configured?
 - d) Who is involved with using and maintaining the system and data processing at each stage? Is any data processing done by non-governmental employees or third parties?
 - e) What action is taken if an electronic certificate is refused (because the person has some criminal records)?
 - f) What will happen if a certificate is refused in error?
 - g) How are records collected by the courts/prosecutors and transferred to the Ministry? electronic or paper?
 - h) Does the written judicial status record include information about rehabilitated judgments?
 - i) Will all "public or private institutions, Albanian or foreign" be able to get a written certificate if the electronic one is refused (Art. 6.2)? How will they request it? Were these institutions able to get a written certificate before? Does the new law expand the categories of those who can get written certificates beyond Criminal Procedure Code Art. 484?
 - j) How will institutions fulfill the legal requirements and request electronic certificates by mail or email?
 - k) Has the self-declaration form been prepared? What will it contain? What information will it give to citizens about the consequences of using it? About their data protection rights?
 - l) How will the Head of the Office of Judicial Register make the authorizations for other ministry officials to use the system? Will these authorizations be publicly available?
- 2) Nature of the regulatory environment
 - a) Has the Council of Ministers issued the decision listing the entities that will have online access to electronic certificates? Will this be done by categories or by naming specific institutions? How will this list be publicized?
 - b) Has the Minister issued the detailed rules for obtaining electronic certificates? How will these be publicized?
 - c) Is the Office of Judicial Register (mentioned in Law 9614) established and staffed? Does it have written working regulations? Is this the same office the existing one that handles judicial registers and certificates, or a reorganization?
 - d) What laws and regulatory instruments are applicable to the judicial status register system?
 - (1) 8517 on Data Protection
 - ii) Law 9614 on Electronic Certificates of Judicial Status
 - iii) Criminal Procedure Code
 - iv) CoE Convention 108
 - v) others?
 - e) Are there any applicable codes of conduct or informal rules?
 - f) Which organizations have a role in monitoring the data protection practices of this system? What is that role?
 - i) State Audit?
 - ii) People's Advocate?

- iii) Council of Europe?
 - iv) Council of Ministers?
- 3) Measures in relation to data protection standards and principles
- a) Purpose limitation, transparency, subject knowledge
 - i) Could the personal data collected for the e-certificate system be used for other purposes? Why not, or what other purposes?
 - ii) To whom may the data be disclosed? What are the rules for this?
 - iii) Are data subjects informed before collection or during the processing of their data? How and what are they told?
 - iv) Data quality and proportionality
 - v) How will the electronic register be updated every 24 hours as stated in the law?
 - vi) Does the system have measures to keep data accurate, complete and updated? What are they? How are changes transferred to data recipients or third parties?
 - vii) How long are the data stored? What measures exist for deletion of old data, especially those listed in Criminal Procedure Code Art. 483, and rehabilitated sentences?
 - b) Data security
 - i) What measures (to the extent they are not confidential) are taken against risks of data loss, or unauthorised access or use, modification, disclosure or destruction?
 - ii) Who is responsible for designing, installing and maintaining security measures?
 - iii) What would be done in the event of a security breach or threatened breach? Who are the "competent organs" to be notified under Law 9614 Art. 10.2?
 - c) Access and rectification
 - i) Do citizens have access to and a way to verify the accuracy of the online registry? Is there any way besides in-person request for a certificate in Tirana? Is there any cost to the person?
 - ii) What can a citizen do if they find an error in their own judicial status records?
 - d) Onward processing
 - i) Are there any restrictions on foreigners who access the online system?
 - ii) Is there any restriction on which countries electronic certificates can be sent to?
 - iii) Do (or will) the Ministry regulations or the Council of Ministers list make any considerations about which countries provide adequate protection for personal data?
 - e) Remedies
 - i) What is the procedure, if any, for receiving and handling complaints about processing criminal records data or electronic certificates?
 - ii) What will be the applicable criminal sanctions for unauthorized intervention in the online registry?
 - iii) Is there any education for judges about the data protection laws?
 - iv) How will citizens know about the remedies available to them?
 - f) Accountability
 - i) What training is given to the employees of the Office of Judicial Status?
 - ii) Are there written guidelines or manuals of procedure for the OJS?
 - iii) What role will the Council of Ministers play in monitoring or updating the regulations concerning the online system?

Attachment 5. Comparison of sources of Fair Information Principles (FIPs)

Bennett & Raab 2003	Bygrave 2002	CoE Convention 108	Kuner 2007 (EU Directive)	OECD Guidelines	UN Data Prot'n Guidelines	Carey 2004 (Younger Commission)
Accountability		8(d): right to remedy for refusal to comply with request for information, correction, erasure or destruction	Control by data protection authorities (Art. 28)	Accountability Principle	Supervision and Sanctions	(g) monitoring system for breaches of security
Purpose identification	Purpose specification	5(b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes	Purpose limitation (Art. 6b—only for specific, explicit, legitimate purposes)	Purpose Specification Principle	Principle of Purpose Specification	(a) specific, limited purpose; (c) minimal, purpose-limited collection
Knowledge and consent of individual	Data subject participation and control		Legitimacy (Art. 7—processing only w/consent or where necessary for stated reasons)	Collection Limitation Principle; Use Limitation Principle	Principle of Purpose Specification	
limited collection	Minimality	5(c) adequate, relevant and not excessive in relation to the purposes for which they are stored	Security (Art. 17)	Collection Limitation Principle	Principle of Purpose Specification	(c) minimal, purpose-limited collection
Finality of use/disclosure	Purpose specification; disclosure limitation	5(b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes	Purpose limitation (Art. 6b—only for specific, explicit, legitimate purposes)	Purpose Specification Principle; Use Limitation Principle	Principle of Purpose Specification	(a) specific, limited purpose; (b) authorized access/use only
Limited retention	Minimality; purpose specification	5(e) identification of the data subjects for no longer than is required for the purpose	Proportionality (Art. 6e—retained no longer than needed)		Principle of Purpose Specification	(h) limited retention periods
Accuracy, completeness and currency of data	Information quality	5(d) accurate and, where necessary, kept up to date; 5(c) adequate, relevant and not excessive in relation to the purposes for which they are stored	Proportionality (Art. 6c—adequate, relevant and not excessive for purpose, 6d—accurate and updated, complete and erased when not needed)	Data Quality Principle	Principle of Accuracy	(i) data accuracy, mechanisms for correction

Bennett & Raab 2003	Bygrave 2002	CoE Convention 108	Kuner 2007 (EU Directive)	OECD Guidelines	UN Data Prot'n Guidelines	Carey 2004 (Younger Commission)
Security safeguards	Information security	7: appropriate security measures against accidental or unauthorised destruction, loss, and unauthorised access, alteration or dissemination	Security (Art. 17)	Security Safeguards Principle	Principle of Security	(f) security and safeguards against abuse/misuse; (g) monitoring system for breaches of security
Openness	Data subject participation and control; fairness	8(a) right to establish the existence of database and its main purposes, and controller's identity and address	Transparency (Arts. 10/11—info to data subject on controller's identity and purpose of processing; Art 18/19//21—notification to supervisory authorities, register, publicizing of processing operations)	Openness Principle		(e) right to be informed about own data
Access by data subjects	Data subject participation and control	8(a) right to establish the existence of database and its main purposes, and controller's identity and address; 8(b) access to own data; 8(c) rectification or erasure of data	Transparency (Arts. 10/11—info to data subject on controller's identity and purpose of processing, 12—right of access/correction)	Openness Principle; Individual Participation Principle	Principle of Interested-person Access	(e) right to be informed about own data
	Fair and lawful processing	5(a): obtained and processed fairly and lawfully	Legitimacy (Art. 6a—fair and lawful)	Collection Limitation Principle; Use Limitation Principle (lawful processing)	Principle of lawfulness and fairness; Power to make exceptions; Principle of Non-discrimination	
	Sensitivity	6: special categories of data processed only with appropriate safeguards	Legitimacy (Art. 8—special categories of data)		Principle of Non-discrimination	(j) care in coding value judgments
						(d) technological means for anonymization

Attachment 6. Albanian Law No. 8517 On the Protection of Personal Data

Law 8517

Unofficial translation edited by Gina Schaar, August 2007
from the original found at:
http://www.hidaa.gov.al/english/pub/l_8517.htm

LAW
No.8517, dated 22.07.1999
ON THE PROTECTION OF PERSONAL DATA

Based on articles 35, 78 and 83(1) of the Constitution, upon the proposal of the Council of Ministers,

THE ASSEMBLY OF THE REPUBLIC OF ALBANIA
DECIDED:

CHAPTER I
GENERAL PROVISIONS

Article 1
Aim of the law

The aim of this law is to guarantee the protection and lawful use of personal data and their processing by public authorities.

Article 2
Definitions

The following terms shall be understood as follows:

- a) "Personal data" shall mean any data about an individual identified or identifiable directly or indirectly from this data;
- b) "sensitive personal data" shall mean data such as:
 - racial and ethnic origin, political opinion or affiliation, religious convictions and the like;
 - health condition, sexual life and criminal status.
- c) "Data processing" shall mean any act carried out with or without support of electronic equipment for the collection, registration, organisation, retention, elaboration, modification, selection, extraction, confrontation, use, suspension, communication, distribution, deletion, destruction, as well as any other act with regard to the data;
- ç) "Personal data subject" shall mean every individual to whom personal data relates;
- d) "Person in charge of personal data processing" shall mean every other person charged by law or regulation with processing the personal data of others;
- dh) "Personal data user" shall mean any individual person, other than the personal data subject, authorised to process such data by the person in charge of personal data processing.
- e) "Anonymous data" shall mean any data by which no person can be identified directly or indirectly;
- ë) "The public" shall mean at least one individual, domestic or foreigner.
- f) "Public authority" shall mean those state institutions specified by the same term in Law Nr. 8503, dated 30 June 1999 "On the Right to Information About Official Documents".

Article 3
General Rule

The public may be informed about personal data of an individual only according to the manner and extent provided by this law.

Article 4
Exemptions

The dispositive provisions of this law shall not apply in the following cases:

- a) Processing of personal data by the subject of that personal data;
- b) Processing of anonymous data;
- c) Personal data obtained in the course of investigations and proceedings in the courts;
- ç) Data classified state secret;

- d) Processing of data for the purposes of national security, crime prevention and protection of public health
- dh) Processing of data for the purpose of population registration.

CHAPTER II PERSONAL DATA PROCESSING

SECTION I Conditions for the processing of personal data

Article 5

Manner of processing personal data

Personal data processing shall be conducted:

- a) in the manner provided by this law;
- b) with a specified, clear and legitimate purpose;
- c) in an accurate way and on the basis of updated data;
- ç) without exceeding the purpose for which they are processed and for a period no longer than necessary to achieve the purpose of processing;
- d) under conditions designed to protect them from damage;
- dh) making use of only such data as are relevant and necessary to achieve the purpose of processing;

Article 6

Notification of the data subject

The data subject shall be given preliminary notification prior to collection of personal data by the person in charge of the data processing about:

- a) the name and address of the person in charge of data processing, as well as that of other persons who will process the data;
- b) the purpose or purposes of the data processing;
- c) the category or categories of personal data to be processed;
- ç) the persons or categories of persons who will use the data;
- d) the possibility of transfer of these data to third countries;
- dh) the fulfillment of conditions for the security of data processing.

Article 7

The Person in Charge of Data Processing

In order to ensure all legal guarantees for the processing of personal data, the person in charge of data processing and any other person involved with the data processing shall be a person with experience in data processing, with a high level of moral integrity and with technical aptitude, in order to guarantee the security of the data.

Article 8

Other Persons Processing Personal Data

Every other person who processes personal data shall be authorised in writing by the person in charge of the data, except in cases when processing of the data is required by law.

Other persons who deal with data processing, shall comply with all rules determined by the person in charge of the data.

The person authorised to process personal data may not transfer these data to a third person.

Article 9

Security of data processing

The person in charge of the personal data must implement all technical and organisational measures to protect these data against any damage or loss, whether accidental or unlawful, against any unauthorised alteration, disclosure or access, in particular where the processing involves networked information technology, and against all other unlawful forms of processing.

In the case of sensitive data, such measures shall ensure a level of security proportional to the risk posed by the processing and the specific nature of these data.

SECTION II Rights of the data subject

Article 10 *Prior Consent Requirement*

Personal data processing by other persons shall only be permitted if the subject of these data has expressly given consent for this processing.
Prior consent may be given for the entire processing procedure or for only one or more parts of this procedure.
Prior consent shall be valid only if it was given freely or in cases where the data subject has been notified in accordance with article 6 of this law.
For the processing of sensitive personal data, prior consent shall be valid only if given in writing.

Article 11 *Cases When Prior Consent is not Required*

The prior consent of the data subject is not required when one of the following conditions is fulfilled:

- a) when the processing is necessary for the fulfilment of a contract in which the data subject is a party, or for fulfillment of conditions precedent to the data subject's entry into a contractual relationship;
- b) when the processing of data is necessary for the fulfilment of the data subject's own legal obligation;
- c) when the data in question are extracted from public registries, or from lists, acts or documents publicly known to everyone;
- ç) when the processing is necessary in order to safeguard the life and physical integrity of the personal data subject or of another physical person, provided that the personal data subject is unable to provide his/her consent due to physical disability, lack of legal capacity or responsibility

Article 12 *Right to be Informed About Personal Data*

Every person has the right to be informed at any time about the procedure of processing of his/her personal data. The person in charge of the data processing, as well as any other persons involved in the processing of the personal data, must, within 10 days from the date when the request for information is submitted, provide the requested information to the data subject.

Article 13 *The Data Subject's Right to Object to Processing*

In all cases except those provided in articles 4 and 10 of this law, the data subject may object to the processing of any of his/her personal data.
Any person is entitled to request the correction or deletion of data that are false, incomplete or that are collected in violation of the law.
The person in charge of data processing shall respond in writing to the request of the data subject within 15 days from the day when the request was made that the processing is in violation.
In case the person in charge of the processing of personal data declines to accept the request of the data subject for their correction, then the data presented by the subject of these data shall be attached to the data possessed by the person in charge and shall accompany them in every case when they are processed.

Article 14 *Transfer of Personal Data Abroad*

Personal data may only be forwarded from the Republic of Albania to a foreign user, outside the Republic of Albania, in the following case:

- a) when the data subject has given a written consent;
- b) when it is permitted by law;
- c) when the jurisdiction where the foreign person in charge of processing the personal data is located provides the same guarantees for their processing as are provided by this law..

CHAPTER III APPEAL

Article 15

Complaint to the People's Advocate

Presentation of a complaint to the People's Advocate and his competencies in the field of personal data are regulated by Law No.8454, dated 04.02.1999, "On the People's Advocate. "
The People's Advocate shall create a registry of personal data processing.

Article 16

General rule

Violation of the provisions of this law, to the extent it does not constitute a criminal offence, constitutes a violation of administrative rules, and is regulated according to Law No.7697 , dated 07.04.1993, "On Violation of Administrative Rules", with the necessary changes and additions.

Article 17

Administrative Appeal

Anyone who believes that his/her rights, as recognised by this law, have been infringed, is entitled to lodge an administrative appeal.

The procedure for the administrative appeal is provided for by law.

Article 18

Judicial Appeal

Anyone who believes that his/her rights, as recognised by this law, have been infringed, is entitled to lodge a judicial appeal.

The procedure for judicial appeals is provided for by the provisions of the Code of Civil Procedure on judicial review of administrative disagreements.

Article 19

Compensation for Damages

Any person is entitled to seek compensation for damages from subjects who violate the rights recognised by this law, when violation in question causes damage.

The procedure for claiming and awarding the compensation for damages is provided by law.

CHAPTER IV TRANSITORY AND FINAL PROVISIONS

Article 20

Taking of Technical-administrative Measures for the Implementation of This Law

All subjects whose activity is totally or partially related to the processing of personal data, within six months from the date this law enters into force, shall take all technical-administrative measures to adjust and regulate their activity in accordance with this law.

Article 21

Entry into Force

This law shall come into effect four months after its publication in the Official Gazette.

Proclaimed by Decree No.2432, dated 28.07.1999 of the President of the Republic, Rexhep Meidani.

Attachment 7. Law No. 9614 On Electronic Certificates of Judicial Status

Law 9614

Unofficial translation edited by Gina Schaar, August 2007

from the unofficial translation by Kathleen Imholz and Mimoza Pano, September 2006

**REPUBLIC OF ALBANIA
THE ASSEMBLY**

LAW

No. 9614 of 21 September 2006

**ON
ELECTRONIC CERTIFICATES OF JUDICIAL STATUS**

In reliance on articles 78 and 83 point 1 of the Constitution, on the proposal of the Council of Ministers,

**THE ASSEMBLY
OF THE REPUBLIC OF ALBANIA**

D E C I D E D:

**Article 1
The object**

This law has the object of determining the rules for the administration of the register of judicial status by electronic means.

**Article 2
Definitions**

In implementation of this law, the terms below have the following meanings:

1. "Register of judicial status" is the written register of judicial status, the basic electronic register of judicial status and the electronic register of judicial status.
2. "Written register of judicial status" is the entry of data in a register in writing according to the provisions of articles 481 et seq. of chapter III of the Code of Criminal Procedure, which will be called herein the "written register."
3. "Basic electronic register of judicial status" is the electronic database of criminal convictions and rehabilitation, drawn up on the basis of final criminal decisions of the Albanian courts, for Albanian citizens, foreign citizens or stateless persons, in which data are processed through written and automatic means, guaranteeing the preservation, processing and non-intervention in the system without the respective authorisation. The above register is not *on line* and herein will be called the "basic electronic register."
4. "Electronic register of judicial status" is the electronic database only of the fact whether a person has been convicted or not. These data are drawn from the basic electronic register only with the intervention of the person authorised by the head of the Office. This register will be called herein the "electronic register."
5. "Automatic data processing" includes the operations of entering data in the basic register only by the employee authorised, while guaranteeing the preservation of the data, the performance of

logical and/or arithmetical actions with these data, their receipt by the respective institutions, the court and the prosecutor's office, and the transfer of these data to the electronic register.

6. "Electronic certificate of judicial status" is the verification obtained electronically from the electronic register of judicial status, which verifies that the person has not been criminally convicted by the Albanian courts, and which herein will be called "electronic certificate."

7. "Written certificate of judicial status" is the document issued from the "basic electronic register", in written form, by the head of the Office of Judicial Status and which herein will be called "written certificate."

8. "Self-declaration of a person" is the declaration that a person makes to a public or private institution, Albanian or foreign, about the fact of whether he has been convicted or not, accompanied by written authorisation and with an identification document in order to permit the institution to make the necessary verifications.

9. "Self-declaration form" is the form drawn up by the Ministry of Justice and approved by the Council of Ministers, which contains the self-declaration as well as the necessary data for the identification of the self-declaring person and which is disseminated to the institutions authorised by the Council of Ministers.

Article 3 Office of Judicial Status

1. The Office of Judicial Status shall function within the Ministry of Justice. Its organisation and structure shall be approved by the Minister of Justice.

2. The Office of Judicial Status shall keep and process the data in the basic electronic register of judicial status, in the electronic register of judicial status, and also in the written register of judicial status.

Article 4 Data processing and protection

1. The automatic processing of data in the basic electronic register and in the electronic register shall be done only by persons authorised by the head of the Office of Judicial Status.

2. The entry of data, their preservation, the performance of logical actions on these data, their protection from changes, their receipt and their dissemination shall be done through the levels of security determined by a person licensed in this field, and through entry codes that are administered only by the head of the Office.

3. The notations and their removal in/from the registers of judicial status shall be done according to the provisions of the Criminal Code and the Code of Criminal Procedure.

4. The head of the Office is prohibited from giving data to third persons about the level of security.

Article 5 Administration of the electronic register

1. The electronic register of judicial status shall be administered by the Office of Judicial Status.

2. The electronic register shall give data only about the fact that a person has not been convicted. The register shall not contain detailed data about criminal convictions.

3. The head [of the Office] takes measures for the electronic register to be updated every 24 hours.

Article 6 **Electronic certificates**

1. Electronic certificates verify that a citizen has not been convicted by a final judicial decision.

2. A citizen convicted by a final decision or an institution seeking information about him according to article 8 of this law shall not given an electronic certificate. He/it shall be entitled to obtain a written certificate.

Article 7 **Self-declaration of judicial status**

1. Citizens of the Republic of Albania, as well as foreign citizens or stateless persons, are permitted to affirm their judicial status through the self-declaration before public or private institutions, whether Albanian or foreign, when data about their judicial status are sought.

2. The self-declaration should also be accompanied by an authorisation signed by the citizen, which authorises these institutions to verify the judicial status in the electronic register.

3. The self-declaration and the authorisation constitute official documents and the submission of false data in them is punished according to the provisions of the Criminal Code.

Article 8 **Distribution of electronic certificates**

1. The distribution of electronic certificates of the electronic register shall be performed while guaranteeing the security of the system, of the data and of the confidentiality of the personal data of citizens, through several levels of security according to article 4 of this law.

2. By decision of the Council of Ministers, public or private institutions, whether local or foreign, shall be given an entry code and the right to receive data directly only from the electronic register and not from the basic register, which is not *on-line*, while guaranteeing technically the impossibility of manipulating the electronic register through an electronic *fingerprint* system.

3. Public or private institutions, whether local or foreign, that have the right to have access to the electronic *fingerprint* system may get electronic certificates directly.

4. Other institutions, which do not have the right of access according to point 3 of this article, shall have the right to ask the Office of Judicial Status for the respective information by e-mail or ordinary mail, in return for fulfilment of the requirements of the articles of this law.

5. The head of the Office shall verify every 24 hours whether the receipt of these data by the subjects has been done in compliance with the provisions of this law.

Article 9 **Distribution of written certificates**

1. Written certificates are obtained according to the provisions of article 484 of the Code of Criminal Procedure.

2. The directors, inspectors and specialists of the Ministry of Justice, in order to consult the data of the written register and the electronic registers, must have a periodic or special authorisation from the Minister of Justice or an official assigned by him. For the employees of the Office, the authorisation shall be issued by the head of the Office of the Judicial Register.

Article 10
Unlawful interventions

1. When an unlawful intervention is found in the register of judicial status, the competent organs must be notified immediately.
2. Unlawful interventions in the register of judicial status or in the computer transmission and dissemination of data about the judicial status of persons by the employees authorised for automatic processing of the data, constitute a criminal offence and are punished according to the provisions of the Criminal Code.

Article 11
Issuance of subordinate legal acts

1. The Council of Ministers, within 15 days from the entry of this law into force, shall specify the subjects who may present a request to obtain an electronic certificate at the Office of Judicial Status.
2. The Minister of Justice, within 30 days from the entry of this law into force, shall specify detailed rules for obtaining certificates electronically, according to article 8 of this law.

Article 12
Entry into force

This law enters into force 15 days after publication in the Official Journal.

SPEAKER
JOZEFINA TOPALLI (ÇOBA)

Declared by decree no. 5063, dated 04.10.2006, of the President of the Republic of Albania, Alfred Moisiu.

Attachment 8. Provisions of Criminal Code / Criminal Procedure Code referenced in E-cJS Law

Unofficial translation edited by Gina Schaar,
based on the originals available at

<http://www.legislationline.org/upload/legislations/ba/fb/3e7ef0be7ad60ee6e16cbd8b63db.htm> and
<http://www.legislationline.org/upload/legislations/0f/55/d46a10bcf55b80aae189eb6840b4.htm>

[Referenced in Law 9614, art. 2(2), art. 4(3), art. 9(1)]:

Criminal Procedure Code

CHAPTER III

CRIMINAL RECORDS

Article 481

Criminal record office

1. In the criminal record office which is under the Ministry of Justice, there are deposited the abridgements of the decisions for the persons tried for criminal matters.

Article 482

Entries in the criminal record book

1. In the criminal record there are registered by abbreviations:

- a) the sentences, once they become final;
- b) the sentences rendered by the court in the stage of execution;
- c) the decisions related to the execution of supplementary sentences;
- d) decisions of acquittal and dismissal.

Article 483

Deleting entries

1. The notes in the register are cancelled after the reception of the official notification of the death of the person to whom the notes belong or when he reaches the age of eighty.

2. There shall also be cancelled the notes related to:

- a) decisions revoked due to review or abrogation of the criminal offence;
- b) the decisions of acquittal or dismissal on expiry of ten years from the date on which the decision has become final;
- c) decisions of punishment for contraventions when a fine penalty is involved, on expiry of ten years from the day when the decision has been executed.

Article 484

Criminal record certificates

1. The authorities of justice, state administration and entities charged with public services are entitled to take certificates of notes of a particular person when the certificate is necessary to carry out their duties.

2. The prosecutor may request the above certificate for the defendant or the sentenced and, by authorization of the court, he and the defense lawyer may also request a certificate for the victims and witnesses.

3. The person who is the subject of the note in the criminal record is entitled to take the respective certificate and he has no obligation to explain the reasons in the request.

[Referenced in Law 9614, art. 4(3)]:

Criminal Code

Article 69

Rehabilitation

The sentencing of the following is considered null and void for:

- a) those who are convicted with imprisonment sentences less than six months or with any other lighter sentence, who have not committed any other criminal act for two years since the [last] day of their served sentence.
- b) those who are convicted of imprisonment sentences ranging from six months up to five years and who have not committed other criminal act for five years since the [last] day of their served sentence
- c) those who are convicted of imprisonment sentences ranging from five to ten years and who have not committed any other criminal act for seven years since the [last] day of their served sentence.
- c) those who are convicted of imprisonment sentences ranging from ten to twenty-five years and who have not committed any other criminal act for ten years since the [last] day of their served sentence.

[Referenced in Law 9614, art. 7(3)]:

Criminal Code

SECTION VIII

FALSIFYING DOCUMENTS

Article 186

Falsifying documents

Falsifying or use of falsified documents is punishable by a fine or up to three years of imprisonment.

When the person having the capacity to issue the document makes the falsification, it is sentenced up to seven years of imprisonment.

Article 191

Falsifying acts of civil records

Falsifying or use of falsified civil records is punishable by a fine or up to three years of imprisonment.

When the person having the capacity to issue the record commits the falsification, it is sentenced up to five years of imprisonment.

[Reference in Law 9614, art. 10(2)]

Criminal Code

Article 121

Intruding without ground into someone's privacy

Fixing appliances which serve for hearing or recording words or images, the hearing, recording or airing words, fixing, taping or transmitting images, as well as their preserving for publication or the publication of the data which exposes an aspect of the private life of the person without his consent, constitutes criminal contravention and is punishable by a fine or up to two years of imprisonment.

Article 122

Spreading personal secrets

Spreading a secret which belongs to someone's private life by the person who obtains that [secret] because of his duty or profession, when he is compelled to not spread it without prior authorization, constitutes criminal contravention and is punishable by a fine or up to one year of imprisonment.

The same act committed with the intent of embezzlement or of damaging another person, constitutes criminal contravention and is punishable by a fine or up to two years of imprisonment.

Article 192/a

Disappearance and theft of documents

(Added by Law No. 8733, date 24 January 2001, article 53)

Destruction by any manner of archive or library documents, as well as disappearance of documents that are of particular importance, in violation of legal requirements, is punished by fine or up to three years of imprisonment.

Theft of archive or library documents, that are of particular importance, or their export in violation of legal requirements, is punished by fine or up to five years of imprisonment.

Article 192/b

Interference in computerized transmissions

(Added by Law No. 8733, date 24 January 2001, article 53)

Interference in any form in computerized transmissions and programs constitutes criminal contravention and is punished by fine or up to three years of imprisonment.

The same offense, if it has caused serious consequences, is punished up to seven years of imprisonment.

SECTION II

CRIMINAL ACTS AGAINST THE ACTIVITY OF THE STATE COMMITTED BY PUBLIC OFFICIALS OR IN PUBLIC SERVICE

Article 248

Abuse of office

(Amended by Law No. 8733, date 24 January 2001, article 58)

Intentional commission or nonperformance of actions or omission of actions in violation of law, which constitutes ordinary nonperformance of duty by a person exercising a public function, when it brings unauthorized material or nonmaterial benefits to the person or to others, or causes damage to the lawful interests of citizens, the state or other juridical persons, if it does not constitute any other criminal act, is punished by imprisonment from six months up to five years or by a fine from three hundred thousand up to one million [Albanian] lek.

Article 313/a

Disappearance or loss of file

(Added by Law No. 8733, date 24 January 2001, article 77)

Disappearance or loss, in any manner, of an investigation or court proceeding file, as well as removal of documents, writings, or other data that are attached to such a file, if it causes serious consequences to the detriment of interests of citizens or the state, is punished by a fine or imprisonment up to five years.

Article 30

Supplementary punishments

Besides the principal punishment, a person who has committed offences or criminal contravention may also be punished by one or some of the following supplemental punishments:

1. Denial of the right to work as a state employee or in public service;

2. Confiscation of the means relevant to the commitment of the criminal act and of the profits deriving from it;
3. Ban on driving;
4. Stripping off decorations, honorary titles.
5. Deprivation of the right to exercise a profession or skill;
6. Deprivation of the right to undertake leading positions related to juridical persons;
7. Denial of the right to stay in one or some administrative units;
8. Expulsion from the territory;
9. Compulsion to make the court sentence public.

In particular cases, when the criminal punishment is deemed to be inappropriate and when the law provides for imprisonment up to 3 years or other lighter punishments, the court may decide only for the supplementary sentence.