SECRETARIAT GENERAL

Directorate General
Human Rights and Rule of Law

DGI(2014)8
Strasbourg, 14 February 2014

Opinion

of the
Directorate General Human Rights and Rule of Law
Data Protection Unit
on the

Draft laws of Georgia relating to Surveillance Activities of Law Enforcement Authorities and National Security Agencies

Prepared on the basis of the expertise by

Douwe KORFF (The Netherlands)
European human rights and data protection expert, Professor of International Law at London Metropolitan University

Joseph A. CANNATACI (Malta)
Chair in European Information Policy & Technology Law, Co-Director STeP - Security, Technology & e-Privacy Research Group, Department of European and Economic Law, Faculty of Law, University of Groningen

Graham SUTTON (United Kingdom)
Independent Data Protection Expert, Former Policy Adviser,
Department of Constitutional Affairs, Ministry of Justice

Table of contents

List of abbreviations

DP	Data protection
Convention 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
CPC	Criminal Procedure Code
LEA	Law enforcement agency
OSA	Operational-Search Activities
SIS	Security and Intelligence Services
DPA	Data Protection Authority
DRD	Data Retention Directive
PDP Inspector	Personal Data Protection Inspector
LEA	Law Enforcement Agency
ECHR	European Convention on Human Rights
DPRP	Data Protection Reform Package
CJEU	Court of Justice of the European Union

Executive summary

The legislative proposals seem to seek to achieve the following:

- expand the scope of personal data protection;
- bring law enforcement under the purview of the general data protection regime;
- reinforce the rights of data subjects;
- toughen legal safeguards against illegal surveillance;
- mandate notice and simplify redress procedures;
- extend the powers of the Personal Data Protection Inspector;
- introduce parliamentary control over personal data protection.

It is recommended that the following issues be considered by the Parliament of Georgia:

1. Prior to any legislative action (unless already done), an in-depth qualitative study of personal data handling by Law Enforcement Agencies (LEAs) and Security and Intelligence Services (SIS) in Georgia should be carried out as a matter of urgency.
2. Compliance with the Council of Europe's Rec(87)15 regulating the use of personal data in the police sector be established as a key goal of reform of the related laws.
3. In a country like Georgia where expertise on data protection laws is, for historical reasons, limited, it would make sense to bring together oversight functions of all privacy and data protection matters in one agency provided that it is sufficiently resourced (cf. Austria and Luxembourg approach).
4. Regulation should be properly thought through and reflect modern technological realities where much personal data is not actually generated and retained by either LEAs or SIS but rather by commercial entities and citizens themselves and what LEAs and SIS wish to do is access and/or monitor/intercept personal data generated and retained by the private sector or elsewhere in the public sector.
5. Surveillance and smart surveillance are growth areas which are also seeing a blurring or lines between the public and the private sectors and Georgia might follow closely and await the outcomes of the international debates on these subjects.
6. The time factor is also important, subject to the outcome and findings of the in-depth study recommended in 1 above, and taking account of the international debate on the subject, the most urgent needs in terms of legal framework, resources and other matters should be identified and agreed.
7. Reconsider plans for implementing provisions of the Data Retention Directive into Georgian law.
8. Further consideration is proposed of specific amendments.

1 Introduction

The Council of Europe has been requested by the Chair of the Parliament of Georgia to provide an expert analysis of a series of texts, aimed at framing the surveillance activities of the law enforcement agencies (and possibly also those of the national security agencies) of the Republic of Georgia. The texts consist of proposed amendments to the following laws:

- The Law of Georgia on the Amendments to the Law of Georgia on the "Personal Data Protection".
- The Law of Georgia on the Amendments to the Law of Georgia on “Electronic Communications”.
- The Law of Georgia on the Amendments to the “Regulations of the Parliament of Georgia”.
- The Law of Georgia on the Amendments to the Criminal Procedure Code of Georgia.
- The Law of Georgia on the Amendments to the Law of Georgia on the “Operational-Search Activities”.

The present opinion is based on the European Convention on Human Rights, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, its Additional Protocol, Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (which amends Directive 2002/58/EC), , as well as the Opinion of the Advocate General of the Court of Justice of the European Union (CJEU), Mr Cruz Villalón, in relation to the Data Retention Directive.

The opinion is built on comments prepared by the following scientific experts:

- Douwe Korff, who is a European human rights and data protection expert working closely on those issues with the Council of Europe and the European Union, and with European and national civil liberties and digital rights organisations. As a Council of Europe expert, he has trained many judges and prosecutors in Georgia in ECHR law, and he edited the English translation of the 2005 Council of Europe report by Prof. Konstantin Kordelia and others on Compatibility of Georgian Legislation with the standards of the European Convention on Human Rights. He is Professor of International Law at London Metropolitan University.

- Joseph A. Cannataci, who is a European information policy and technology law expert working closely on these issues with the Council of Europe and the European Union. As a Council of Europe expert, he has carried out expert missions in a number of countries including Bulgaria, Czech Republic and Ukraine. Over the past quarter of a century he has served as Chairman of several Committees of Experts of the Council of Europe: MedialLex (1994), Working Party on Data Protection in Insurance (1994-1997), Working Party on Data Protection in New technologies (1995-2000), the Committee of Experts on Data Protection (1996-98) and Vice-Chairman of the Group of Specialists on the impact of New Communications Technologies on Fundamental Rights & Democratic Values (1999-2001). Most recently he has been Expert Consultant to the Council of Europe’s Consultative Committee on Data Protection responsible for drawing up the report (2011-2013) on data protection in the police sector and to the Council of Europe’s Cybercrime division preparing an analysis on data protection and network security (2012-2013). He is the chief architect and overall scientific coordinator of several recent or current major EU-funded research projects dealing with privacy and surveillance, including CONSENT, SMART and RESPECT.

For the purposes of this analysis, Professor Cannataci also enjoyed the close collaboration of a team member and colleague, Dr Oleksandr Pastukhov, with close knowledge of data protection in the emerging democracies of Central and Eastern Europe.

- Graham Sutton, who formerly worked for the UK civil service where he spent twelve years in charge of data protection policy. Since taking early retirement in 2004, he has continued to work on data protection as a free-lance consultant. Among other things, he has advised on the development of data protection policy in China as well as a number of the new democracies in central and eastern Europe.

2 Preliminary considerations: local knowledge, international context & a matter of form

The legislative package appears to, at least partially, have been formulated in response to a number of scandals that shook Georgia following the parliamentary elections of 2012. The present analysis assumes that the reader is familiar with these and other relevant international and Georgian developments and has access to a number of background publications which would help place the comments and conclusions in an appropriate context.

2.1 An understanding of the operational requirements and the local data protection context

It would not be unreasonable to expect that amendments to existing laws or new laws on data protection in Georgia would strive to achieve a combination of two main objectives:

- to specifically address a number of problem situations that may have arisen in Georgia in the context of data protection over the past years especially in the area of handling of personal data by LEAs and SIS;

- to ensure that legal provisions, financial, material, human and other resources as well as relevant national policies are in line with accepted broadly minimum standards in Europe.

It has been difficult for the expert team to ascertain whether the proposed legislative proposals are part of a comprehensive carefully-thought through package of measures which respond adequately to the situation on the ground in Georgia. The legislative proposals received for evaluation were not accompanied by the type of in-depth report that one would normally expect to have been carried out as a pre-requisite to legislative and complementary actions. It is reasonable to expect that legislative proposals, especially of provisions intended to “fix” data protection laws which have not even been in force for two years as in the case of Georgia, provide a reasoned response to a well-defined set of circumstances.

An analysis and practices on technical capacities for interception, monitoring and general surveillance practices within Georgia has not been made available either. In other words, it has not been possible to discern what kind of surveillance technologies are being deployed on a regular basis and the level of sophistication or coverage that these technologies may have attained within Georgia, thus enabling an assessment of capabilities to be accurately carried out even through various forms of comparative analysis which would be placed in the context of a post-Snowden Europe.

Finally, Georgia is not one of those countries which have contributed data to the PUPIE project so its level of compliance or implementation of Rec(87)15 has not been gauged in a structured manner at par with that of over 30 other European states.

The Parliament of Georgia ought to have a solid factual base and good understanding on the policy objective to ensure the best legislative outcome.

It is expected that the Parliament of Georgia would be seeking to base its decisions on an evidence-based approach and therefore would be reluctant to endorse legislative or other action unless and until the required level of evidence is collected, analysed and published as and when appropriate. This in itself would suggest that embarking immediately on a course of legislative intervention may ultimately result in a case of “more haste, less speed”. The facts of the case need to be better known or if they are already known to be reported upon and analysed in the most transparent of manners in order to enable a more reliable evaluation of the legislative requirements.

2.2 The current European and wider international context

The preceding arguments deal with the situation inside Georgia and with the relevance of an accurate level of knowledge of various practices inside that country. They do not take into account the level of fluidity currently being experienced within the wider European context. It should be borne in mind that, at the time of writing (December 2013-January 2014) the EU's January 2012 Data Protection Reform Package (DPRP) is not finalized.

The Council of Europe is still in the process of deciding how to take things forward in the modernisation of its legal instruments dealing with data protection issues for LEAs and SIS. The debate in Strasbourg in a CoE context, like the one in Brussels in an EU context, is not mature enough to suggest rushing into immediate legislative action. Not only will there continue to be debates in parallel in Brussels (EU) and in Strasbourg (CoE) but necessarily in parallel there will be developments or stalemate in the international regulation of mass surveillance across borders as an outcome over the consequences of the Snowden revelations.

2.3 A matter of legislative approach and philosophy

When surveying the legislative package it is clear that the drafters took an approach whereby they have attempted to subject the activities of Law Enforcement Agencies (LEAs) to ordinary or general Data Protection Law unlike many states which have separate laws regulating the personal data handling by LEAs. This omnibus approach is one taken hitherto by a small minority of European states but this does not render it any the less valid. Indeed the discussion about whether to have separate or consolidated data protection laws covering LEAs as well as other public and private entities has been raging for over 30 years and has continued right into the debate over the EU’s recent January 2012 Data Protection Reform Package (DPRP). There are in point of fact no clear objections arising from fundamental legal theory or indeed from practical operational practice as to having LEAs covered by the same piece of legislation and indeed in some recent cases it has been publicly argued by MEPs and commentators alike that this may be a preferable approach since it introduces clarity and reduces fragmentation and dissonance between different legal texts.

It is perfectly possible to have a single over-arching law on data protection with detailed sub-sections – or indeed subordinate legislation – written to make more detailed provision where this is needed, for example in areas of application as diverse as law enforcement, medical data, statistical data, insurance data, etc. As recently confirmed in the PUPIE project some countries have taken the Council of Europe’s Rec(87)15 on data protection in the police sector and transposed it into law as subordinate legislation as part of their generic data protection law and apparently with perfectly valid results. Indeed, it may be argued that the reasons for the existence of different laws and oversight regimes is historical and does not find any basis in legal logic or operational requirements.

There is no publicly available evidence that those countries where LEAs are regulated under general Data Protection Law or sub-legislation enacted in terms of a general data protection law enjoy a lower standard of privacy and data protection than those countries which have LEAs and Security & Intelligence Services (SIS) regulated under completely separate pieces of legislation. All the evidence available instead points in the direction of the existence of the two separate regimes being an accident of history which arose simply because of the rate of speed of culture change in society.

This is a long drawn-out struggle where the LEAs and SIS attempt to justify separate regimes for the way that they handle personal data. This is becoming increasingly more difficult as technologies converge and LEAs and SIS increasingly wish to have access to the same personal data going across the same fiber-optic cables or processed in the same databases by the same large private corporations or public entities. The latest available research suggests that the public at large are increasingly privacy-conscious: what they mind is being watched or spied upon and who is doing the watching does not significantly allay their fears of being unnecessarily and obtrusively watched. Therefore the issue of these measures being incorporated in one law or in separate pieces of legislation is not in this report treated as a matter of dogma or indeed one of consequence. Instead it is treated as a matter of form in an area where our primary focus will be on the substance of what the law may actually contain. If having everything condensed into one law instead of being spread across two or more pieces of legislation actually contributes to increased clarity and reduce fragmentation then so be it.

3 Comments on the draft amendments

3.1 Proposed amendments to the Data Protection Law and to the Parliamentary Regulations[1]

3.1.1 Draft laws generally

The first of the two Draft Laws is an omnibus legislative act introducing changes to Georgia's current DP Law, while the second one is of an auxiliary character and stipulates the procedure for electing the Personal Data Protection Inspector in the Parliament of Georgia. The changes both Drafts introduce together are numerous and of varied nature and significance, but can be grouped into several categories examined in turn below.

3.1.2 Bringing law enforcement under the general data protection regime

By introducing new Article 31 and removing corresponding exceptions to the scope of the Law's applicability contained in Article 3 (para 3 sub-para 'd') personal data protection "for the purposes of public and state security (including economic security), defense, operational-search measures and investigation of crimes" is being brought under the purview of the general data protection regime and makes it subject to control by the Personal Data Protection Inspector. These developments are in accordance with the letter and the spirit of the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the 2001 Additional Protocol regarding supervisory authorities and transborder data flows, and the Recommendation No. R (87) 15 of the Committee of Ministers of the Council of Europe on Regulating the Use of Personal Data in the Police Sector.

Processing of personal data in the said areas is limited only by the restrictions to the Law's Chapters II, III and IV envisaged in the Criminal Procedure Code, the Law on Operational-Search Activities "or other special law" (Art. 31 para 1) and grants the data subject a right to redress in case his/her rights under the Law were violated during such processing. The Inspector's powers are reinforced by dropping the requirement of a 3-day notice to be given

[1] Draft of 9 September 2013

under the current Law to an "institution, activities of which are related to the state security and defense, or which carries out operational-search activities" that he/she plans to inspect (Art. 35 para 6). These novelties introduced by the Draft Law correspond to the position of the European Court of Human Rights, according to which "there must be a measure of legal protection in domestic law against arbitrary interferences… especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident".

The scope of the Law's applicability is further expanded by limiting its protection to the data being processed by courts for case management purposes until the final judgment is delivered, while the current version of the DP Law does not apply to the whole "processing of data for case management purposes at the courts" (Art. 3 para 3 sub-para 'b'). Although both such derogations are possible under the Convention, it takes a notice by a declaration addressed to the Secretary General of the Council of Europe to be given and a list of categories of personal data to which the state will not apply the Convention to be deposited or amended; the list cannot contain categories of data protected under domestic law (Art. 3(2)(a)). Not a single such notice has been given by Georgia to date.

3.1.3 Toughening the legal safeguards

The legal safeguards of the right to personal data protection provided for in the current DP Law are considerably reinforced by the Draft. Thus, the bases for restrictions of the rights of a data subject under Articles 15, 21 and 22 (the latter is the Georgian counterpart of the Convention's Art. 8) of the Law no longer include "important financial or economic (including monetary, budgetary and tax-related) interests of the country" (Art. 24 para 1 sub-para 'd'), which exceeds what is required by the Convention that allows derogations in the interests of "the monetary interests of the State" (Art. 9 para 2). This can be seen as an effective measure against privacy abuses under the pretexts of fighting tax evasion, money laundering and terrorist finance.

Furthermore, the requirement of a written consent of the data subject has been extended to include all the instances of processing of the "special category of data" allowed under Article 6 of the Law (para 2) and in all such instances the disclosure of the data to a third person without the consent of the data subject is now prohibited (para 3). The new rules come short of the strict requirements for consent envisaged in Articles 7 and 8 of the proposed EU Data Protection Regulation, but they are definitely a step in the right direction. At the same time, removing the voluntary making public of personal data by its subject from the list of grounds for legal processing of the "special category of data" seems to be too restrictive compared to Directive 95/46/EC that makes such processing legal if it "relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims" (Art. 8(2)(e)).

3.1.4 Extending the powers of the Personal Data Protection Inspector

The powers of the Personal Data Protection Inspector are substantially extended under the proposed amendments to the DP Law. Upon the amendments coming into force, the Inspector will get the powers to consider a data subject's complaint concerning a violation of his/her rights by a private institution, inspect a private institution and take enforcement measures. Under the current Law, these powers the Inspector was supposed to get only on 1 January 2016 (Art. 56 para 3).

According to the amendments to the DP Law, the Inspector's requests for information should be met within 10 days, as opposed to 15 days prescribed by the current Law (Art. 21 para 3). The duty to notify the Inspector of creating a filing system and entering new category of data therein now does not depend on the size of a data processor, whereas the current Law provides an exemption for companies with less than 20 employees (Art. 20 para 3).

While all these changes are not dictated by the need to bring provisions of the Georgian DP Law in line with those of the Council of Europe instruments, they are definitely in accordance with the spirit of the Additional Protocol to the Convention that envisages "powers of investigation and intervention" to be vested in the data protection supervisory authorities of the participating states (Art. 1(2)(a)).

3.1.5 Introduction of the parliamentary control

The two Draft Laws introduce parliamentary control of personal data protection in Georgia. Under the draft amendments to the DP Law, the Prime Minister now, instead of appointing the Personal Data Protection Inspector, submits one of the three candidacies selected by the competition commission to the Parliament (Art. 28 paras 4-5). Thereafter, according to the new paragraph 51 of Article 28 of the DP Law and the identical new Article 2152 of the Parliamentary Regulations, the Parliament elects the Inspector by simple majority vote. If the candidate fails to receive the required number of votes, the Prime Minister submits another candidacy from the three selected by the competition commission. Every candidacy can be submitted up to two times. If none of the candidates receives sufficient number of votes, a new competition is held by the commission.

The report on the state of affairs with personal data protection in the country that the Inspector submits to the Government and has published annually now has to be submitted to the Parliament as well (Art. 38 para 1).

While the procedure for electing a data protection supervisor is not prescribed by any of the Council of Europe or EU instruments, the proposed multi-stage election procedure involving Georgia's executive and legislature, along with reporting to both branches of the government, is a big step towards meeting the standard set by the Additional Protocol and Directive 95/46/EC (Art. 28(1)), according to which the supervisory authority exercises its functions in "complete independence" (Art. 1(3)). A lot remains to be done, however, to achieve the Inspector's true freedom from political and economic influences in budgetary and staffing matters, the importance of which has been recognized by the relevant EU case law.

As explained in the Explanatory Note to the proposed amendments, the Personal Data Protection Inspector (PDP Inspector) is currently appointed by and accountable only to the Government, and this is an insufficient guarantee for the effective control over the personal data protection in the state institutions. If adopted, the amendments would ensure that the PDP Inspector will in future be appointed by, and will report to, Parliament.

This is a positive proposal that can be quite simply introduced. There should also be a separate, equally independent authority for the supervision of LEA and SIS surveillance measures (including in particular interception and analysis of Internet activity and e-communications data), and such an authority too should be appointed by and answerable to Parliament.

3.1.6 Comments on specific amendments to the Data Protection Law

Amendment 1

At present, by virtue of Article 3(3)(b), the Law on the Protection of Personal Data does not apply to the processing of personal data for case management purposes at the courts. The effect of this amendment is that the DP Law would apply once the court had rendered its final judgment in a particular case. While this restriction on the scope of the exemption is welcome, it is not clear why a complete exemption until the passing of the final judgment is needed. A better approach would be to apply the DP Law but to provide for an exemption to the extent that the application of that law would be likely to prejudice the court proceedings.

It is recommended that a regulation be drawn up jointly by the Personal Data Protection Inspector and the Council of Judges on the application of the test of "likely prejudice" in practice. That regulation should also clarify the procedural aspects (like the need to seek judicial approval for exceptions in certain cases). The amendment should expressly require the drawing up of such a regulation.

The DP Law could also stipulate that if certain matters are specifically regulated in the Criminal Procedure Code (e.g., access to a case file by the defence, and exceptions to such access), the rules in the CPC override the rules in the DP Law. However, it would be important to review the relevant rules in the CPC to bring them as much as possible in line with the rules in the DP Law (with deviations from the DP rules limited to what is necessary under the "likely prejudice" test).

Amendment 3

Paragraph 1 of the new article added by this amendment would limit the scope of the Law in its application to the fields of activity newly brought within the scope of the Law by Amendment 2 (that is "public and state security (including economic security), defence, operational-search activities and criminal investigation"). Its effect is that Chapters II, III and IV of the Law (which deal respectively with the Rules on Processing of Data; the Rights and Obligations of a Data Processor and an Authorised Person;[2] and the Rights of a Data Subject – that is to say, the main substantive data protection rules) do not apply if "the matter is regulated otherwise" under certain specified other laws.

While it may be necessary to have special arrangements for dealing with the processing of personal data in these sensitive areas of public policy, it would be more transparent if those arrangements were set out on the face of the data protection law. Moreover, the words "the matter is regulated otherwise" are imprecise. More precision would be required.

It is recommended that this amendment be replaced by one that provides that Chapters II, III and IV of the DP Law do not apply if "the matter is expressly and specifically regulated in another Law".

Specific data protection rules of this kind must be drawn up for insertion in the Criminal Procedure Code (which will incorporate the OSA Law); and specific data protection rules must also be included in the law or laws covering the work of the Georgian Security Agencies.

Amendment 4

This amendment would further restrict the circumstances in which sensitive personal data may be processed. Article 6 of the Law currently prohibits the processing of such data except in the fields of activity which it specifies. The amendment would tighten that restriction by permitting the processing of sensitive data only in certain of those fields of activity and only with the written consent of the data subject.

If this amendment is made it will have a very serious effect on many legitimate activities. The processing of sensitive personal data is necessary for very many purposes: obtaining certain categories of insurance; assessing individuals entitlement to certain categories of benefit;

[2] The English version of the DP Law use the term "data processor" for the entity described in European data protection instruments (of Convention No. 108; EC Directive 95/46/EC; the draft EU General Data Protection Regulation; etc.) as "data controller". In those European instruments, a "data processor" is a body that carries out processing operations on behalf of the controller, i.e., a processing agent - what the English translation of the Georgian DP Law refers to as an "Authorized Person". It is strongly advisable to bring the terminology used in the Georgian DP Law, and in its translations, in line with the European terminology.

determining whether individuals have special dietary or other needs, for example when travelling by air. There are many other examples. The amendment would mean that sensitive data could no longer be processed for these purposes - even with the individuals' consent - since they are not among the fields of activity specified in the amendment.

Moreover, even in those fields of activity where it would still be possible to process sensitive personal data, it is difficult to see how the amendment can operate effectively and without causing serious problems. For example, in the employment field (which is one of those in which the processing of sensitive data would still be permitted) the data subject would have to give written permission any time for recording when he/she had been absent from work for health reasons. If consent was refused, no record could be made, with potentially serious consequences for the management of the establishment.

The amendment is also technically deficient. Paragraph 2(b) of Article 6 as in the proposed amendment requests for the processing of sensitive data the data subject's written consent where the "data subject is physically or legally incapable of giving his/her consent". Perhaps the word "or" has accidentally been omitted from the text or the translation, and the amendment should read) as follows: "Processing of data referred to in Paragraph 1 of this article shall be possible only with a written consent of the data subject, or in the following circumstances".

Amendment 6

Article 20 of the Law requires organisations processing personal data (referred to in the Law as "data processors")[3] to provide specified information to the Personal Data Protection Inspector before undertaking processing. Article 20(3) currently provides that organisations with 20 or fewer employees do not need to provide this information. This amendment would remove that provision, and thus require even the smallest organisations to provide the information.

A similar notification procedure is a requirement, with exceptions, of the EU Data Protection Directive. However, there is a view that the procedure is disproportionately bureaucratic when compared against the data protection benefits that it achieves. The proposals for new EU General Data Protection Regulation would abolish the notification requirement. This amendment goes against the trend within the EU. An alternative solution would be to make notification the exception rather than the rule, i.e. to list the types of sensitive processing which would need to be notified to the Personal Data Protection Inspector.

It is important that all data controllers are aware of, and consciously and meticulously review the details of their operations. It is recommended to require controllers to maintain a record with all these details, in relation to each specific, separate data processing operation; with a requirement to have this record available for inspection by the data protection authority in case there is an investigation or complaint.

Amendment 8

Article 24(1) of the Law sets out exemptions from certain of the Law's provisions relating to individuals' rights. Paragraph (d) provides an exemption to protect the important financial or economic interests of the country. This amendment would remove that exemption.

3.2 Proposed amendments to the e-Communications Law[4]

3.2.1 The Draft Law generally

[3] See footnote 2

[4] Draft of 9 September 2013

The Draft Law is an attempt at implementing provisions of the so-called EU Data Retention Directive into Georgian legislation. The EU Directive 2006/24/EC requires traffic data, location data and the related data necessary to identify the subscriber or user to be retained by "providers of publicly available electronic communications services or of a public communications network" for a period of 6 to 24 months.

The Directive proved to be controversial in the EU itself. Even before its adoption, it sparked vigorous debate as to its compatibility with human rights, particularly with the rights to privacy and personal data protection, as provided for in Article 8 of the European Convention of Human Rights (ECHR). The Article 29 Data Protection Working Party has concluded that "the mandatory retention of all types of data on every use of telecommunication services for public order purposes, under the conditions provided…, is not acceptable within the legal framework set in Art. 8 ECHR." The European Data Protection Supervisor (EDPS) has found "the simple reference to the existing legal framework on data protection" in the Commission proposal insufficient and called for additional legal safeguards.

The Directive was challenged in the European Court of Justice on the grounds of being adopted on an inappropriate legal basis, but survived. Afterwards, specific provisions of the implementing legislation were declared unconstitutional as violating the rights to privacy and data protection in several EU member states (Romania in 2009, Germany in 2010, The Czech Republic and Cyprus in 2011). Moreover, several similar cases are still pending in Poland, Slovenia and Slovakia, while in Hungary such case, initiated in 2008, failed only due to a change in the procedure of the Constitutional Court. Finally, in July 2012, the Irish High Court requested a preliminary ruling on the compatibility of the Data Retention Directive with fundamental rights to the CJEU. Similar requests from the Austrian Constitutional Court and the Austrian Data Protection Commissioner followed soon thereafter. At the time of writing, all the three cases were pending but the Opinion of the CJEUs Advocate General, Mr Cruz Villalón, concluded that the Data Retention Directive is incompatible with the Charter of Fundamental Rights.

Considering that the EU Directive is controversial and its future uncertain, the Georgian legislator may reconsider introducing a data retention scheme with the justification that "it is expedient that the legislation of Georgia becomes compliant with the 15 May 2006 EU Directive 2006/24/EC on the retention of data".[5]

3.2.2 New Paragraph 3 of Art. 8

The newly introduced paragraph 3 is almost a literal transposition of the Directive's Art. 5. The categories of data enumerated in the paragraph include data on communications traffic (data on the origin, destination, type and time of the communication), equipment used (telephone numbers, IMSI and IMEI codes) and its location (cell IDs and data identifying the cells' geographical location) and correspond to those mentioned in the Directive. The term of retention (1 year) is in conformity with the Directive as well.

Under the Directive, the retained data are provided only to the competent national authorities and in accordance with national law. It is up to the Member States to specify the procedures that have to be followed and the conditions to be fulfilled in order for the competent national authorities to gain access to retained data; these procedures and conditions have to be defined in accordance with the requirements of necessity and proportionality, in the light of ECHR as interpreted by the European Court of Human Rights (Art. 4). The proposed Chapter XVI[1] 'Computer Related Investigative Actions' of the CPC referred to in paragraph 3 provides for the procedures to be followed by an investigator to gain access to electronic evidence and appears to meet the requirements of necessity and proportionality.

[5] Explanatory Note on the Amendments to the Law of Georgia on "Electronic Communications".

However, under the Directive, the retained data are to be made available to law enforcement agencies for the purposes of investigation, detection and prosecution of "serious crime" (Art.1(1)). While the term is not defined in the Directive, the Council urged the EU member states to have due regard to the criminal offences listed in Art. 2(2) of the Framework Decision on the European Arrest Warrant and crime involving telecommunications when defining the scope of the national implementing legislation. At the same time, the scope of application of Chapter XVI[1] of the CPC is limited only to "deliberate" crime (Art. 143[2] para 1).

According to Art. 7 of the Directive, the providers must comply with four fundamental obligations related to the security of data retained by them:

- they must ensure that the retained data are of the same quality and subject to the same security measures and protections as other data on the network;
- the retained data must be subject to appropriate technical and organisational measures to protect them against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;
- appropriate technical and organisational measures must be taken in order to ensure that the retained data can only be accessed by specially authorised personnel; and
- all other retained data, except those that have been accessed and preserved, must be destroyed at the end of the retention period;
- moreover, the data must be retained in such a way that they, along with any other necessary information relating to such data, can be transmitted upon request to the competent authorities without undue delay (Art. 8). None of these requirements, however, are to be found in paragraph 3 or elsewhere in the Draft Law.

3.2.3 New Paragraph 4 of Art. 8

The paragraph establishes the duty of telecommunications providers to erase the data bearing the contents of communications immediately and automatically or, when it was provided to the competent authorities according to the procedures of Chapter XVI[1] of the Criminal Code, "without delay".

Since Georgia's current legislation does not provide for terms of storing content-bearing data strictly necessary for transmission purposes and the duty of telecommunications providers to erase such data when they are no longer needed for transmission or law enforcement purposes, the introduction of the new paragraph into Art. 8, even if merely reflecting the realities of the telecommunications business, is an important additional legal safeguard to the privacy of telecommunications in Georgia.

However, this amendment might be aimed, not at data retained under the proposed rules on the suspicionless retention of data on everyone under the previous amendment, but at the passing on of communication content to LEAs in the context of specific inquiries, on the basis of a specific judicial warrant, i.e., at traditional law enforcement tapping of communications.

If that is the case, the amendment as such may appear reasonable. However, there is an issue here, relating to ensuring the integrity of the captured communication content. It will be crucially important to the fairness and reliability of any criminal process that mechanisms are put in place to ensure:

- that communications content is only passed on to LEAs, or SISs, on the basis of a valid judicial authorisation;
- that this is recorded by both the LEA or SIS involved and, separately, by the Internet- or e-communications service provider served with the warrant (with the identity of the requesting authority, the judge and the provider, the time limit, etc.);

– that the data are provided (in copy, or recording, or by streaming) in such a way that that providing can be verified afterwards and, crucially, in such a way that an authentic record of the content is retained somewhere where it cannot be tampered with (e.g., in the form of a sealed copy).

The proposed amendment, requiring the erasure of the provider's copy of the data "without delay" after their communication to an LEA or SIS, may actually operate against such safeguards, as would "back doors" the use of which cannot be monitored by the providers.

A system for the interception of Internet activity or other e-communications must be fundamentally considered, both in terms of the laws and in terms of the technologies involved, and the required rules and technical mechanisms can only be properly created in the light of the findings of exhaustive inquiries.

3.2.4 New Sub-Paragraph 'p' of Paragraph 2 of Art. 11

The new sub-paragraph, whereby the Georgian National Telecommunications Commission is vested with powers to "[i]ntroduce control over the degree of privacy of information in the communications sector", should be seen as a generally positive development. Whether Georgia's telecommunications regulator is equipped to perform the new duties and able to effectively coordinate action with the Personal Data Protection Inspector, the national data protection authority, remains outside the scope of this assessment.

3.3 Proposed amendments to the Criminal Procedure Code & to the Law[6] on "Operational Search Activities"[7]

3.3.1 Draft Laws generally

The proposed amendments introduce a whole new category of procedural actions – "secret investigative actions"[8] – into the CPC and reinforce legal safeguards against abuse of investigatory powers exercised by law enforcement agencies under the OSA Law. The very fact that the legal rules on electronic surveillance are moved from a Law to a Code, a legal instrument of higher levels of authority and stability, should be welcomed.

Both Draft Laws considerably contribute to the transparency of surveillance activities in Georgia. These developments are in conformity with the case law of the European Court of Human Rights, according to which, regardless of the goal, no right envisaged in the ECHR can be interfered with unless a citizen knows the basis for the interference through an ascertainable national law. This requirement of transparency presupposes that the law is to be sufficiently clear and accessible to ensure that one could adequately determine with some degree of certainty when and how his or her rights get affected. The Court has found it "essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated".

3.3.2 New Chapter XVI[1] of the CPC

The measures to be brought under the CPC are the following:

"a) Wiretapping and recording of a telephone conversation;

[6] Drafts of 9 September 2013.

[7] In laws in other countries (in particular in various Criminal Procedure Codes of former Soviet countries), the kinds of measures covered by the OSA Law may be referred to as "special investigative measures", or similar.

[8] Terminology used in the English translation of the draft law.

b) Withdrawal and fixation of information from a communications channel (by connecting to the communications facilities, computer networks, linear communications and the station equipment), a computer system (as directly, as well as remotely), and the installation of respective software devices in a computer system for these purposes;
c) Control of a postal-telegraphic message/shipment (except for the diplomatic mail);
d) Secret video and audio recording, filmmaking and photography;
e) Electronic surveillance by technical facilities, use of which does not cause harm to a human life, health and environment."
(Article 143[1])

The lists of these measures in the two proposed laws include two limitations to the above: at the end of the third indent, the proposed text says "except for diplomatic mail"; and at the end of the last indent, the proposed text adds the words "[facilities], the use of which does not cause harm to a human life, health and environment".

These measures already, under the current OSA Law, require a judicial (the text says court) ruling, but the effect of their removal from that law is that they would be more clearly related to the framework of the CPC.

The CPC, according to its first article, regulates "the activities of Georgian criminal procedure agencies regarding the prosecution and trial of criminally punishable acts specified by the criminal law of Georgia as well as procedural issues raised during the execution of a court decision."

In principle, it is good that the secret surveillance measures currently covered by the OSA Law are moved to the CPC: as far as the use of such measures by LEAs is concerned, they should indeed be embedded in the main legal framework for the LEAs' activities, the CPC.

However, if this modification means that the use of such tools by other agencies, and in particular by the Georgian SIS(s), is left unregulated altogether, it should not be accepted. The Law with the proposed amendments to the OSA Law should indeed remove these measures from that law and move them to the CPC - but only insofar as the use of these tools by the LEAs is concerned. For the time being, and assuming that the Georgian SIS(s) are subject to the OSA at present, the rules in the OSA Law on those tools/measures should continue to apply to their use by non-LEAs.

As concerns the limitations: the first is intended to mean that secret surveillance measures may not be used (or at least not by LEAs, once these matters are brought under the CPC) against diplomatic mail. Under the Vienna Convention on Diplomatic Immunities, the exception should apply to all diplomatic communications. The inviolability of all diplomatic communications from the special surveillance measures should be much more clearly spelled out in the CPC. And whatever rules there are that apply to Georgia's SIS(s) should contain a similar, clear prohibition of this kind.

The second exception should be understood as intended to say that the "other" types of measures mentioned should not cause harm to a human life, health and environment. However, the way it is phrased now, the text can be read (at least in English) as meaning that these "other" secret measures are only subject to the restrictions in the new chapter if they do not cause such harm - but that such measures if they do cause harm are unregulated. It would thus be better to spell out this requirement of no harm in a separate sentence.

Although the definition of "secret investigative actions" is not provided in the proposed new chapter of the CPC, a formal-logical analysis of the two drafts leads to the conclusion that the newly created category of procedural actions are meant to be the "secret methods" of conducting "operational-search activities" mentioned in the definition of the latter in the OSA

Law (Art. 1 para 1) and essentially forms a type of lawful covert surveillance. Accordingly, the amended definition of "withdrawal of information from a communication channel" (Art. 1 para 'h'), along with the provisions on the procedure to be followed when wiretapping, secret video and audio recording and other forms of electronic surveillance are used (Art. 7 para 2 sub-paras 'h' and 'i', paras 3-5), were moved to the newly introduced Chapter XVI[1] of the CPC.

The lack of clarity in definitions described above can lead to doubts whether the "secret investigative actions" are, in fact, a form of the "operational-search activities" and, consequently, whether the reasonable suspicion test prescribed by the CPC's definition of "probable cause" (Art. 3 para 11) applies to this new category of procedural actions. To avoid doubt, it is advisable to make the CPC expressly specify that the reasonableness test is applicable to the procedures prescribed by the new Chapter, as is it was done in case of, for example, search and seizure procedures (Art. 119).

3.3.3 New strict rules

The partially new and partially tightened rules on the use of the relevant secret measures (by LEAs) include a set of principles, including that secret measures may only be used if the aim of the criminal investigation cannot be achieved by open investigative means; and that they can only be used against certain high public authorities or the media and religious organisations in certain very exceptional cases. Most importantly, they stipulate that (except for especially urgent cases) the measures must be applied for by a prosecutor in a reasoned motion; then assessed by a judge in an in camera hearing; and authorised by the judge only if s/he is satisfied that the requirements for such a measure are met, which are quite strict. They also stipulate a time-limit of two months, renewable once by a ruling by the same judge (or court?), and once more only upon a motion from the Chief Prosecutor of Georgia.

The above rules seem strict enough in principle, except that the two-month periods is considered to be rather long by the experts: a one-month period would be more appropriate, renewable once as envisaged, and possibly extendable for one month at a time to a maximum of six months in extremely exceptional cases, upon the motion of the Chief Prosecutor, by order of a Supreme Court Judge.

Various references in the text, and the very fact that the measures are to be moved to the CPC, strongly suggest that the measures will, under the CPC, only relate to investigations into (serious) crimes. However, there are a few references to such measures being necessary to "ensur[ing] national security or public safety, prevent disorder or commission of a crime, and protect the interests of the country's economic well-being or the rights and freedoms of other persons" - words clearly taken from the ECHR.

It should be clarified that the secret measures can only be taken under the CPC (i.e., under the new chapter in the CPC) if a specific (serious) crime has been committed, or if there is clear factual evidence that such a crime is about to be committed, or is clearly being planned. Of course, the crimes in question can be related to national security, or public safety, or may result in, or even be aimed at creating, public disorder. But the references to these wider interests should not lead to the secret measures being used by the Georgian LEAs in a non-criminal context, such as broader "intelligence" gathering. And as already repeatedly stressed, the use of such measures by the Georgian SIS(s) for wider, non-criminal "national security" purposes should be separately (strictly) regulated.

3.3.4 Guiding principles

Legal safeguards for human rights are significantly reinforced in both Draft Laws. Thus, both drafts contain identical provisions on the principles on which the conduct of the secret investigative actions and operational-search activities should be based. Under those provisions

(Art. 2 paras 1-3 of the OSA Law; Art. 143^2 paras 2, 3, 5 of the CPC), conducting a secret investigative action or an operational-search measure shall be possible only if it is:

- prescribed by law and necessary for achieving legitimate purposes in a democratic society – to ensure national security or public safety, prevent disorder or commission of a crime, and protect the interests of the country's economic well-being or the rights and freedoms of other persons;
- necessary in a democratic society, if pursuing it is caused by an urgent public need and if it represents an adequate and proportionate means for achieving a legitimate purpose;
- the scope of the action or measure and the data obtained from it is proportionate to a legitimate purpose of a secret investigative action.

Unfortunately, the additional safeguards of the OSA Law did not find their way into the CPC. The amended OSA Law (Art. 2 para 5), just like its old version, prohibits conducting an operational-search measure, if it:

- endangers human life, health, honor and dignity, the property;
- endangers the rights of a legal entity;
- is related to deceit, blackmail, agreeing by force, commission of a crime or other illegal action.

The legal basis for the amendments are easily identifiable: Art. 8 of the ECHR providing for the protection of privacy and stipulating the principles of legality, necessity and proportionality, as well as legitimacy, according to which this right can be limited. The Article reads:

> 8(1). Everyone has the right to respect for his private and family life, his home and his correspondence.
> 8(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.

When it comes to the principle of legitimacy, the Draft Laws go even further than what is required by the ECHR and do not envisage restrictions on the right to privacy for reasons of protecting health and morals.

Under the amended CPC, a secret investigative action can be conducted only when obtaining substantial evidence of crime through other means is impossible or involves "unjustifiably huge efforts" (Art. 143^2 para 4). Moreover, if other types of investigative actions "failed to achieve the set objective", they must be described in the prosecutor's motion for authorisation of a secret investigative action (Art. 143^3 para 3). This is in line with the European Court's case law, according to which covert surveillance should be a measure of last resort and consideration should be given to whether there is a less intrusive alternative to covert surveillance.

The new Article 143^6 of the CPC has significantly narrowed the circle of people who can be subjected to covert surveillance by obligating the authorities and their officers "to limit to a maximum extent the monitoring of communication and persons having no link with the investigation" (para 1). The CPC still does not provide for the exact categories of persons who can be subjected to covert surveillance. Such categories can be derived from either a precise description of the persons who can be put under covert surveillance or of the crimes they are allegedly linked to. The CPC provides both such descriptions, but both are too broad: while the respective crime is described as "deliberate", the respective persons are described as someone who "is directly or indirectly linked with the committed crime" (Art. 143^3 para 2 sub-paras 'a' and

'b'). The European Court has previously found a similar language of the Moldovan Operational Investigative Activities Act 1994 too broad and in violation of the ECHR.

Furthermore, Article 143^6 prohibits "[c]onducting a secret investigative action in respect of a cleric, attorney, doctor, journalist or a person enjoying the immunity" who acts in his or her professional capacity (para 2). This novelty can be only welcomed, for the need to secure exchanges of information falling under the attorney-client privilege, as reiterated by the European Court's case law, has been until now not reflected in Georgian law. Simply providing for the rule prohibiting interception of communications between an attorney and a client is not enough, however. Practical steps safeguarding the said communications are to be taken. The Dutch arrangement, for instance, whereby a representative of the bar association and the prosecutor are involved in screening the intercepted communications of attorneys with the view of telling protected information from unprotected one was approved by the Court.

Both drafts contain the norm, according to which the person subjected to a secretive investigation action or an operational-search measure must be notified about the fact of collecting information about him or her, the contents of that information and its fate, when such notification can no longer undermine legal proceedings (CPC Art. 143^9; OSA Law Art. 6 para 4). This notification requirement is in compliance with and even exceeds what is required by the Council of Europe Recommendation No. R (87) 15 stipulating that "[w]here data concerning an individual have been collected and stored without his knowledge, and unless the data are deleted, he should be informed, where practicable, that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced." The notification of the data subject is of extreme importance for achieving transparency and accountability of a surveillance measure and, in case of abuse, can become the first step on the road to redress, the right for which is guaranteed by both Draft Laws (CPC Art. 7 para 3; OSA Law Art. 6 para 2).

3.3.5 Transparency and accountability

The amended CPC (Art. 143^3 para 2) envisages the possibility of conducting a secret investigative action only in relation of a person "directly or indirectly linked" to a committed deliberate crime, only in cases of an urgent public need and only if it represents an adequate and proportionate means for achieving a legitimate purpose. The presence of these circumstances should be indicated in the prosecutor's motion and in the court ruling, which substantiates the lawfulness and soundness of the approval of the action (Art. 143^3 paras 5, 8 and 10).

A need to have relevant and sufficient reasons based on reliable information provided in support of a particular restrictive measure has been repeatedly emphasised in the European Court's jurisprudence. The reasons provided for a particular surveillance operation cannot be arbitrary, but are to be based on relevant considerations.

While an amendment to the OSA Law has removed the possibility of wiretapping without a court order envisaged in the old version of the Law (Art. 9 para 2), the new chapter of the CPC still allows secret investigative actions "in case of urgent necessity, when the delay may result in the destruction of substantial factual data for the case (investigation) or impossibility of obtaining such data" based on the "prosecutor's motivated resolution" alone (Art. 143^3 para 6).

Although the concept of hot pursuit as reflected in the new chapter of CPC is common, there must be sufficient safeguards against abuse of this exception to the general rule. In a decision on a case involving surveillance, the European Court of Human Rights has observed that "[o]ne of the fundamental principles of a democratic society is the rule of law which[…] implies, inter

alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control […]"[9].

Mechanisms for such control in the amended CPC are provided in the form of judicial oversight. In cases of secret investigative actions without a court order or in excess of what is allowed by the order, not later than in 12 hours from launching such action, the prosecutor must submit to the court a motion requesting the validation of the lawfulness of a secret investigative action. Further, in the motion, the prosecutor must justify the need for a secret investigative action and for conducting it without the judge's ruling or in excess of the scope of the ruling. The resulting court order must indicate the presence of the same circumstances and recognise as legal or illegal the secret investigative action conducted without court's authorisation. The information obtained in the course of an invalidated secret investigative action, as well as the data resulting from an action conducted without or in excess of a court order must be delivered for destruction (Art. 143^3 paras 7-9).

The duration of a secret investigative action is limited by the CPC to "the period necessary for fulfilling the objective of investigation, but not for more than two months" (Art. 143^3 para 12). Extensions by a court ruling are possible, but only twice: once upon a new motivated motion from the prosecutor and the second time for a maximum of two months on motion of the Chief Prosecutor of Georgia. While the said terms are longer than the one-month period recommended by the Supreme Court of Georgia, it is within the limits approved of the European Court in a number of cases.

3.3.6 Destruction of information

The proposed new articles contain extensive provisions on the compulsory destruction of information obtained as a result of secret measures, in particular of "materials obtained from an operational-search measure, which do not relate to a person's [alleged?] criminal activities but include information on his/her private life or of another person or persons".

They also lay down strict procedural rules:

> the material obtained from a secret investigative action is destructed by the prosecutor exercising procedural supervision on the investigation of this case or exercising state prosecution or their superior prosecutor, in the presence of that judge or the judge of that court, which had decided to conduct this secret investigative action or to recognize as legal or illegal a secret investigative action conducted due to urgent necessity without the judge's ruling or in excess of scope of the judge's ruling. The protocol on the destruction of material obtained from a secret investigative action, certified by signatures of the respective prosecutor and judge, shall be transferred to the Personal Data Protection Inspector and the Commission for destruction of information obtained from secret investigative actions and shall be reflected in the Register of Secret Investigative Actions.
>
> (Proposed Article 143^7(5))

The proposed rules on the compulsory destruction of information obtained by means of secret surveillance are clearly well-intended. The Commission to which all this is to be reported is very high-level and potentially powerful.

However it should be underlined that these proposed rules may not work. Most of the information obtained by secret surveillance will be in digital format: e-communications data (both content and meta-data), audio- and video-recordings, data captured by means of "trojans"

[9] ECHR, Klass & others v. Germany, 6 September 1978, paragraph 55

and other spyware from the targets' PCs or other devices such as mobile phones. Such data are easy to copy, at any stage and abuses of formal processes can occur.

It will be important for the Georgian authorities to examine ways to introduce technical means to ensure that data are captured and recordings are made in verifiable, tamper-proof ways, and that the captured data and the recordings are held in formats and ways that ensure that only three authorised copies are created: one for use by the authorities; one for the defence (electronically and physically sealed until it is handed over to the defence); and another, equally sealed copy, to ensure the evidence is not tampered with and to resolve disputes. Moreover, technical measures will have to be taken to ensure that no unauthorised copies (beyond these three authorised ones) can be made, and that any attempt to make an unauthorised copy is itself recorded. The proposed laws should expressly require that such technical measures are taken, and the authorities should obtain the best possible technical advice on how these things can be achieved, and report on their technical measures to the Commission, which itself should ensure it understands the technical problems.

The measures to ensure abuse no longer occurs should moreover be reinforced by strong dissuasive penalties for non-compliance with the new rules. If even the most trivial breach of the new, on-paper-strict rules were to carry serious penalties, like instant dismissal and criminal prosecution of law enforcement officials, that might have an effect - but even then, that effect would have to be shown in statistics on actual dismissals and prosecutions after a number of years.

One of the most vivid manifestations of both Draft Laws' novel approach is the detailed procedure for the destruction of information laid down by them. Under the amended CPC, the information obtained from a secret investigative action that is no longer of value for the criminal investigation must be destroyed by the prosecutor's decision immediately after the termination or completion of a secret investigative action. The information obtained from a secret investigative action, which was conducted without a court order or in excess of such order, provided the prosecutor has not moved before the court requesting recognition of these materials as legal, must be also immediately destroyed. Further, the information obtained from a secret investigative action, which was conducted due to an urgent necessity without the judge's ruling or in excess of scope of the ruling, and the court has rendered the ruling on recognition of this secret investigative action as illegal and the destruction of materials obtained from this action, must be also immediately destroyed (Art. 143^7 para 1 sub-para 1). In the new OSA law, the same rules apply to materials obtained as a result of operational-search activities that is not relevant to the investigated crime, but contains information on the suspect's private life (Art. 6 para 4).

Moreover, under the CPC, materials obtained from a secret investigative action that was considered inadmissible evidence by a court must be destroyed after 6 months from rendering a ruling on the case by the last court that heard the case. Prior to their destruction, such materials must be stored in a special storeroom of the court. Access to the said materials, copying them and/or using them by anyone is prohibited, except by the parties to the case in the course of exercising their procedural rights (Art. 143^7 para 1 sub-para 2). The new OSA law contains similar provisions (Art. 6 para 41).

Finally, according to the CPC, materials obtained from a secret investigative action and attached to the case as material evidence must be stored in the court for the period of retention prescribed for criminal cases. Immediately upon expiration of that term, the said materials must be destroyed (Art. 143^7 para 1 sub-para 3). The amended OSA Law provides for similar rules (Art. 6 para 42).

Regrettably, the law is still silent about the fate of personal data of third persons, i.e. those people against whom there is no reasonable suspicion that they are involved in criminal activities, but who were unfortunate enough to come into contact with the suspects.

Materials obtained from a secret investigative action is destroyed within the time limits described above by the prosecutor in the presence of the judge and notification of that fact by means of a protocol signed by them is made to the Commission for destruction of information obtained from secret investigative actions and the Personal Data Protection Inspector and has to be entered in the Register of Secret Investigative Actions (CPC Art. 143^{7} para 1 sub-para 3; OSA Law Art. 6 para 4). Such Register is to be set up in every court and the court is obliged to publish the information kept in the Register on an annual basis (CPC Art. 143^{10}).

Such degree of detail is hard to come by in a Law (statute) and usually can be found in pieces of secondary legislation (regulations). Such is the case in Ukraine, for instance, where the OSA Law (Art. 9 part 12) only provides for the general obligation to destroy private information irrelevant to the investigation and leaves the procedural details to secondary legislation. Given the Georgian experiences with the use of leaked personal data used for political purposes, however, such level of detailing statutory provisions can be seen as appropriate.

The level of detailed protection does not stop here. The new chapter of CPC envisages creating a ten-member commission to be put together by the Parliament and tasked with monitoring the destruction of materials obtained from investigative actions. The creation of an additional controlling organ might be complicating matters and burdening public spending too much, but again, is possibly justified under the current political situation in Georgia.

The resulting legal regime of collection, storage and destruction of the information obtained from a secret investigative action or an operational-search measure rules out the possibility of amassing and retaining information unaccounted for. What is more, such regime minimizes the possibility of illegal alteration and use of information related to the private life of a person suspected of being related to criminal activities and warrants that the information is safely retained throughout the period strictly necessary for carrying out a criminal investigation and achieving the legitimate purposes of the measures undertaken in respect of the person. Therefore, the regime created by the two Draft Laws is in compliance with Principles 2 (Collection of data), 4 (Use of data by the police), 7 (Length of storage and updating of data) and 8 (Data security), forming part of the basic principles that should guide the processing of personal data for police purposes according to Recommendation R (87) 15 of the Council of Europe.

Much remains to be done, however, in areas that present no less risk of abuse than non-destruction of data: sharing data among government agencies, data screening, matching and cross-referencing, as well as preserving their integrity and confidentiality during the storage period, i.e. the procedures followed between the obtaining and destruction of the data. These are the issues the Draft Laws are silent about, while their regulation in detail is required in light of the European Court of Human Rights case law.

3.3.7 Brief comments on more specific proposals.

Amendment 1

This amendment would extend the right to compensation for damages caused by the unlawful disclosure of information by the authorities (in particular, law enforcement authorities), to compensation for damages caused by the unlawful collection and/or storage of information, and clarifies that this includes these unlawful actions in relation to “personal data on [the victim’s] private life”.

This is in principle to be welcomed. It should be made clear (unless this is already clear within the overall system) that damages here include both actual pecuniary damages and non-pecuniary damages for distress, etc. It would be helpful to include the concept of exemplary damages in cases of particularly grave violations, and to introduce class actions for cases in which many people are affected.

Amendment 2

Based on the English translation provided, this amendment says:

> The court can restrict the right of the defense to receive information based on the motion of the prosecution only in the part of information obtained as a result of operational-search measures and the secret investigative actions, and only prior to a pre-trial hearing.

A better syntax for this sentence is required, showing what is meant in the context of Art. 83 CPC, may be the following:

> On the basis of a motion of the prosecution, and only prior to a pre-trial hearing, the court can restrict the right of the defense to receive part of any information obtained as a result of operational-search measures and secret investigative actions.

Moreover, it should at the very least be amended and clarified as follows (proposed changes and additions in bold):

> On the basis of a motion of the prosecution, **during the investigation stage of the proceedings**, the court can restrict the right of the defense to receive part of any information obtained as a result of operational-search measures and secret investigative actions. **However, once a person has been formally indicted, he and his defense lawyer should always be informed of the fact that evidence against him was obtained as a result of operational search measures; and before any actual pre-trial hearing, the defense should be provided with all the evidence obtained by such measures, including certified full copies of any such evidence.**

The issue addressed here is so important that it should require more fundamental re-thinking.

4 Conclusions and recommendations

The Parliament of Georgia is invited to review the present proposals in the light of the comments here above, before they are put forward for adoption.

While reviewing the amendment proposals, the following issues should be considered by the Parliament of Georgia:

1. Prior to any legislative action being taken, if one has not been carried out to date, an in-depth qualitative study of personal data handling by LEAs and SIS in Georgia should be carried out. If it has already been carried out then its contents, results and recommendations should be made available to the teams of local and international experts engaged to assist in the reforms of Georgia's applicable laws. This would enable drafters and policy-makers alike to take into account any issues, existing practices, local sensitivities or historical mistakes which are particular to the Georgian context. If at all possible and feasible it would also be desirable for such a study to take into account public perceptions of privacy in Georgia with a special focus on citizen attitudes to surveillance and personal data handling by LEAs and SIS;

2. Data protection rules for LEAs should be set out in detail in a separate detailed law, or in a detailed separate part of the general data protection law, or in a detailed data protection section in the CPC: no such detailed rules are included in the present proposals, but they could be set out in a subsidiary instrument. Specific data protection rules must also be included in the law or laws covering the work of the Georgian SIS(s);

3. Compliance with the Council of Europe's Rec(87)15 regulating the use of personal data in the police sector should be a key goal of the reform of the related laws . Although some elements of Rec(87)15 are now complied with in the latest proposals being considered, a systemic effort is required which should probably result in a distinct sub-set of data protection rules governing LEAs most probably as a detailed separate part of the general data protection law or regulations made in terms of enabling clauses in such a law;

4. In a country like Georgia where, for historical reasons, expertise in data protection law is limited, it would make sense to bring together oversight functions of all privacy and data protection matters in the hands of one agency provided that it is sufficiently resourced (cf. Austria and Luxembourg approach). Experiences of Data Protection Authorities of small countries where the DPA has competence and oversight over LEAs as well as all other data controllers suggests that this approach may have much to commend it thanks to the cross-fertilisation of understandings that takes place and indeed helps prevent insularity and insensitivity of both the LEAs and the DPAs. The extent to which separate oversight agencies undertake such competencies in larger countries has also been the subject of much debate and this can be easily avoided in a small country like Georgia where the culture of data protection is still being introduced at all levels in all sectors so separation and fragmentation which could be amplified through the creation of different oversight agencies for public/private entities, LEAs and SIS would not appear to be recommendable in a Georgian context. Thus the current proposal of independent oversight of secret surveillance measures by LEAs to be put in the hands of the PDP Inspector may be supported, solely provided that his or her office is adequately resourced (financially, technically & human resource-wise) to deal with such matters with such resourcing levels possibly being established and protected by law. The proposed very high-level and powerful data destruction oversight Commission would likewise only be able to exercise its functions if it is by law equipped to exercise day-to-day control; otherwise it would be unlikely to ensure destruction of incriminating information in practice. On the longer term and ideally, a special, technically competent and sufficiently resourced authority is needed. Whatever the oversight arrangements certain lacunae need to be addressed and specifically the absence of strongly dissuasive sanctions against officials (or politicians) who retain incriminating data in spite of the new rules;

5. Unlike the case of the EU Treaty, the Council of Europe's Convention 108 does not preclude from extending the protection granted in that Convention to the handling of personal data carried out by SIS. The precise form is actually relatively unimportant i.e. whether the handling of personal data by SIS is covered by a separate law or by a precise detailed sub-set of the general data protection law is a matter which should not be a casus belli. What is important is that such regulations are properly thought through and that they reflect modern technological realities where much personal data is not actually generated and retained by either LEAs or SIS but rather by commercial entities and citizens themselves and what LEAs and SIS wish to do is access and/or monitor/intercept personal data generated and retained by the private sector or elsewhere in the public sector. Given this convergence of data processing opportunities it is probably much more useful that the law consistently sets out the grounds where such data may be onward processed for compatible purposes and by

whom rather than attempt to regulate its processing in strictly compartmentalised pieces of legislation which follow a historical trend to regulate according to WHO processes the data rather than which data is actually processed and WHY;

6. Surveillance and smart surveillance are growth areas which are also seeing a blurring or lines between the public and the private sectors. In this case it is recommended that Georgia might follow closely and await the outcomes of the debates over these subjects which may be expected to take place over the next 24-48 months and then act accordingly taking all reasonable precautions should it decide to be an "early adopter" for any of the new legislative and other policy measures currently being considered;

7. The time factor is also important, subject to the outcome and findings of the in-depth study recommended in 1 above, and taking account of the international debate on the subject, the most urgent needs in terms of legal framework, resources and other matters should be identified and agreed;

8. Considering that the EU Directive is controversial and its future uncertain, the Georgian legislator may reconsider introducing a data retention scheme with the justification that "it is expedient that the legislation of Georgia becomes compliant with the 15 May 2006 EU Directive 2006/24/EC on the retention of data";

9. Further consideration is proposed as regards to specific amendments to the DP Law, on the lines suggested previously and most particularly:

   a. define the categories of persons who can be subjected to secret investigative actions and the categories of crimes that can give rise to such measures;
   b. prescribe procedure for destruction of third parties' data being collected as a result of the secret investigative actions;
   c. specify that the reasonable suspicion test of CPC Article 3 paragraph 11 is applicable to the secret investigative actions under the CPC's new Chapter XVI[1];
   d. provide for in a Law detailed rules that will safeguard the inviolability of communications under the attorney-client privilege and the separation of data obtained from lawful interception of such communications from the data collected as a result of interception of attorneys' communication in personal capacity;
   e. Crucial technical arrangements are required to ensure that no unauthorised recordings or copies of recordings of data are made (which is a serious technical challenge).

And finally, the wider review of surveillance for national security purposes should be linked to, and informed, by reforms currently considered in other countries in the wake of the reports on mass surveillance, taking due account of international agreements signed by Georgia.