Progress through technology

Privacy Rights in Kosovo

The Legal Framework and Implementation

TABLE OF CONTENTS

Executive summary

The amazing progress in telecommunications and information technology has had a remarkable impact on the world; life without a cellular phone or internet connection seems unimaginable now even though very few of us have had access to it only 20 years ago. This has however also entirely changed the way personal data and private information is gathered, stored and transmitted, exposing them greatly to the dangers of abuse. The law is therefore an indispensable instrument regarding the protection of privacy rights and the security of personal information.

Kosovo Assembly has adopted the Law on Protection of Personal Data (LPPD) on 29 April 2010 and a government agency to supervise and assist in its implementation was established over a year later. This project has aimed to review the most relevant legislation related to the protection of privacy currently in place in Kosovo, to compare it to the European context and to identify the potential obstacles to its implementation. It should be noted and acknowledged though, that the issue of privacy is complex and extends beyond the legal perspective to social, cultural and political dimensions.

The LPPD in itself is found to provide an adequate level of protection and it covers a wide area of challenges to data protection, without leaving out modern infringements of privacy such as video surveillance. Some amendment is seen as necessary; especially in treating private sector and public bodies equally and in levelling the fines with the severity of violations as well as the introduction of skimming of excess profits. While there are very few issues found in three other pieces of legislation related to the matter, the Law on Telecommunications, the Criminal Code and the Criminal Procedure Code, there is a certain need for regulation regarding internet providers, web-based media outlets and e-commerce, something that would be equivalent to the German Tele-media Law. It can however be said that there is generally a sound legal infrastructure in place, which, provided some necessary adjustments and modifications are performed, could provide sufficient protection of privacy rights and personal data in the near future.

The actual implementation of the legislation on the matter on the other hand would face a range of difficulties, some more acute than others. The striking lack of awareness and sheer ignorance among both the controllers and the data subjects is the single most significant practical obstacle to the implementation of legislation on the protection of personal data. Against this backdrop, the legitimizing effect of the data subject's consent raises severe problems. Namely, the Kosovo LPPD does in accordance with the EU legislation render any personal data free for processing so long as the data subject states his consent. Having in mind the alarmingly low level of awareness on the matter this provision is extremely problematic.

1. Introduction and European dimension

Phenomenal technological progress and increasing coalescence of daily practice and automated data processing have not only dramatically enhanced the need to gather and handle personal data, they have also led to an enormous stock of correlating knowledge to any given isolated data, rendering practically any information potentially relevant due to the inherent option to link and relate it to already existing data without notable effort. Unconsenting disclosure of or corrupt personal data can thereby yield severe consequences for the data subject, for example unfavourable conditions or even the complete refusal of a loan or a private life or health insurance policy. But there is also the interest of the citizen vis-à-vis the state of not becoming totally transparent and universally monitored. Therefore, an adequate legal framework regarding the protection and security of personal data is an imperative prerequisite for any constitutional democracy and a vital component of the rule of law. However, even the most elaborate law is bound to become ultimately futile without proper reception and implementation.

Furthermore, no European Country can reasonably be analyzed in any legal context without consideration of the supranational dimension. The essential and decisive regulatory instrument on the subject in question in the European Union is the EU Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data. Despite having been enacted as the legislative tool of a directive, the European Court of Justice made it clear in his ruling of November 24th 2011 (case C-468/10 and C-469/10 - “ASNEF”), that the Directive 95/46/EC is geared towards a full harmonization (as already indicated by the ruling of November 6th 2003, case C-101/01 - “Lindquist”) to the extent of prohibiting any alteration of its fundamental principles, even if they led to an increase of the level of protection. Consequently, any efforts to reach European standards and best practice have to be oriented closely towards said Directive. On top of that, a Regulation[1] is currently being drafted to replace the Directive with an overall higher level of protection, unfolding immediate effect in every member state and thus leaving even less room for individual concretization once implemented. At the same time, the draft provides a number of concretization powers for the European Commission. However, the legislative process can be expected to last about another two years, with an additional two years transitional period after entry into force (see Art. 91 of the draft).

[1] Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final. Available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

2. Overview of the Legal framework

Beside the General Law on the Protection of Personal Data, which is the main focus of this analysis, there are several other specifically relevant laws covering issues regarding privacy and the treatment of personal data in the respective sector-specific context that shall be covered in the present report.

2.1. Law on the Protection of Personal Data (LPPD)

The "Law on the Protection of Personal Data" (Law No. 03/L-172), adopted by the Kosovo Assembly on April 29th 2010, is the central legal document regarding the subject of data protection and data security in Kosovo. Overall, its regulatory content reflects the focal rulings of the EU Directive 95/46/EC and provides an adequate level of protection, accommodating the complexity of the subject matter and the practical challenges of data treatment. In particular, it provides detailed regulations on the lawfulness of the processing of personal data (Artt. 5 et seq. LPPD) with specifics regarding special categories of data (sensitive personal data) and automated individual decisions, on the information to be given to (Art. 10 LPPD) and the rights of the data subject (Artt. 21 et seq. LPPD), on the confidentiality and security of processing (Artt. 14 et seq. LPPD), on the Supervisory Authority (Artt. 29 et seq. LPPD) and the correlating notification obligations (Artt. 17 et seq. LPPD), on judicial remedies and sanctions (inter alia Artt. 26, 27, 79 et seq. and 92 LPPD), on the transfer of personal data to third countries (Artt. 51 et seq. LPPD) and even inter alia special provisions regarding direct marketing (Artt. 59, 60 LPPD), video surveillance (Artt. 61 et seq. LPPD), the use of biometric features (Artt. 65 et seq. LPPD), linking filing systems (Artt. 71 et seq. LPPD) and the data protection official for public bodies (Artt. 74 et seq. LPPD). Given this backdrop, criticisms and suggestions in this respect are of limited reach and importance.

Nevertheless, it should be pointed out that the appointment of a data protection official being mandatory solely in public bodies is insufficient. There should in fact also be adequate regulations for the private sector (medium to large businesses etc.). In so doing, the obligation to choose and appoint an internal data protection official should be contingent upon the individual number of employees permanently engaged in the processing of personal data. While according to statements of the authorized Supervisory Agency (National Agency for Protection of Personal Data) guidelines containing corresponding regulations are currently being implemented in the form of sub-legal acts[2] , the incorporation in the LPPD itself would be an even more expedient course of action to account for the significance of the issue.

Furthermore, the maximum fees seem far too benevolent. In order to effectively serve their purpose and have a sufficient deterrent effect they should in fact be increased. Otherwise eminently severe violations of privacy cannot be addressed accordingly and controllers have insufficient incentive to actually obey the law, specifically in situations where a violation

[2] Interview with State Deputy Chief Supervisor Mentor Hoxhaj on March 30th 2012.

provides a substantial economic benefit. For that very reason, an additional option for skimming of excess profits should be implemented.

2.2. Law on Telecommunication

The Law on Telecommunication (Law No. 2002/7) covers aspects of Data Protection in Chapter 13 Section 74 et seq. which overall provide a sufficient level of protection. Section 74 subjects telecommunications service providers to specific confidentiality obligations and paragraph 2 in particular limits the obtaining of information related to the content, facts or circumstances of messages transmitted to the absolute minimum required for the performance of individual telecommunications services. However, the regulation regarding the Monitoring of Telecommunications Traffic in Chapter 8 Section 46 raises some concerns as to whether the existing legal bases for such conduct provide the clarity and precision needed to meet the requirement of legal certainty in the context of such an invasive measure. Therefore, the section "pursuant to the applicable rules of criminal procedure or any other relevant law or UNMIK Regulation" should be adjusted in order to determine specifically which laws are applicable.

2.3. Criminal Code

Artt. 168 et seq. of the Provisional Criminal Code of Kosovo (UNMIK/REG/2003/25) fundamentally provide sufficient bases for punishable offences regarding severe violations of privacy. However, the fundamental violation of another person's privacy by means of video surveillance without consent not being criminally relevant according to Art. 171 of the Criminal Code unless conducted in the "personal premises" of the victim is a particularly suspect legal assessment and contradicts the telos of the law. The relevance of this subject has been exemplified very recently by a startling case pertaining the National Dance Ensemble "Shota", where reputedly (yet contested by the director) video surveillance measures were implemented in the dancers' dressing room[3]. The Supervisory Agency addressed the issue and ascertained a violation of the LPPD, temporarily shutting down the surveillance. The specifics at hand notwithstanding, blatant violations of privacy like surveillance measures in particular intimate settings (e.g. dressing rooms, bathrooms, showers etc.) should be a matter of criminal law regardless of the "non-personal" nature of the concerned premises. It is therefore advisable to adjust the law accordingly.

2.4. Criminal Procedural Code

The legal provisions in the Provisional Criminal Procedure Code of Kosovo (UNMIK/REG/2003/26) regarding matters concerning personal data overall do not raise reasons for objections. The particularly relevant regulations in this context respecting covert and technical measures of surveillance and investigation (Artt. 256 et seq.) are each conditional

[3] cf http://www.koha.net/?page=1%2C5%2C93254.

upon a grounded suspicion of a qualified offence and provide the clarity and precision needed to meet the requirement of legal certainty.

2.5. Lack of specific Telemedia Law

It is however notable, that there is no specific Telemedia Law currently implemented. This deficit should be remedied due to the great practical significance and the specific idiosyncrasy of the subject matter, especially regarding questions related to the protection of personal data on the internet and in ubiquitous environments.

3. Implementation

In spite of the existence of a detailed and overall adequate legal framework, as illustrated above, the actual implementation meets several difficulties.

3.1. Inscrutability of Internal Data Processing Operations

A structural problem of implementation and enforcement of regulations regarding the protection of personal data is the fact, that significant parts of data processing procedures are basically inscrutable for Supervisory Agencies as well as data subjects due to lack of comprehensive insight into actual internal data processing operations. Whether a legal obligation to delete personal data is actually obeyed by the controller in order that no traces of the data are still in existence or remain reconstructable can be almost impossible to examine, personal data can be gathered, stored and most importantly passed on without the data subject ever knowing and the more entities possess (and share as the case may be) the same information about a person permissibly, the harder it becomes to retrace the perpetrator of even manifest violations. Since there is no real option to address this inherent issue it is crucial for data subjects as well as law-abiding controllers to operate according to the principles of data avoidance and data economy and to make data treatment procedures as transparent as possible. The compliance with obligations to provide information is an important aspect but ultimately the most effective way to prevent clandestine or even manifest misuse of personal data is for the data subject to prevent unnecessary disclosure of personal data in the first place.

3.2. Ignorance and Lack of Awareness

But then, presumably the most significant practical obstacle regarding the implementation of data protection law is the striking lack of awareness among controllers and data subjects alike. Neither are data subjects aware of the value and sensitivity of their personal data and that they are actually protected by law, nor do controllers generally know about their responsibilities concerning this matter or have a sense of wrongdoing while illicitly gathering and sharing protected personal data. Characteristically, according to insight gathered for a Policy Brief on the Protection of Personal Data in Kosovo of August 22nd 2011 neither the key officials leading the process of the Census 2011 nor any of the officials of the Telecommunication Regulation Authority involved in the process of Registration of Mobile Phone Users 2011 were even aware of the existence of the LPPD and the obligations deriving from it. [4] According to statements by citizens it is not uncommon for telecommunications service providers to give away comprehensive personal information (full name, address, birth date and -place etc.) about the holder of a specific mobile phone number just on request by telephone.

[4] KCSS Policy Brief Protection of Personal Data in Kosovo, conducted by Mentor Vrajolli and Sofije Kryeziu, page 3.

A survey conducted under strict conditions of anonymity (as requested by the majority of subjects) involving major Kosovo banks and insurance companies, not excluding communications and internet services providers, showed that private sector has only recently started to consider issues related to protection of personal data and that even officers managing compliance issues within most organizations (with very few exceptions) had little knowledge of subject in matter. The less senior staff directly involved in collection of personal data was virtually uniformed of limitations and potential violations. Another finding that was quite clear in this survey was the immediate need for training of both senior and junior staff in private sector.

It should be noted however, that in most cases NAPPD had established initial contact and briefed to a certain extent the subjects.

3.3. Indeterminate Legal Terms

Furthermore, the applicable norms of the legal framework contain numerous indeterminate legal terms, which are open to and require interpretation as well as concretization. Being drafted mainly by international experts and strongly based on the respective laws of the European Union or individual member states which possess elaborate jurisdiction and administrative ascertainment concepts, that have been established in praxis over long periods of time, they present the rudimentary Kosovan implementation entities with seemingly insurmountable operationalization difficulties. For want of a corresponding concretization concept, the average Kosovan data controller can by no means be realistically expected to adequately decide, whether a specific data processing is e.g. “necessary” in a legal sense and therefore permissible in the given context. While the problem is mitigated to a certain extent by each data controller’s legal obligation to establish filing system catalogues (Art. 17 LPPD) and to notify in advance the Supervisory Agency (Art. 18 LPPD), thus allowing for influence and support on the part of the latter through the approval proceedings, neither every process of data treatment nor every case-by-case decision is covered to begin with and the provided concretization inherently cannot reach the necessary magnitude and level of detail. Moreover, the whole process in question is very time-consuming.

It is therefore recommendable to introduce concretizing guidelines at a level of medium abstraction in the form of administrative provisions for the public sector and corresponding instructions for the private sector. These guidelines should contain concrete weighting parameters and exemplifications for central legal terms of practical relevance.

3.4. References to Additional Law

The practical need for sector-specific regulation of data protection related fields leads to the risk of legislative discord or even incommensurability in regard to the general Law on the Protection of Personal Data, especially as far as older laws that have been drafted and adopted without the consideration of current problems in the field of data protection are concerned. It is

therefore necessary to harmonize sector-specific laws referenced in that way (already existing as well as newly created laws) in order to reach or maintain an equal level of protection.

3.5. Legitimizing Effect of the Data Subject's Consent

In accordance with the respective regulations at a European level (Art. 7 lit. a Directive 95/46/EC), the LPPD provides the option to legitimize the processing of personal data on the basis of the data subject's consent, as long as it is an "unambiguous, freely given specific and informed indication of the data subjects wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed" (Art. 2 1.10 LPPD). Thus, as long as the data subject agrees correspondingly, practically any use of the relevant data is permitted according to the law. Especially in view of the severe lack of awareness and thematic insight among the population of Kosovo, as depicted above, this brings about serious problems.

First of all, the specific requirements for an "informed" consent are very hard to determine. It is in any case essential for the data subject to fully grasp the meaning and scope of the decision to agree to a particular treatment of his or her personal data. However, this does not only presuppose a comprehensive clarification of nature, purpose and circumstances of the data handling but also the ability of the data subject to accurately assess the consequences and implications for him or her. In other words, an informed consent requires knowledge, competence and responsibility on the part of the controller and a sense of privacy and awareness regarding the value of personal data as well as the risks involved in disclosing them on the part of the data subject. Against the background of the general situation in Kosovo with respect to the ignorance and the lack of awareness regarding the topic of protection of personal data, as depicted above, this will in praxi very rarely be the case.

Furthermore, the requirement of a "freely given" consent is rather problematic in several common situations with an inherent lack of voluntariness. Typical constellations in this respect would be asymmetrical power relations (e.g. during a job application process or a loan negotiation) or situations of structural dependency (like data gathering during an emergency admission) where it would be an absurd notion to assume the data subject could actually assess the appropriate extent of disclosure or even think about refusing to declare his or her consent regarding the gathering of personal data deemed unnecessary in the given context.

While against this backdrop the subject of informed and freely given consent is problematic even in countries with a comparatively well established legal and administrative environment and state of public awareness, these difficulties appear dramatically exacerbated under the afore-mentioned conditions currently obtaining in Kosovo. Therefore, the significant extent of the legitimizing effect of the consent is not in the interest of the data subject and should be limited in order to prevent excessive data treatment. The legal framework should thus be temporarily adjusted so that the legitimization of data treatment via the data subject's consent becomes a priori only possible in entirely unambiguous cases where it is obvious, that the data subject fully grasps the meaning, scope and consequences of the decision and that the voluntariness is not impaired. While such action restricts the autonomy of the data subject and

introduces a partial legal incapacitation, this disadvantage is outweighed by the dangers of excessive data treatment and the data subject's interest to prevent it. Resulting in an alteration of one of the fundamental principles of the Directive 95/46/EC (e.i. data treatment generally being lawful if based on the data subject's unambiguously given consent) the suggested changes would put the respective laws in discord with harmonized European Law de lege lata and de lege ferenda. However, in order to reach a state that would allow for Kosovo to actually become a member state and thus immediate subject to European Law, the afore-mentioned deficits would have to be eliminated anyway and the necessity of temporary restrictions to the legitimizing effect of consent therefore rendered obsolete. The problem could also be addressed by exceptionally strict interpretation of the existing legal requirements for a valid consent, ideally leading to the same results as the law adjustment suggested above. This would however introduce an unnecessary mediate and indirect character to these requirements (especially given the fact, that the concretization of indeterminate legal terms is an implementation problem of its own, vide supra) and sacrifice legal certainty without any less incapacitation of the data subjects autonomy while carried out as intended. The first alternative is therefore preferable.

4.1 Conclusions

The legal framework regarding the protection and security of personal data in Kosovo is overall adequate. The actual implementation on the other hand meets several severe difficulties:

First of all. there is a structural problem of inscrutability of internal data processing, that can only be addressed by a policy according to the principles of data avoidance and data economy as well as restrained disclosure on the part of the data subject.

However, the gravest obstacle to proper implementation is the striking lack of awareness among data controllers and data subjects alike. Neither citizens nor people professionally concerned with the handling of personal data are generally aware of the existence of a legal framework and even the most fundamental obligations deriving from it.

Against this background, the legitimizing effect of the data subject's consent is highly problematic as well due to the inherent lack of the basic premises for an informed and freely given indication of the data subject's agreement.

Furthermore, the frequent use of very abstract indeterminate legal terms without concretizing guidelines presents the implementation entities with significant problems due to the lack of elaborate jurisdiction and administrative ascertainment concepts, that have been established in praxis over long periods of time.

4.2 Recommendations

I. The appointment of a data protection official being mandatory solely in public bodies is insufficient, there should in fact also be the obligation to choose and appoint an internal data protection official contingent upon the individual number of employees permanently engaged in the processing of personal data for the private sector. This obligation should ideally ne implemented directly into the LPPD.

II. In order to effectively serve their purpose and have a sufficient deterrent effect, the maximum fees for violations should be increased.

III. Furthermore, specifically for situations where a violation provides a substantial economic benefit an additional option for skimming of excess profits should be implemented.

IV. In order to provide the clarity and precision needed to meet the requirement of legal certainty, in the regulation regarding the Monitoring of Telecommunications Traffic in Chapter 8 Section 46 of the Law on Telecommunication the section "pursuant to the

applicable rules of criminal procedure or any other relevant law or UNMIK Regulation" should be adjusted in order to determine specifically which laws are applicable.

V. In the Criminal Code Art. 171 should be adjusted so the fundamental violation of another person's privacy by means of video surveillance without consent is no longer restricted to conduct in the personal premises of the victim. It should rather apply to particular intimate settings in general (e.g. dressing rooms, bathrooms, showers etc.).

VI. Due to the great practical significance and the specific idiosyncrasy of the subject matter, especially regarding questions related to the protection of personal data on the internet and in ubiquitous environments, a specific Telemedia Law should be drafted.

VII. In order to raise awareness among the population of Kosovo additional campaigns regarding the topic of the protection of personal data and the respective legal framework are necessary.

VIII. There is an immediate need for training of both senior and junior staff in the private sector regarding the legal framework as well as the practical implementation of data protection and data security.

IX. It is furthermore recommendable to introduce concretizing guidelines for the interpretation of decisive indeterminate legal terms at a level of medium abstraction in the form of administrative provisions for the public sector and corresponding instructions for the private sector. These guidelines should contain concrete weighting parameters and exemplifications for central legal terms of practical relevance.

X. Sector-specific laws touching topics of the protection of personal data (already existing as well as newly created laws) that are referenced in general law on that matter should be continually harmonized in order to reach or maintain an equal level of protection.

XI. The significant extent of the legitimizing effect of the consent is currently not in the interest of the data subject and should be limited in order to prevent excessive data treatment. The legal framework should thus be temporarily adjusted so that the legitimization of data treatment via the data subject's consent becomes a priori only possible in entirely unambiguous cases where it is obvious, that the data subject fully grasps the meaning, scope and consequences of the decision and that the voluntariness is not impaired.

Annex 1.

List of abbreviations used in the report

EU	European Union
EC	European Commission
COM	Council of Ministers
UNMIK	United Nations Interim Administration Mission in Kosovo
EULEX	European Union Rule of Law Mission in Kosovo
LPPD	Law on Protection of Personal Data
NAPPD	National Agency for Protection of Personal Data
CC	Criminal Code
CPC	Criminal Procedure Code
KCSS	Kosovo Centre for Security and Stability