Funded by the European Union and the Council of Europe
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Implemented by the Council of Europe
Continued support to the criminal justice reform in Ukraine
MINISTRY OF FOREIGN AFFAIRS OF DENMARK
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

DGI(2016)19
3 November 2016

OPINION
OF THE DIRECTORATE GENERAL HUMAN RIGHTS AND RULE OF LAW OF THE COUNCIL OF EUROPE

ON THE DRAFT LAW OF UKRAINE NO. 4778 ON DETECTIVE OPERATIONS

Prepared on the basis of the expertise by:
Brian Chappell, Ralph Roche, Sarah Shirazyan and Eric Svanidze

Table of contents

1. Executive Summary

1.1 This opinion concerns the draft Law of Ukraine No. 4778 on Detective Operations, which is intended to increase the effectiveness of the relevant agencies to conduct detective operations and ensure compliance with European standards.

1.2 There is a wide range of European standards of relevance to the draft Law, in particular concerning secret surveillance and data protection. Secret surveillance raises significant issues of compliance, with a strong focus on procedural safeguards. Recent technological advances pose new challenges in securing the right to respect for private life and in ensuring that any processing of personal data is conducted properly and for a clearly-defined purpose. The opinion sets out the most relevant of these standards in detail.

1.3 The draft Law is comprehensive in terms of meeting the challenge of providing enabling legislation for those responsible for protecting national (State) security, investigating and prosecuting serious and organised crime and other offences designated by the State of Ukraine. It provides for a wide range of covert and overt investigative tactics and provides an authorisation and accountability framework.

1.4 However, there are a number of shortcomings and gaps in this framework, which should be remedied to ensure compliance with European standards and the requirements of the Criminal Procedure Code (CPC) of Ukraine. A number of recommendations envisaged in the opinion are aimed primarily at increasing the level of procedural safeguards in the draft Law (in particular as regards judicial control and oversight) and by developing guidance for the use of specific powers, including publicly-available information where possible.

1.5 Examples of some of the recommendations include setting out clearly the basis for the initiation of detective operations and specifying the types of crimes they can be deployed against, ensuring ex post facto notification of persons subject to secret surveillance, aligning the draft Law with the CPC requirements concerning prosecutorial and judicial oversight, the threshold of apprehension, the entry of information in the Unified Register of Pre-trial Investigations, etc. Furthermore, the draft Law should apply similar definitions of various terms as set out in the CPC in order to ensure consistency and prevent misuse of the powers contained in it. There are also a number of issues in the draft Law which would benefit from clarification, for example the circumstances in which Covert Human Intelligence Sources can be used.

1.6 Another set of recommendations deals with the compliance with European data protection standards and protecting the rights of children.

1.7 Whilst the draft Law is concise and has the utility to provide law enforcement and security agencies with a coherent legal framework to support their activity for the aforementioned reasons, it is suggested there are a number of areas that could be developed and more comprehensively covered drawing on similar legislation.

1.8 The successful implementation of the recommendations contained in the opinion would ensure that the goal of giving effect to European standards is more satisfactorily achieved and would improve the draft Law further with a view to providing a firm basis for the lawful and effective use of detective operations by the relevant bodies in Ukraine.

2. Introduction

2.1 This opinion is concerned with the draft Law of Ukraine No. 4778 on Detective Operations[1] ("the draft Law"), the adoption of which is being considered by the Verkhovna Rada of Ukraine.

2.2 The stated purpose of the draft Law is to reduce bureaucracy and enable the relevant operational units to be more effective in their ability to investigate crime, whilst ensuring compliance with human rights standards.[2] The Explanatory Note to the draft Law ("the Explanatory Note") states that it is intended "to improve the legal principles for conducting detective operations, bring it in line with the European standards applicable to the activity related to temporary restriction of human rights and freedoms, synchronize detective operations and procedural activity carried out in accordance with the provisions of the Criminal Procedure Code of Ukraine ("CPC"). According to the Explanatory Note, this is required as a result of a number of factors:

- The current Law of Ukraine "On Detective Operations" was enacted in 1992, at a time when Ukraine was not a member of the Council of Europe or a signatory to the European Convention on Human Rights ("the Convention");

- The adoption of the new CPC of Ukraine in 2013 has caused a number of practical issues in the implementation of operative search activities. These include the requirement under Article 214 of the CPC to register all reports of actual or suspected criminal offences in the Integrated Register of Pre-Trial Investigations within 24 hours of their receipt;

- The creation of new law enforcement agencies such as the National Anti-Corruption Bureau of Ukraine and the State Investigation Bureau has created a need for consistency regarding the authorization and conduct of operative search activities across different agencies.

2.3 The present opinion reviews the compliance of the draft Law with European standards and, in particular, with the requirements of the Convention and its Protocols as interpreted and applied by the European Court of Human Rights ("the ECtHR"). The analysis underlying this opinion examines the conceptual approach of the draft Law and its likely impact upon the criminal justice system. It also examines the coherence of the draft Law with the recent reforms of the Ukrainian CPC.

2.4 The opinion is prepared under the auspices of the Council of Europe's Project "Continued Support to the Criminal Justice Reform in Ukraine" funded by the Danish government and the European Union/Council of Europe PCF Project "Strengthening the implementation of the European human rights standards in Ukraine". The comments are based on the English translation of the Ukrainian text of the draft Law.[3]

2.5 The draft was reviewed by the following Council of Europe consultants:

Brian Chappell is currently an independent criminal justice consultant and part time senior lecturer at the University of Portsmouth, Institute of Criminal Justice Studies, where he has taught at both

[1] The title of the current Law is generally translated into English as the Law of Ukraine in Operative-Search Activities. The draft Law, despite having the same title in the original Ukrainian version, is translated as the draft Law of Ukraine on Detective Operations. Therefore, this Opinion uses the term "Detective Operations" throughout.

[2] Explanatory Note to the draft Law - August 2016.

3 The translation has been carried out within the framework of the Projects "Continued Support to the Criminal Justice Reform in Ukraine" funded by the Danish government and the European Union/Council of Europe PCF Project "Strengthening the implementation of the European human rights standards in Ukraine".

undergraduate and post graduate level. His specialisms include criminal investigation; intelligence; organised crime; ethics, leadership and management in intelligence and investigations. Previously, he completed a thirty-year career with the Metropolitan Police Service, New Scotland Yard, where he was a senior detective and operational head within the Specialist Crime Directorate. He has operational and management experience of all aspects of proactive investigation, intelligence development, analysis and related specialist training to police departments, overseas law enforcement and external agencies. This also includes national and international strategic experience in the development of best practice and human rights compliance in relation to covert policing. He has also led capability building projects for a number of international law enforcement agencies. He holds a Doctorate of Criminal Justice (DCrimJ) from the University of Portsmouth and a MA in Intelligence and Security Studies from Brunel University.

Ralph Roche has studied at Trinity College Dublin, University College Dublin and Queen's University Belfast. He is a solicitor, admitted in Northern Ireland and in England and Wales. He has long experience as a human rights lawyer, including as a Senior International Lawyer at the Human Rights Chamber for Bosnia and Herzegovina, and at the Independent Judicial Commission in Bosnia and Herzegovina, which implemented a comprehensive programme of judicial reform. He has a number of publications, including *The European Convention on Human Rights and Policing* (jointly with Prof. Jim Murdoch), published by the Council of Europe in 2013. He has devised and delivered training to investigators of the Ministry of Interior of Ukraine, including the programme "Human rights guarantees at the pre-trial stage of criminal proceedings", held in Kiev in 2014.

Sarah Shirazyan is an international lawyer, specializing in civil liberties, data protection and national security. Sarah serves as a Council of Europe consultant developing curricula on European human rights standards for data privacy and data protection in the framework of the project HELP in the 28. Previously she served as a Drafting Lawyer for the European Court of Human Rights; worked on issues of nuclear security at the United Nations Secretariat; and handled international drug investigations at INTERPOL Secretariat. Sarah is currently pursuing her Doctor of Juridical Sciences (J.S.D.) degree at Stanford Law School. At Stanford, Sarah co-teaches classes on American Foreign Policy and Democracy and Social Entrepreneurship. Prior to Stanford, Sarah designed and taught graduate courses on International Human Rights Law and Public International Law at the Yerevan State University, Armenia. She also worked as a Staff Attorney at the American Bar Association Rule of Law Initiative implementing criminal justice reform projects in Armenia.

Eric Svanidze is an international lawyer/expert, Council of Europe consultant/ former prosecutor in Georgia, deputy minister of justice, member/expert of the European Committee for the Prevention of Torture, member of the Council of Europe group of consultants providing expertise of the new Ukrainian CPC, Law on the Public Prosecution Service (including relevant opinion of the Venice Commission), State Bureau of Investigation and other related legislative acts. He holds the LL.M. in Human Rights Law from University of Lund, Sweden. Currently he leads the EU Project on Justice Monitoring in Armenia.

3. Relevant European standards

Introduction

3.1 The purpose of this chapter is to set out briefly some of the main European standards concerning secret surveillance and data protection.[4]

3.2 European countries face a range of different threats to the security of their citizens. In order to protect those within their jurisdiction, it is necessary that their law enforcement and intelligence agencies are granted the powers necessary to enable them to be effective. In certain situations, law enforcement agencies are under a duty to take investigative or protective actions, and any failure to do so may result in a failure to comply with the State's positive or procedural obligations under Article 2 of the Convention.[5]

3.3 "Secret surveillance" includes powers of interception of communications, covert searches and other powers that are included in the draft Law. The term, as used by the ECtHR, includes the observation and recording of a person's movements, the use of hidden listening devices and the interception of communications.[6]

3.4 Recent years have seen rapid and continuing technological advances in the field of secret surveillance, including facial recognition and bulk data collection and analysis. The ECtHR has noted "the extent to which intrusions into private life are made possible by new, more and more sophisticated technologies."[7] The CoE Parliamentary Assembly has noted with concern the emergence of a "massive "surveillance-industrial complex""[8] which threatens human rights across Europe.

3.5 Secret surveillance is by its very nature open to arbitrariness and abuse and the ECtHR has identified the "risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it".[9] There are frequent instances throughout European history of secret surveillance being misused by authoritarian regimes to abuse the human rights of those within their jurisdiction. The case-law of the ECtHR is influenced by this, in particular through the vigilance and scrutiny it exercises over the practical implementation of secret surveillance measures.[10] The Committee of Ministers of the Council of Europe has warned that mass surveillance "capabilities and practices can have a chilling effect on citizen participation in social, cultural and political life and, in the longer term, could have damaging effects on democracy."[11]

---

[4] The term "secret surveillance" is used by the European Court of Human Rights and is used throughout this Opinion.
[5] See, for example, Murdoch and Roche, *The European Convention on Human Rights and Policing*, Council of Europe, 2013, at page 64.
[6] Harris, O'Boyle and Warbrick, *Law of the European Convention on Human Rights*, 3rd edition, OUP 2014 at page 555.
[7] *Köpke v. Germany*, decision of 5 October 2010, Application No. 420/07.
[8] Resolution 2045 (2015) "*Mass Surveillance*" available at http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692&lang=en
[9] *Roman Zakharov v. Russia,* judgment (Grand Chamber) of 4 December 2015, Application No. 47143/06, at paragraph 232.
[10] See, e.g. *Kopp v. Switzerland*, judgment of 25 March 1998, Application No. 23224/94.
[11] Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies *(Adopted by the Committee of Ministers on 11 June 2013 at the 1173rd meeting of the Ministers' Deputies)*

3.6 A rapidly developing area of law concerns the retention, storage and sharing of information obtained by means of secret surveillance. This area is dealt with in the parts of this opinion concerned with the compliance with data protection standards.

Right to respect for private life

3.7 The exercise of powers of secret surveillance in relation to an individual or members of a group will invariably result in an interference with their right to respect for private life, as guaranteed by Article 8 of the Convention. In the field of investigations covered by the draft Law, it is often necessary that the person under investigation is unaware that their communications or other aspects of their private life are being monitored. As a result, as noted by the ECtHR, "especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident".[12] This reinforces the need for clear and accessible rules setting out the circumstances in which a person's communications may be intercepted, or other secret surveillance tactic used in relation to them.[13]

3.8 The retention and storage of any information on a permanent record is an interference with the right to respect for private life and therefore requires justification.[14]

3.9 The Parliamentary Assembly of the Council of Europe has stated that "a legal framework must be put in place at the national and international levels which ensures the protection of human rights, especially the protection of the right to privacy."[15]

"In accordance with the law"

3.10 The ECtHR has held that, in order for any interference with the right to respect for private life to be justified, it must be "in accordance with the law". This "requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus meet quality requirements: it must be accessible to the person concerned and foreseeable as to its effects".[16] This is not a requirement that an individual be able to "pinpoint exactly when the police were likely to be listening in on their conversations" as "this would defeat the purpose of secret surveillance."[17] However, "domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures."[18]

3.11 In a number of countries, the legislation governing secret surveillance is supplemented by administrative acts such as Internal Rulebooks issued by the relevant Ministry, or a Code of Practice. In the United Kingdom, a number of publicly-available Codes of Practice contain information on issues such as authorization levels and procedures for different types of secret surveillance, and provide significant amounts of detail regarding the types of situations where they may be authorized. The ECtHR has held that this renders the domestic law adequately accessible.[19] While decisions of

[12] *Ibid.* at paragraph 229.
[13] *Malone v. United Kingdom*, judgment of 2 August 1984, Application No. 8691/79.
[14] *Rotaru v. Romania*, judgment of 4 May 2000 (Grand Chamber), Application No. 28341/95.
[15] Resolution 2045 (2015) "Mass Surveillance" available at http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692&lang=en
[16] *Roman Zakharov v. Russia*, judgment (Grand Chamber) of 4 December 2015, Application No. 47143/06 at paragraph 228.
[17] Jacobs, White and Ovey, *The European Convention on Human Rights*, 6th ed., Oxford University Press, 2014, at page 371.
[18] *Šantare and Labaznikovs v. Latvia*, judgment of 31 March 2016, Application No. 34148/07, at paragraph 53.
[19] *R.E. v. United Kingdom*, judgment of 27 October 2015, Application No. 62498/11, at paragraph 121.

Constitutional, Supreme and other courts may interpret and apply primary legal provisions, they should not dilute or undermine legal protections in those provisions. For example, jurisprudence of the Croatian courts which effectively removed the legal requirement for prior approval of secret surveillance was found by the ECtHR to result in a violation of Article 8 of the Convention.[20]

3.12 Another key aspect of the requirement for secret surveillance measures to be "in accordance with the law" is the existence of adequate safeguards against abuse.[21] In order to meet this requirement, the law must be sufficiently clear in its terms to give people an adequate indication of the circumstances and conditions in which secret surveillance may be conducted. A very clear example of a lack of adequate safeguards against abuse is highlighted in the judgment of the ECtHR in the case *Malone v. United Kingdom*.[22] This case concerned interception of communications. The Court held that the "obscurity and uncertainty as to the state of the law"[23], in particular the discretion afforded to Government Ministers, meant that the applicable provisions were not "in accordance with the law" in Convention terms.

3.13 The degree of safeguards required will, to an extent, depend on the level of intrusiveness of different operative search activities. For example, the deployment of a vehicle tracking device, which records the movements of a vehicle, is less intrusive than the recording of conversations inside a vehicle as it does not disclose information on a person's opinions, conduct or feelings.[24] By contrast the deployment of an undercover agent wearing recording equipment in private property was "virtually identical" to telephone interception, in terms of the level of interference with privacy.[25]

Legitimate aim

3.14 If secret surveillance is provided for by a law which meets the standards of legality and necessity, and if it is authorized and conducted in accordance with that law, the next question is to assess whether it is in pursuance of a legitimate aim. Examples of legitimate aims include the prevention of crime, the protection of public safety and the protection of the rights and freedoms of others. However, intrusive investigative tactics should only be available in relation to serious crimes. The ECtHR has, for example, criticized the availability of telephone interception in relation to the offence of pickpocketing.[26] In addition, any discretion afforded to law enforcement authorities must not be unduly broad. For example, an emergency procedure in the Russian Operational-Search Activities Act of 12 August 2005 on which afforded "the authorities an unlimited degree of discretion in determining in which situations it is justified to use",[27] it meant that there was no effective judicial oversight of that procedure. In a case concerning France, the ECtHR held that the lack of definition of the types of offences that could result in telephone interception resulted in a violation of Article 8 of the Convention.[28]

Oversight of the exercise of secret surveillance powers

3.15 A fundamental element of the procedural safeguards required is independent scrutiny of secret surveillance. This is required in order to ensure "that there are adequate and effective

[20] *Dragojević v. Croatia*, judgment of 15 January 2015, Application No. 68955/11, at paragraphs 94-102.
[21] *Klass v. Germany*, judgment of 6 September 1978, Application No. 5029/71, at paragraph 50.
[22] *Ibid.*
[23] *Ibid*. at paragraph 79.
[24] *Uzun v. Germany*, judgment of 2 September 2010, Application No. 35623/05, at paragraph 52.
[25] *Bykov v. Russia*, judgment of 10 March 2009, Application No. 4378/02, at paragraph 79.
[26] *Roman Zakharov v. Russia*, judgment of 4 December 2015, Application No. 47143/06, at paragraph 244.
[27] *Ibid.* at paragraph 266.
[28] *Huvig v. France*, judgment of 24 April 1990, Application No. 11105/84.

guarantees against abuse"[29] by the authorities. The precise nature of how this is conducted is not decided by the ECtHR. In particular, scrutiny may take place "when the surveillance is first ordered, while it is being carried out, or after it has been terminated".[30]

3.16 The ECtHR is primarily concerned with the qualitative nature of the oversight system. In most countries with a civil law system, such as Ukraine, authorization of particularly intrusive forms of secret surveillance are carried out by an independent judicial or quasi-judicial figure. This may be an investigating judge or a prosecutor. Countries with a common law legal system, such as the United Kingdom and Cyprus, tend to have internal authorization with external oversight by independent bodies. In *Kennedy v. United Kingdom*, the ECtHR examined the role of the Interception of Communications Commissioner. The Commissioner is appointed in accordance with domestic law and examines the compliance of warrants for the interception of communications with the applicable law.[31] While warrants for interception are authorized by a Government Minister, the ECtHR held that "the Commissioner's role in ensuring that the (domestic law is) observed and applied correctly is of particular value and his biannual review of a random selection of specific cases in which interception has been authorized provides an important control of the activities of the intercepting agencies…"[32]

3.17 One of the primary methods of ensuring oversight of secret surveillance is subsequent notification to the person or persons who have been the subject of it. In a recent case against Hungary, the ECtHR held that "(a)s soon as notification can be carried out without jeopardizing the purpose of the restriction after the termination of the surveillance measure, information should be provided to the persons concerned".[33] Accordingly, while subsequent notification is not an absolute requirement, any failure to provide it requires strong justification, for example a potential compromise of the identity of an informant. This is because any failure to do so limits greatly the ability of those affected to seek judicial review of the surveillance.

3.18 The ECtHR will look at the effectiveness of oversight mechanisms, and not just at the legal basis for their existence. It is important that such mechanisms are adequately resourced and institutionally capable of exercising their competencies and mandate. The relevant legal provisions must ensure that it has access to all documents necessary for the oversight mechanism to verify that the applicable conditions for authorizing secret surveillance are fulfilled.[34] The Court found a violation of this requirement in the Russian Operational-Search Activities Act of 12 August 2005 and the Code of Criminal Procedure of 18 December 2001, as they did not require the authorizing judge to be provided with information concerning the involvement of undercover agents or the details of operational-search tactics.[35] In addition, the lack of a requirement to verify that there are reasonable grounds to suspect the commission of a crime by those subjected to the secret surveillance was criticized.[36] Details regarding the activities of oversight mechanisms should be published[37], with due regard for the need to protect confidential information.

Data Protection

[29] *Roman Zakharov v. Russia*, judgment of 4 December 2015, Application No. 47143/06, at paragraph 232.
[30] *Ibid*., at paragraph 233.
[31] The Regulation of Investigatory Powers Act 2000. Replacement legislation, the Investigatory Power Bill, is at an advanced stage of preparation.
[32] *Kennedy v. United Kingdom*, judgment of 18 May 2010, Application No. 26839/05 at paragraph 166.
[33] *Szabó and Vissy v. Hungary*, judgment of 12 January 2016, Application No. 37138/14, at paragraph 86.
[34] *Ibid.*
[35] *Roman Zakharov v. Russia*, judgment of 4 December 2015, Application No. 47143/06, at paragraphs 257 to 267.
[36] *Ibid.*
[37] *Kennedy v. United Kingdom*, judgment of 18 May 2010, Application No. 26839/05 at paragraph 166; *Roman Zakharov v. Russia*, judgment of 4 December 2015, Application No. 47143/06, at paragraph 283.

3.19 The key European legal instruments in the field of data privacy and data protection guide this opinion. It draws upon the Convention, including as interpreted by the jurisprudence of the ECtHR; 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. Reference is made where appropriate to relevant European Union standards, such as the EU 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; Council Framework Decision 2008/977/JHA;[38] ePrivacy Directive 2002/58/EC, Data Retention Directive 2006/24/EC,[39] 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 2006/24/EC; and the CJEU judgments of *Digital Rights Ireland et. al* and *Schrems* cases.[40]

3.20 The jurisprudence of the ECtHR and relevant Council of Europe standards concerning data protection set out a wide range of clearly accessible and practical standards to which the draft Law must adhere. The ECtHR has recognized that the collection, storage, access or use and dissemination of personal data for purposes (e.g. national security or intelligence) other than those it was originally transferred for, can only be justified when it is "strictly necessary in a democratic society." The ECtHR has set "minimum safeguards against abuse" of these fundamental human rights. The "minimum safeguards that according to the Court should be set out in statute law in order to avoid abuses of power" relate to the following:[41]

- The nature of the offences in relation to which surveillance may be ordered;
- The definition of the categories of people who are liable to be placed under surveillance;

[38] The Framework Decision 2008/977/JHA guarantees a number of principles of data protection and these principles are only applicable to the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. The Recommendation No. R(87)15, however, has a broader scope and provides a specific and more complete set of rules.

[39] The Data Retention Directive has now been declared null and void. Marin, Luisa. "The fate of the Data Retention Directive: about mass surveillance and fundamental rights in the EU legal order." Research Handbook on EU Criminal Law, Forthcoming (2015).

[40] At the time of drafting this opinion, the EU's Data Protection Reform Package was finalized resulting in the adoption of the General Data Protection Regulation 2016/679; Directive 2016/680, governing the handling of data in law enforcement situations; and the Passenger Name Record Directive (Directive 2016/68). Despite the fact that Ukraine is not a EU member, these legislative changes are likely to pose implications beyond the boundaries of the EU member states. While the principal secondary EU law instrument on data protection still remains Data Protection Directive (95/46/EC), the General Data Protection Regulation (GDPR) will replace this directive soon. The new GDPR will be effective from May 2018 and will be directly applicable in all EU Member States without further need of national implementation. The data protection reform package also introduced EU Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (commonly referred as "Police Directive"). The Police Directive will repeal Council Framework Decision 2008/977/JHA.

[41] *Weber and Saravia v. Germany*, decision of 29 June 2006, Application No. 54934/00. In other cases, the ECtHR has reiterated that account must be taken of all relevant circumstances, including the nature, scope and duration of possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the remedies provided by national law (*Kennedy v. the United Kingdom*, judgment of 18 Amy 2010, Application No. 26839/05; see also *Shimovolos v. Russia*, judgment of 21 June 2011, Application No. 30194/09), CJEU, Schrems, §91. *See also* Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, Patrick Breyer, European Law Journal, Vol. 11, No. 3, May 2005, pp. 365-375. Internet: Case Law of The European Court of Human Rights, June 2015, http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf.

- The limits on the duration of the surveillance;
- The procedure to be followed for ordering the examination, use and storage of the data obtained; these "should be set out in a form which is open to public scrutiny and knowledge";
- The precautions to be taken when communicating the data to other parties; and
- The circumstances in which the intercept data may or must be erased or destroyed.[42]

3.21 In order to understand the scope and the limits of handling of personal data in law enforcement situations, it is necessary to ascertain the general data protection rules of Ukraine, specifically by looking at the Law on Protection of Personal Data (referred as Data Protection Law). An issue of particular importance is to ensure that Ukrainian general data protection law mirrors the key foundational principles of European data protection law, such as data must be (a) obtained and processed fairly and lawfully; (b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes; (c) adequate, relevant and not excessive in relation to the purposes for which they are stored; (d) accurate and, where necessary, kept up to date; [and] (e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.[43] This is because these principles are the basis of processing of personal data and are generally relevant for data handling in law enforcement context too.[44]

3.22 Key European essential safeguards to handling personal data in law enforcement context are summarized below:

Safeguards	**Characteristics:**
1. Safeguards related to data collection in law enforcement context.	- Lawfulness of processing, including strict purpose/use limitation of collected data/data minimization,[45] and limits on further processing; - Fairness of processing; - Informing data subject; - Processing special categories of data (sensitive/non sensitive data); differentiation of data subjects (e.g. processing of data related to non-suspects; and children).

[42] Korff, Douwe. "Expert Opinion prepared for the Committee of Inquiry of the Bundestag into the „5EYES" global surveillance systems revealed by Edward Snowden, Deutscher Bundestag, 1." Untersuchungsausschuss der 18 (2014).

[43] Tourkochoriti, Ioanna. "The Transatlantic Flow of Data and the National Security Exception in the European Data Privacy Regulation: In Search for Legal Protection Against Surveillance." University of Pennsylvania Journal of International Law 36 (2014): 459-524.

[44] The CJEU in its landmark judgment on the data retention directive has articulated that processing which entail a limitation on the fundamental rights of the individuals must be carried out in full compliance with core principles of data protection and any restrictions must be exceptional and narrowly construed. *See* judgment in Digital Rights Ireland and Others, C-293/12 and C-594/12, paragraph 52.

[45] As the CJEU has recently reiterated in its Schrems judgment and in Digital Rights Ireland and Others judgment, interferences in the private life of individuals and in the right to protection of personal data shall be limited to what is strictly necessary and proportionate to the objectives of general interest foreseen, i.e. the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

2. Safeguards related to control and notification: Data controllers and processors' obligations.	- Role and Power of Supervisory Authorities (the supervisory authorities powers should be independent and responsible to, and be appointed by, parliament rather than the Executive); - Prior consultation of the supervisor authority; - Notification to supervisory authority, including notification on manual and ad hoc files; - Privacy Impact Assessments; Logging or other reasonable measures; - Security of data processing, data breach notifications.
3. Safeguards related to Data Subjects Rights.	- Information to data subject; - Right of access for the data subject and limitations to the right of access; - Right to rectification/erasure; - Right to object; - Right to lodge a complaint; appeal to supervisory authority.
4. Safeguards related to communication and transfers of personal data to other public and private bodies, third countries or international organizations.	- A strict purpose limitation of transfers only for the prevention, investigation, detection or prosecution of specific criminal offences or the execution of criminal penalties in the framework of a specific investigation/procedure; - Prohibition of massive, repeated and structured transfers of personal data to third countries; - Restrictive interpretations of exceptions; - Documentation of transfers; - Requirements of an adequate level of protection when transferring personal data to third countries (Shrems v. Data Protection Commissioner judgment).
5. Safeguards for storage of data and length of the storage.	- Data quality principle; - Accuracy and reliability (distinction between fact based and opinion-based data); - Administrative data (shall not be subject to rules applicable to police); - Strict rules/procedures on the destruction/erasure of intercepted data.

4. General Considerations

4.1 The draft Law is comprehensive in terms of meeting the challenge of providing enabling legislation for those responsible for protecting national (State) security, investigating and prosecuting serious and organised crime and other offences designated by the State of Ukraine. It provides for a full range of covert and overt investigative tactics that can be utilised to conduct proactive criminal and intelligence-led investigations, and provides an authorisation and accountability framework. There are some comments set out below in the opinion regarding gaps in this framework, which could be remedied by ensuring that the equivalent provisions in the CPC are applicable to detective operations conducted under the draft Law. This would bring Ukraine into line with other countries across Europe and facilitate compliance with the human rights requirements set out in the Convention as interpreted by the ECtHR.

4.2 Whilst the draft law is concise and has the utility to provide law enforcement and security agencies with a coherent legal framework to support their activity for the aforementioned reasons, it is suggested there are a number of areas that could be developed and more comprehensively covered drawing on similar legislation. An example of a positive approach towards public information can be seen in the United Kingdom, where publicly available Codes of Practice outline the full range of covert activity available to the law enforcement and intelligence and security agencies.[46] These Codes go into some detail regarding individual tactics and have been favourably commented upon in a number of cases decided by the ECtHR.[47]

4.3 Before analysing the draft Law in detail, it is appropriate to recall that the recently-adopted CPC represents a departure from the repetitive and cumbersome Soviet-era criminal procedure, which involved three stages. In particular, the Code abolished the concept of a 'pre-investigative inquiry', which preceded the formal criminal (pre-trial) investigation stage. The third stage was comprised of the trial and any appeals. In practice, pre-investigative inquires consisted of operative verification activities, and were carried out by a broad range of law-enforcement agencies and officials. The existence of such a wide range of authorities with what amounted to investigative powers undermined the independence and lawfulness of the pre-trial process, the effectiveness of fair trial and other guarantees, and the criminal justice system in general.

4.4 The previous system of diffusion of powers to operative subdivisions and officers led to wide-spread abuse of those powers, and facilitated corrupt practices. It also resulted in human rights violations that are reflected, *inter alia*, in the significant number of ECtHR judgments against Ukraine. These include unofficial detention, reliance on appropriate grounds for deprivation of liberty and its continuance;[48] torture, ill-treatment, often combined with the use of improper methods

[46] Regulation of Investigatory Powers Act 2000 (UK) including Part 3 Police Act 1997 https://www.gov.uk/government/collections/ripa-codes

[47] See for example *Kennedy v. United Kingdom*, judgment of 18 May 2010, Application No. 26839/05.

[48] E.g., *Osypenko v. Ukraine*, judgment of 9 November 2011, Application No. 4634/04; *Doronin v. Ukraine*, judgment of 19 February 2009, Application No. 16505/02; *Garkavyy v. Ukraine*, judgment of 18 February 2010, Application No. 25978/07; *Ichin and Others v. Ukraine*, judgment of 21 December 2010, Applicaton Nos. 28189/04 and 28192/04; *Kornev and Karpenko v. Ukraine* and *Nechiporuk* and *Yonkalo v. Ukraine*, judgment of 21 April 2011, Application No. 42310/04.

of gathering evidence;[49] insufficient legal framework and procedure for the use of secret surveillance[50] as well as other human rights violations.

4.5 It is accordingly appropriate that the CPC has abolished the requirement to take a formal decision on whether or not to initiate a criminal investigation. Instead, it requires that the commencement of criminal investigations be registered in the Integrated Register of Pre-Trial Investigations. In addition, the CPC requires that all criminal investigations, and those involved in conducting them, adhere to a comprehensive and coherent framework which ensures appropriate procedural safeguards, including judicial oversight and the involvement of suspects and other affected persons. The CPC has further improved compliance with the Convention through implementing elements of an adversarial procedure to all stages of ongoing criminal proceedings. Examples are the exclusion of evidence obtained in violation of provisions of the CPC from any trial and the prohibition of unauthorised involvement of members of 'operative units' in the criminal process.

4.6 It is worthy of note that both domestic and international monitoring mechanisms indicate that the CPC has resulted in positive changes, including in terms of reducing ill-treatment and other serious human rights violations.[51]

4.7 Any reform of this magnitude will inevitably involve difficulties during the implementation phase, and the current one is no exception. The new CPC requires a paradigm shift in attitudes among stakeholders, in particular law enforcement agencies and the prosecution.

4.8 Allied to this, the CPC sets the threshold for the commencement of pre-trial investigations at a relatively low level ("circumstances which are likely to indicate that a criminal offence has been committed")[52] and establishes a framework for the role and mandate of various operative units.[53] The CPC has thereby reconciled the principle of mandatory prosecution with the need for those units to have an appropriate level of involvement and competence. This is reflective of best practice in other jurisdictions, where there is scope for detective operations to gather intelligence in order to support criminal prosecutions, with the prosecutor leading. In situations where secret surveillance has been focused primarily on gathering intelligence, this has frequently resulted in a failure to focus on ensuring the rule of law through the application of the criminal law to hold those who commit crimes accountable.[54]

4.9 Accordingly, it is not conceptually correct to state that criminal proceedings have become paralysed 'because detective officers have been unreasonably deprived of independence in decision-making related to taking any measures in criminal proceedings'. Detective officers have unique and

[49] E.g. *Afanasev v. Ukraine*, judgment of 5 April 2005, Application No. 38722/02; *Vergelskyy v. Ukraine*, judgment of 12 March 2009, Application No. 19312/06; *Khaylo v. Ukraine*, judgment of 12 November 2008, Application No. 39964/02; *Mikhalkova v. Ukraine*, judgment of 13 January 2011, Application No. 10919/05; *Nechiporuk and Yonkalo v. Ukraine*, judgment of 21 April 2011, Application No. 42310/04.

[50] E.g. *Mikhalyuk and Petrov v. Ukraine*, judgment of 10 December 2009, Application No. 11932/02; *Vladimir Polischuk and Svetlana Polischuk v. Ukraine*, judgment of 30 September 2010, Application No. 12451/04.

[51] See, *inter alia*, the Report to the Ukrainian Government on the visit to Ukraine carried out by the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT) from 9 to 21 October 2013 (CPT/Inf (2014) 15. Report on an evaluation of the implementation of the Criminal Procedure Code of Ukraine, February 2015, prepared as part of the Project "Support to Criminal Justice Reform in Ukraine.

[52] Article 214 of the CPC.

[53] Article 41 of the CPC.

[54] See, for example, Organisation for Security and Co-operation in Europe, Human Rights in Counter-Terrorism Investigations: A Practical Manual for Law Enforcement Officers, Warsaw, 2013 at pages 46 to 49.

specialist skills, which should be utilized to suggest investigative and other opportunities to investigators and prosecutors. This division of competencies in the CPC has been rightly reinforced by the Law on Prosecution and recent amendments to Article 131[1] of the Constitution.

4.10 The recent constitutional and legal amendments demonstrate that Ukraine has implemented a system whereby undercover/detective operations conducted by law-enforcement agencies are subject to prosecutorial supervision. While there is a role for the conduct of detective operations to develop intelligence (particularly in the sphere of national security), the initiation of criminal investigations in accordance with the requirements of Article 214 of the CPC should always be a clear focus.

4.11 While this requirement is reflected in the draft Law to an extent, it is not laid down in a sufficiently strict manner and thus leaves scope for detective/operative officers to seek to undermine it. For example, Article 12 paragraph 2 of the draft Law refers to the fulfilment by detective units of "inquiries of competent state authorities, institutions and organisations regarding detective measures". Article 39 paragraphs 3 and 4 allow for the taking of emergency measures in certain cases ("if they receive information that crimes have been committed"). These exceptions are very broadly formulated and could allow state authorities, etc., to order the conduct of detective measures in a very broad set of circumstances and potentially to circumvent the requirements of Article 214 of the CPC. In addition, they do not set any temporal limits on measures, which is a significant omission due to the potential duration of complex detective activities. These measures should be explicitly subjugated to the general applicability of Article 214 of the CPC, in order to prevent abuse.

Recommendation 1: It is recommended that Article 12 paragraph 3 and Article 39 paragraphs 3 and 4 are specifically subjugated to the requirement in Article 214 of the CPC concerning the entry of information about actual or likely crimes within a 24-hour period. In addition, the conduct of any detective operations beyond that period should be prohibited without approval as required for the specific operation as set out in the draft Law. Finally, the conduct of any unauthorised activities by detective officers should be expressly prohibited and provision made for specific procedures for obtaining instructions from the investigative authority or prosecutor, to be issued in accordance with Article 41 of the CPC.[55]

4.12 Throughout the draft Law, various terms such as "suspicion" and other terms which are defined terms in the CPC are used, but are not defined in the draft Law. This could lead to confusion as to the relationship between the terms in the context of the draft Law and the CPC.

Recommendation 2: In order to reduce the scope for confusion as to the meaning of a number of terms used both in the draft Law and in the CPC, it would be advisable for them to be given the same definition in both laws.

4.13 The draft Law envisages a significant role for detective functions, across a range of law enforcement and other agencies. Their role is expanded considerably, in comparison to the current Law on Detective Operations from 1992. For example, they are to play a leading role in performing intelligence-specific, preventive and other related functions. They have a range of competencies, including proposing measures on the policy level, to establishing the existence of sufficient grounds for the use of certain tactics against individuals, as well as the practical use of detective activities in

[55] As to detention of perpetrators, the detectives are entitled to it under the CPC framework established in its Articles 207-213. See also para. 21 of the current opinion below.

specific cases. This approach is consistent with the European Union's conception of a proactive and intelligence-led approach towards ensuring the Union's internal security.[56]

4.14 Many of the provisions of the draft Law echo the overt and covert investigative actions provided for in the CPC, in particular in terms of the powers and competencies granted to the relevant law enforcement agencies and detective units within them.

4.15 However, there is a lacuna in the draft Law in terms of procedural safeguards. The CPC contains a carefully calibrated set of procedural safeguards and guarantees, which can ensure compliance with relevant Convention standards.[57] The draft Law, in contrast, lacks distinctions in terms of the conduct of various forms of secret surveillance in public and private places (the latter being more intrusive), a definition of "home", as well as other special conditions that overt or covert detective activities must comply with in order to ensure compliance with the human rights of those affected by them. This is of significant importance due to the sheer breadth of detective activities which are provided for under the draft Law, and the lack of a specific statement in it that detective operations may be carried out solely in compliance with the authorisation and oversight provisions provided for in the CPC. Article 31 of the draft Law does state that "Judicial control over detective operations shall be exercised in the manner prescribed by provisions of the Criminal Procedure Code of Ukraine applicable to covert investigative (search) measures." However, it is considered that this requirement should be spelt out in more detail, with exact references to the relevant provisions of the CPC, in order to ensure full compliance with the requirements of the CPC.

4.16 The effect of this lacuna is that there is a significant risk of detective operations carried out under the draft Law resulting in violations of human rights of those who are subject to them.

Recommendation 3: the draft Law should contain a specific and explicit requirement that the same level of procedural safeguards as are set out in the CPC, in particular prosecutorial and judicial oversight, is incorporated into the draft Law.

4.17 The draft Law does not provide specifically that persons who have been the subject of covert detective operations should be notified, where it is possible to do so. This (as set out at paragraph 3.17 above) is a key procedural safeguard in terms of ensuring judicial oversight of secret surveillance and its importance is stressed by the ECtHR.

Recommendation 4: the draft Law should provide, in terms analogous to those set out in Articles 253 and 254 of the CPC, that once detective operations are concluded those affected by them should be notified where it is possible to do so.

4.18 The thresholds for detention of persons in Article 10 paragraph 6 sub-paragraph 2 and Article 39 paragraph 3 are not consistent with the applicable provisions of the CPC (Article 207) or sufficiently high to ensure compliance with Article 5 of the Convention, as they do not require reasonable grounds that person has committed an offence or is attempting to commit an offence. While it is appropriate for persons to be apprehended in the course of detective operations if there is a pressing need to do so, the threshold must be the same as for apprehension in other circumstances.

[56] See The Stockholm Programme — An open and secure Europe serving and protecting citizens, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52010XG0504(01) and related EU acquis. See also 'Internal security strategy for the European Union Towards a European security model', European Union, 2010, p. 22.
[57] Which are dealt with in more detail at section 3 above.

Recommendation 5: the thresholds for apprehension in Article 10 paragraph 6 sub-paragraph 2 and Article 39 paragraph 3 should be harmonised with Article 207 of the CPC.

4.19 One of the operations envisaged by the draft Law is the "inspection of financial-economic activity of companies" (Article 10 paragraph 2 sub-paragraph 19). The original text of the draft Law uses the formulation that such powers include an "organisation of examination", which connotes the exercise of some general audit, inspection or oversight powers. While there may be a need for the inspection of financial statements in the course of specific investigations or operations, it should be made clear that the draft Law does not create some form of general power to inspect such records as part of a general review or oversight function. The granting of such powers to the majority of detective agencies, without regard to their substantive jurisdiction, and with inconsistency as to the need for prior judicial authorisation,[58] could be regarded as the equivalent of some form of general supervision.[59]

4.20 The scope for such powers to be abused is high. The legitimate interest in ensuring financial probity in businesses can be ensured through overt measures such as the publication of accounts, audit functions and inspection mechanisms by the competent authorities. Certain other bodies, such as the State Audit Service and the National Commission for Securities and Stock Market, may have relevant competencies in appropriate cases.

Recommendation 6: The draft Law should follow the approach[60] adopted in the CPC and require that inspections of companies, as provided for in Article 10 paragraph 2 sub-paragraph 19, can only be done in the course of individual overt or covert investigative activities.

4.21 In order to ensure legal clarity, avoid jurisdictional conflicts between different agencies and between detective and investigative operations and also to reduce the scope for improper conduct of detective operations, the grounds for conducting detective operations must be set out with great clarity. Article 9 of the draft Law is drafted quite broadly, in particular in terms of the conduct of detective measures targeted against the preparation of crimes. It would be advisable that the draft Law states that, if a crime has been committed (*corpus delicti*), whether consummated or unconsummated,[61] any further actions should be of an investigative nature, conducted under the applicable provisions of the CPC.

4.22 Article 9 paragraph 1 states that sufficient information for the conduct of detective operations includes information concerning "persons fleeing from the pre-trial investigation authorities, investigating judge or court, or evading serving criminal sentence". The procedural status of such persons should require to be clarified in each instance as such persons are likely to be subject to measures of restraint imposed under the CPC. Failure to comply with measures of restraint would provide a specific legal basis for the conduct of investigative actions.

[58] According to para. 4 of Article 10 it is not subject to judicial authorisation and s/para. 3 of para.1 of Article 13 suggests that a request, review, examine and retrieve of any documents and data that characterise the operation of enterprises, institutions and organisations is subject to approval by investigating judge.
[59] See paras. 17, 25, 26 Joint Venice Commission and Directorate General of Human Rights 2013 Opinion on the Draft Law on the Public Prosecutor's Office of Ukraine and preceding assessments of the (draft) legal framework on the PPO of Ukraine, CDL (2013)039.
[60] Articles 36, 40 and 93 of the CPC.
[61] As defined in Article 13 of the Criminal Code of Ukraine.

Recommendation 7: It would be advisable that Article 9 of the draft Law states that, if a crime has been committed (*corpus delicti*), whether consummated or unconsummated,[62] or where specific measures of restraint have not been complied with, any further actions should be of an investigative nature, conducted under the applicable provisions of the CPC.

4.23 The wording of grounds for conducting detective operations, as set out in Article 9 paragraph 1 sub-paragraphs 3 and 4, concerning the "need to obtain intelligence information for the benefit of public and state security" and "generalised materials of the central executive authority" are unduly wide.

4.24 The ground in sub-paragraph 3 should incorporate a stipulation as to the legitimate interest and necessity requiring the obtaining of such information. The Convention, as interpreted by the ECtHR, recognises the pre-eminent importance of protecting national (State) security[63] and the fight against serious crime and terrorism.[64] However, these cannot be used as a blanket justification for secret surveillance; individual justification is required.

4.25 While in the case of detective operations concerning national security, a specific crime is not necessary to be suspected, in respect of sub-paragraph 4, it is necessary that there be sufficient grounds to suspect that there are individual acts involving or potentially involving criminal activities concerned with individual or systemic acts of money-laundering or financing of terrorism, etc.

Recommendation 8: Article 9 paragraph 1 sub-paragraph 3 should require that a basis for the specific detective action is present. Sub-paragraph 4 should require that there are sufficient grounds to suspect that there are individual acts involving or potentially involving criminal activities concerned with individual or systemic acts of money-laundering or financing of terrorism, etc.

4.26 Article 10 paragraph 2 sub-paragraphs 20, 21 and 22 refer to "preventive detective measure", "detective recognition" and "signals intelligence" respectively. These terms should be defined more specifically, as the present definitions are very broad and refer to categories of detective operations, rather than specific detective operations.

Recommendation 9: The terms contained in Article 10 paragraph 2 sub-paragraphs 20, 21 and 22 should be defined more specifically.

4.27 The draft Law envisages unduly broad conditions and grounds permitting the conduct of detective operations prior to obtaining the appropriate authorisation. This is in contrast to the current Law, which incorporates the requirements of Chapter 21 of the CPC for this issue. As a result, instead of adhering to the established framework (with its emphasis on the need for urgency, involvement of the prosecutor, immediate judicial supervision and other important procedural safeguards), the draft Law (at Article 10 paragraphs 5 and 6) simply makes a general reference to "other laws". It does not incorporate the procedural safeguards contained in the established framework. This is despite the fact that detective operations are arguably more intrusive and open to abuse than pre-trial investigations. The effect of this is that the relevant provisions of the draft Law are highly likely to result in violations of the requirements of the Convention.

[62] As defined in Article 13 of the Criminal Code of Ukraine.
[63] See, for example, *Nolan and K. v. Russia*, judgment of 12 February 2009, Application No. 2512/04).
[64] See, for example, *Uzun v. Germany*, judgment of 2 September 2010, Application No. 35623/05.

4.28 Accordingly, the draft Law should specifically incorporate the provisions of Article 250 of the CPC, either directly or by specific reference to the requirements of that Article. This would impose appropriate limitations on the conduct of intrusive detective operations prior to obtaining a court warrant.

Recommendation 10: The draft Law should specifically incorporate the provisions of Article 250 of the CPC, either directly or by specific reference to the requirements of that Article.

4.29 Similar considerations apply as regards the lack of a defined framework for the registration of files containing information obtained during detective operations. It is possible for detective operations to be conducted and not registered. This is as a result of Article 16 of the draft Law, which has the effect that there is no requirement to register information obtained by way of actions conducted under, e.g., Article 10 paragraph 2 sub-paragraph 19 ("inspection of financial-economic activities of companies") and the following sub-paragraphs of that Article. The lack of a requirement to register detective operations is a significant failing in terms of ensuring accountability and facilitating oversight.

Recommendation 11: the draft Law should require that all detective operations are registered appropriately, including a requirement that all information related to them, including information obtained, is included.

4.30 The draft Law, both as currently drafted, and if a subsequent draft incorporates the recommendations in this opinion, will necessitate amendments to various other pieces of legislation, in particular the CPC. Accordingly, it should include a table of amendments to other legislation.

Recommendation 12: the draft Law should include a table setting out the amendments to other legislation which it would require.

4.31 On a practical drafting point, a number of Articles have only one paragraph and therefore it is not necessary to number that paragraph. Examples of where this occurs in the English-language version are Articles 4, 17, 25, 27, 28 and 35.4.32

4.32 From a data protection perspective, the draft Law contains positive aspects that correspond to European standards and references certain safeguards when carrying detective operations including subjecting the covert operations to judicial supervision. For example:

i. Article 8 defines the units conducting detective operations; Article 10 lists the specific detective measures and provides a detailed procedure for filing a motion to conduct the detective operations (motion requires substantiating that all other means of collecting data about alleged criminal activity have been exhausted). Article 11 spells out the bodies and the respective offences for which detective measures can be conducted. Article 42 provides details on classification and de-classification of detective materials. Section 6 of the proposed law sets multi-layered oversight mechanism over detective operations.
ii. Yet, the proposed law raises concerns as regards to its compliance with data protection standards. These concerns are discussed further below in respect of each Article.

4.33 When surveying the Ukrainian Data Protection law and draft Law on Detective Operations, it seems the activities of Law Enforcement Authorities ("LEAs") (or the handling of personal data

processing in the context of law enforcement more generally) are not subject to general Data Protection Law. Unless already provided by other legislation, Ukraine does not have a separate data protection law specifically addressing personal data handling by LEAs. The current draft Law does not comprehensively address data protection issues in the context of crime prevention and investigation.

Recommendation 13: the draft law should address data protection aspects within law enforcement context more systematically (e.g. by introducing a detailed sub-section or adopting a specific data protection law covering LEAs).

5. Article – by – Article comments

Glossary of Terms and Definitions

5.1 The section in the draft Law entitled "Terms and Definitions" is an important innovation, in comparison with the current Law.

5.2 Care should be taken to ensure that definitions are used consistently throughout the entire draft Law. For example, 'Audio surveillance of a person' – it is not specified whether this means telephone interception ("telephone tapping"), as well as other audio recording devices which facilitate eavesdropping (probes). There is also an entry for 'Phone surveillance' and 'Correspondence surveillance', which appears to concern telephone and mail interception. In general terms, telephone interception is considered to be a particularly intrusive tactic, while eavesdropping is considered to be slightly less intrusive (depending on where it occurs). For example, covertly recording a person's conversation in a public area, while an interference with their right to respect for privacy, is far less intrusive than covertly recording a person's telephone conversation or covertly recording their conversation in their home. The exact nature of what is included in the definition of "audio surveillance of a person" should be included. If it is not, it is difficult to ensure that proportionality concerns are met. The ECtHR has stated that domestic laws must set out in detail what is envisaged by different legal provisions, and unduly broad definitions are unacceptable.

Recommendation 14: The definition of "audio surveillance of a person" in the draft Law should distinguish between the various forms of audio surveillance it permits, in particular between the use of eavesdropping devices and telephone interception, and should also distinguish between actions depending on the location in which they occur.

5.3 'Confidential co-operation' appears, although a little vague, to relate to the use of Confidential Informants/agents or Covert Human Intelligence Sources (CHIS). CHIS is a term that has been adopted within law enforcement and more commonly used when using English within the European law enforcement community. It may be worth considering whether this term, appropriately translated, could be used in the draft Law and more generally. In addition, the definition does not deal with juveniles. There are circumstances where a juvenile may be authorised as a CHIS. However, these circumstances should be extremely rare and would require very careful scrutiny and oversight. The best interests of the juvenile should be the primary concern in such an authorisation, as required by Article 3 of the United Nations Convention on the Rights of the Child. It may be more appropriate to have a specific provision in the draft Law dealing with the issue of juveniles generally, rather than specifically in relation to the issue of CHIS.

Recommendation 15: The draft Law should make specific reference to the fact that any actions related to juveniles should have as their primary aim the protection of the best interests of the child.

5.4 'Polygraph Testing' in terms of the necessity and proportionality for polygraph testing; it is unclear what the grounds are for this tactic to be used, notwithstanding the arguments relating to the credibility of the tactic. In addition, there is no explanation of the necessity required for the use of the tactic, and the technicalities of how it would be used in practice. It is suggested that more detail is required to explain this.

Recommendation 16: the draft Law should either incorporate further regulations governing the use of polygraph testing, or a specific reference to the relevant legislation.

5.5 The draft Law introduces a concept of detective experiment. It seems that this could be a result of a mechanical transfer and technical adjustment of the CPC provisions as to investigative experiment. The essence of the latter is that it is purely of evidential value and concerns the reconstruction of circumstances and events. It is not clear what are the circumstances in which it would be necessary and possible to apply the same concept in the operative search activities. If the concept of "detective experiment" implies a staged act which could act as a trigger in the course of detective operations and will be a part of an overall strategy to gather information, then it is unclear how it differs from the other activities (e.g. "detective purchase", etc.), which are already listed in the draft Law in a comprehensive manner. This needs to be clarified.

5.6 The term "Covert entry into and examination of publicly inaccessible places, dwelling premises or other private property" is defined twice. This should be addressed in order to avoid potential confusion.

5.7 The use of 'necessity' and 'proportionality' should be considered and included where applicable within the text e.g. 'necessary' rather than 'important'. The concept of necessity is of fundamental importance in terms of demonstrating a pressing requirement for an action and thus serves to provide a legal basis in Convention terms, as it is a requirement that the State take some action to protect the interests of those affected (e.g. victims). The use of the term "necessary" would provide consistency with the terms used in similar legislation within Europe. In addition, the case-law of the ECtHR uses these terms frequently and it would be of significant assistance in ensuring and explaining the basis and justification for detective operations if these terms were used.

Article 2

5.8 In general, secret surveillance should only be used in relation to crimes of a sufficient degree of seriousness.[65] While Article 10 paragraph 4 of the draft Law limits the use of the measures set out in sub-paragraphs 1 to 11 of Article 10 paragraph 2 to serious crimes, the other measures in paragraph 2 are not limited to such crimes. Allowing their use for crimes that do not reach the required level of seriousness could raise issues of compliance with the Convention.[66]

5.9 Furthermore, the objective, set out in paragraph 2 of Article 2, of obtaining information on any offences other than criminal offences, detecting of which would contribute to combating crime, is inconsistent with and expands the grounds for detective operations, which are defined in Article 9.

Recommendation 17: Consideration should be given to the removal of Article 2 paragraph 2.

5.10 The scope of Article 2 paragraph 3 is not specific enough and may give rise to broad interpretations by authorities. "Obtaining information on any facts and circumstances that do not bear characteristics of a criminal offence, yet require verification," does not appear to be linked to the

[65] For example, in the UK, certain intrusive tactics are limited to serious crimes, which is defined in section 93(4) of the Police Act 1997 as:

"Conduct which:

(a) involves the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose; or

(b) the offence or one of the offences is an offence for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more."

[66] *Roman Zakharov v. Russia*, judgment of 4 December 2015, Application No. 47143/06, at paragraph 244.

notion of criminal offence, is imprecise and may lead to processing of personal data in the widest context of law enforcement.

5.11 Furthermore, according to the entire provisions of the Draft *"the instances of obtaining information on any facts and circumstances that do not bear characteristics of a criminal offence, however, must be verified according to the applicable laws of Ukraine"* (mentioned in paragraph 3) are limited only to a) searching for missing persons already mentioned in the Article in issue and b) checks of individuals in connection with their access to state secrecies and work with nuclear materials and at nuclear facilities (envisaged by sub-paragraph 2 of paragraph 1 of Article 9). In order to prevent any extensive interpretation and unauthorised application of detective activities, it would be necessary to amend it (paragraph 3) so that it provides for an exhaustive set of such instances.

Recommendation 18: The scope of Article 2 paragraph 3 should be reviewed in order to prevent any extensive interpretation and unauthorised application of detective activities, as well as to ensure that it does not allow for the processing of personal data in an unduly broad set of circumstances.

Article 4

5.12 The construction of the provision outlining the principle of proportionality defined as 'relevance and adequacy of the detective measures used to the level of public threat carried by the criminal activity' could be improved and aligned to the wording suggested by Article 8 paragraph 2 of the Convention.

Recommendation 19: In order to ensure coherence with the Convention and the case-law of the ECtHR, Article 4 of the draft Law should include as a principle of detective operations *necessity in a democratic society and interests of national security, public safety, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms.* This should be adopted also in Article 6 paragraph 2.

Article 5

5.13 Article 5 paragraph 2 could be interpreted as a general-purpose limitation clause that allows processing of the personal data only in situations when it is explicitly provided for by the draft Law. This should be welcomed. Purpose limitation is one of the fundamental data protection principles aimed at setting limits in which personal data collected for a specific reason may be further processed for a different purpose. Principle 4 of Council of Europe Recommendation No. (87)15[67] also states this in the following terms: "[...] personal data collected and stored by the police for police purposes should be used exclusively for those purposes". While reference to purpose limitation is positive, the draft Law seems not to address the requirement for distinguishing between different categories of data (specific data or specific categories of data subjects).

5.14 From a purpose limitation perspective, there must be strict rules on when data can be disclosed and further shared between different LEAs (e.g. Article 37, as well as Article 12 paragraphs 2 and 3). While it is important to have inter-agency coordination and cooperation for swift criminal investigation, there must be adequate safeguards to protect against personal data violations. Data collected for a specific crime may also be used by competent authorities for solving another crime provided that compatibility is assessed on a case-by-case basis and subject to a

[67] "Regulating the Use of Personal Data in the Police Sector"

specific legal basis. Principle 5 of Recommendation No.(87)15 offers guidance on communicating the intercepted data.

Article 6

5.15 One important aspect of detective operations is ensuring that all of the foreseeable risks are managed. For example, CHIS or other persons who assist police may be putting themselves at serious risk of harm. In order to manage this risk, appropriate action must be required in terms of the planning and control of detective operations.

5.16 It is likely that any detective action will involve the collection of information. In many cases, information which is not directly relevant to the action may be gathered. This can be considered to be collateral intrusion, e.g. the gathering of information regarding persons with whom the target(s) of a detective action has contact but who are not suspected of any involvement in any wrongdoing. The draft Law should make provision for managing such information.

Recommendation 20: The draft Law should make provision for the management of information collected during the course of detective operations which concerns persons who are not suspected of involvement in any wrongdoing.

5.17 In addition, it is suggested that more emphasis is given on the record keeping of those applications and subsequent authorities, including any review mechanisms, to ensure accountability provisions are fully met. The maintenance of comprehensive records of detective operations is a key method of ensuring accountability through judicial oversight.

5.18 Paragraph 2 of Article 6 incorporates a further application of the principle of proportionality. The definition which is recommended to be adopted in Article 4 above (see recommendation 19 above) should also apply to this Article.

5.19 The provision in paragraph 2 for compensation is welcome. However, there may be circumstances in which a judicial remedy is required, for example in order to ensure appropriate oversight or if the person affected does not consider that any compensation offered is adequate in the circumstances. This remedy should be in addition to that provided for in paragraph 4, which relates to cases where a public prosecutor or judge becomes aware of infringements of human rights.

Recommendation 21: there should be provision in Article 6 paragraph 2 for a judicial remedy regarding compensation in appropriate cases.

5.20 Article 6 paragraph 3 seems to raise issues from a human rights and data protection point of view, especially as regards to the data subject's right to be informed (e.g. person subjected to surveillance). Principle 2.2 of Recommendation No.(87)15[68] recognizes the data subject's right to be informed, especially when the data collection took place without his/her knowledge. While Article 6 paragraph 3 allows individuals to request explanations from respective authorities about restrictions on their rights, there does not appear to be a corresponding obligation or duty on part of the authorities to inform persons about detective measures. While it is important not to endanger national

[68] Principle 2.2 Where 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.

security and criminal investigations, the right to be informed has direct effect on the right to an effective remedy. Therefore, there should be a mechanism for user notification, even after the measures are no longer in place, so that the data subject can exercise its right to an effective remedy at least *ex post facto*.[69]

5.21 Article 11 paragraphs 5 and 6 and Article 15 paragraph 6 concern the maintenance of state secrets regarding detective operations. While this is a legitimate interest, it is necessary to reconcile it with the data subject's right to be able to exercise his or her right to a remedy.

5.22 The recent case of *Roman Zakharov* is relevant in this context and highlights the relationship between the right to be informed and the right to effective remedy. The Court held that "[t]here is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively or, in the alternative, unless any person who suspects that his or her communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications."[70] Further detail regarding this issue is set out at paragraph 3.17 above.

Recommendation 22: Article 6 paragraph 3 should prescribe the exact manner in which the right to be informed of having been subject to detective operations is to be realised in practice. Any limitations on this right required by the need to maintain the secrecy of the organisation and tactics of detective operations should be the minimum necessary to protect them and should not unduly undermine the enjoyment of the right.

Article 7

5.23 Article 7 paragraph 2 may need more explanation to ensure that the confidentiality of the individual is assured. In certain cases, the identify of a CHIS etc. may need to be disclosed to relevant authorities in order to provide assistance to them (e.g. in the event that they are to be provided with a new identity or enter into a witness protection programme). It may be that paragraph 2 only refers to disclosure to the public, but this should be specified.

Recommendation 23: Article 7 paragraph 2 should provide for disclosure of the identity of CHIS where this is necessary for the protection of their vital interests.

Article 9

5.24 Reference is made to the comments and recommendations concerning this Article in the general comments section at paragraphs 4.21 to 4.25 and recommendations 7 and 8 above.

Article 10

[69] This principle should only be derogated from when such information would jeopardize ongoing investigations, expose a person to a danger or harm the rights and freedoms of others.

[70] *Roman Zakharov v. Russia*, judgment of 4 December 2015, Application No. 47143/06, at paragraph 234. See also *Weber and Saravia v. Germany*, decision of 29 June 2006, Application No. 54934/00, where the Court underlined that if the intercept data is destroyed and the persons concerned are not notified of the fact that they were under surveillance, "this may serve to conceal monitoring measures which have been carried out by the authorities". **Such surveillance (also by [national security agencies]) must therefore be "in accordance with law", serve a "legitimate aim in a democratic society", and be "necessary" and "proportionate" in relation to that aim.**

5.25 The list at paragraph 2 does not appear to include a provision for the tasking/deployment of a CHIS who is used to obtain information covertly by a law enforcement agency or other authority. It is unclear if this is an omission or if such a deployment is understood to be an element of other measures, e.g., detective experiment.

Recommendation 24: if deployment of a CHIS is not allowed as an element of an action specified in Article 10 paragraph 2, specific provision for such deployment should be made.

5.26 Article 10 lists specific detective measures and offers two separate regulatory regimes depending on the nature of the measure in question. In view of their intrusive nature, thus warranting stricter procedural safeguards, it is recommended that the detective measures listed in Article 10 paragraph 2 sub-paragraphs 15 ("surveillance of a thing or place") and 22 ("signals intelligence") be added to the first group (which currently includes the detective measures referred to in sub-paragraphs 1-11).

Recommendation 25: The detective measures listed in Article 10 paragraph 2 sub-paragraphs 15 ("surveillance of a thing or place") and 22 ("signals intelligence") should be added to the group of detective measures referred to in sub-paragraphs 1-11, which require additional procedural safeguards.

5.27 Reference is also made to the comments and recommendations concerning this Article in the general comments section at paragraphs 4.19, 4.20 and 4.26 to 4.28 and recommendations 5, 9 and 10 above.

5.28 There is a technical mistake in paragraph 7 that erroneously refers to paragraph 5 of the same Article.

Article 11

5.29 The specification of the specific detective measures that may be taken by each body, linking them specifically to the mandate and competence of the body, is a very positive initiative and will assist in ensuring that any detective measures are proportionate and necessary. This will also assist in reducing the scope and likelihood of abuse or excessive use of detective measures.

Article 12

5.30 Reference is made to the comments and recommendations concerning this Article in the general comments section at paragraph 4.11 and recommendation 1 above.

5.31 The specific listing of the duties of units conducting detective operations is a positive initiative as it provides a clear point of reference for those units. It should also assist in reducing the scope and likelihood of abuse or excessive use of detective measures.

Article 13

5.32 It is not entirely clear if Article 13 paragraph 2 refers to a CHIS, agent or confidential contact. A CHIS is generally paid for his or her assistance, although it is not an absolute requirement. Context is required in order to demonstrate if the individual is a public spirited citizen providing information on a 'free of charge basis', or if there is a system of tasking payments or rewards for the individual, whom may be co-operating for payment or whose motivation is for a reward. The status

of the person is important in terms of understanding their motivation but also in terms of enabling law enforcement agencies and other bodies to manage the risks involved.

5.33 Paragraph 8 allows for the obtaining of a wide range of information, including information classified as "commercial and bank secrecy". The compliance of this provision with Article 269 of the CPC should be considered and the paragraph amended as appropriate.

5.34 Paragraph 14 would benefit from an explicit statement that any use of physical coercive measures should be the minimum necessary to achieve the lawful objective being pursued. The current text appears to be a generic sentence covering the use of force in support of 'detective operations'. Whilst brief, more emphasis may be required to reinforce the principles of necessity and proportionality.

Recommendation 26: Article 13 paragraph 14 should contain an express requirement that any use of physical coercive measures should be the minimum necessary to achieve the lawful objective being pursued.

Recommendation 27: The compliance of Article 13 paragraph 8 of the draft Law with Article 269 of the CPC should be examined carefully.

5.35 Reference is also made to the comments and recommendations concerning this Article in the general comments section at paragraph 4.19 and recommendation 6 above.

5.36 Article 13 of the draft Law allows the units conducting detective operations to access data held by private entities, including by Internet Service Providers or public communication networks. It is beyond the scope of this opinion to assess the Ukrainian national retention laws. However, in order to fully review the compliance of the proposed law with the European data protection standards, it would be necessary to review whether under Ukrainian law public communications networks are obliged to retain data relating to a person's life and to his/her communications and whether such data retention obligations are within what is "strictly necessary" (e.g. what is the duration of such retention and what are the procedure of sharing such information with the public authorities).[71]

Recommendation 28: a review should be undertaken of whether under Ukrainian law public communications networks are obliged to retain data relating to a person's life and to his/her communications and whether such data retention obligations are within what is "strictly necessary".

Article 14

5.37 In paragraph 4 there is a prohibition on instigating or provoking anyone to commit an offence. This is an important safeguard. However, consideration should be given to using 'agent provocateur' as a universal term and making explicit reference to the prohibition on entrapment, as

[71] Following the Digital Rights Ireland judgment that annulled EU Data Retention Directive, a number of European countries have reformed their national retention laws. Currently, European countries are spilt on this issue. Some maintain a firm commitment not to introduce retention, whereas others, like France and the United Kingdom, are firmly committed to continuing with retention. To form its opinion, Ukraine might follow closely the outcomes the debates on these subjects. See Advocate General Saugmandsgaard Øe opinion July 19, 2016. According to AG's opinion, a general obligation to retain data imposed by a Member State on providers of electronic communication services may be compatible with EU law However, however it is imperative that that obligation be circumscribed by strict safeguards, http://curia.europa.eu/jcms/upload/docs/application/pdf/2016-07/cp160079en.pdf.

set out in the ECtHR case-law on Article 6 of the Convention. There is relevant case-law in *Teixeira de Castro v Portugal*[72] and *Ramanauskas v. Lithuania*.[73]

5.38 It may be purely a matter of interpretation, but the prohibition on the use of force in Article 14 paragraph 5 should not be an absolute prohibition. There are situations where units conducting detective operations may be required to use force in order to protect themselves or others. This is specifically provided for in Article 13 sub-paragraph 14.

Article 15

5.39 Security is paramount in ensuring that information obtained in the course of detective operations is not used inappropriately. Adequate security can ensure chain of custody and transparency as regards who has accessed the information.

Recommendation 29: Consideration should be given to whether the word "securely" should be inserted in paragraph 2, so that the text would read as follows: "Information shall be recorded and securely kept in files and catalogues and on digital carriers".

5.40 Article 15 paragraph 5 limits the retention of information relating to terrorist acts for five years. This figure is relatively short and in many countries such information would be held for a significantly longer period of time. If there is a legitimate reason for retaining information regarding terrorism (or other serious crimes) for longer periods, it is lawful to do so.[74]

5.41 The reference in Article 15 paragraph 4 to the "elimination" of information collected in the course of detective operations (including personal data) is formulated in a generic way and does not contain any further details/processes, timelines on data erasure. It is unclear what the drafters mean by the following wording: "unless it contains any information on the actions prohibited under the laws of Ukraine." This can be interpreted broadly, and it is not clear whether this would cover specific criminal offences or any other misconduct.

5.42 European standards, including Principle 6 of Recommendation No.(87)15, require strict rules on the destruction/erasure of surveillance data to prevent surveillance from remaining hidden after the fact. Domestic law must indicate with sufficient clarity the procedures for secure handling, storage and destruction of materials obtained through covert surveillance.[75] Article 20 paragraph 3 is also relevant in this respect and relates to the duration of storage of closed detective files.

Recommendation 30: The proposed law should include processes and procedures for data erasure. If there is a domestic law or other binding regulation for processing intercepted data, the proposed law should contain an explicit reference to this law.

5.43 It is also important for the Ukrainian authorities to examine ways to introduce technical means to ensure proper destruction of data, because most of the secret surveillance gathered will be

[72] Judgment of 9 June 1998, Application No. 25829/94.
[73] Judgment of 5 February 2008, Application No. 74420/01.
[74] See e.g. *Segerstedt-Wiberg v. Sweden*, judgment of 6 June 2006, Application No. 62332/00.
[75] *See* related case law: *R.E. v. United Kingdom*, judgment of 27 October 2015, Application No. 62498/11, *Rotaru v. Romania*, judgment of 4 May 2000 (Grand Chamber), Application No. 28341/95, *Kennedy v. the United Kingdom*, judgment of 18 May 2010, Application No. 26839/05.

in digital form (e-communication data, both content and meta-data), audio and video recordings, data captured through mobile phones and etc. In light of existing and emerging technologies, as well as cloud solutions, such data could remain accessible on servers, cloud or be easy to copy.

Recommendation 31: technical measures to ensure the proper destruction of data should be a requirement under the draft Law.

5.44 The draft law does not specify the processing and use of sensitive data in law enforcement/investigative context. For example, Article 15 has no reference how processing sensitive data is handled. Article 22 paragraph 6 also has implications for the processing of personal sensitive data. If not otherwise provided by Ukrainian law, it is recommended to include a provision mirroring the language of Principle 2.4 of Recommendation No.(87)15 on collection and processing of sensitive data in law enforcement context.[76]

Recommendation 32: If not otherwise provided by Ukrainian law, it is recommended to include a provision mirroring the language of Principle 2.4 of Recommendation No.(87)15 on collection and processing of sensitive data in law enforcement context.

5.45 If not regulated otherwise, it is recommended that the proposed draft incorporate approach adopted by the new EU Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (commonly referred as "Police Directive"). According to the EU Police Directive, "the measures taken by the data controller shall in particular include drawing up and implementing specific safeguards in respect of the treatment of personal data relating to children, where appropriate."

Recommendation 33: The processing data relating to children needs special consideration and should be subjected to strengthened safeguards, such as routine review of the effectiveness of such data processing and stricter storage periods.

5.46 In accordance with the European data protection standards, including with the new EU Police Directive, a distinction should be made between the different categories of data subjects (e.g. processing of data of individuals who are not suspects. Processing of data of persons who are not suspected of having committed any crime (other than victims, witnesses, informants, contacts and associates) is to be strictly distinguished from data of persons related to a specific crime and "should only be allowed under certain specific conditions and when absolutely necessary for a legitimate, well-defined and specific purpose."[77] The proposed draft does not specify how such distinction between the different categories of data would be guaranteed. If not otherwise regulated by the Ukrainian laws, it is recommended that such provision be included in the proposed draft. This distinction also carries important ramifications for accurate implementation of data protection principles (e.g. purpose limitation, lawful processing).

[76] "The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry."

[77] In the view of European data protection authorities, such processing should "be restricted to a limited period and the further use of these data for other purposes should be prohibited." A specific protection of "non-suspects" is particularly required when the processing is not done in a specific criminal investigation or prosecution.

Recommendation 34: In order to ensure convergence with European data protection standards, a distinction should be made between the different categories of data subjects (e.g. processing of data of individuals who are not suspects).

Article 16

5.47 Article 16 paragraph 5 refers to recording standards. For example, is there a prescribed standard for case files and applications/authorisations for covert tactics that is acceptable to the prosecutor and facilitates judicial oversight arrangements? This may be a consideration for inclusion in the legislation or for any internal operating policy or procedures, which will ensure consistency of standards and assist with any inspection processes.

5.48 As was stated above in respect of Article 15 paragraph 2, consideration should be given to the insertion of the word "securely" in Article 16 paragraph 5, so that the provision would read: "Materials related to results of detective measures shall be kept securely in detective operations case files".

5.49 Reference is also made to the comments and recommendations concerning this Article in the general comments section at paragraph 4.31 above.

Article 18

5.50 Article 18 concerns the registration of detective operations case files in defined circumstances. It is important to minimise the likelihood of different bodies conducting operations against the same persons or groups. This situation can occur if similar information is received, as it may fall within the perceived or actual competency of more than one unit or agency.

5.51 If only one detective file is to be registered, it is necessary to ensure that there is a mechanism for ensuring that different units or agencies do not register files regarding the same information. Co-ordination is necessary in order to avoid conflicts, potential risks and also to ensure the best use of resources. This may be a consideration for policy makers within each agency or to be addressed via a co-ordination forum.

Article 24

5.52 Article 24 paragraph 3 allows for evidence to be given by the head of the relevant unit conducting detective operations, in cases where if a person involved in detective operations did so, he or she would be exposed to danger as a result. It is important to ensure that this does not result in violations of the right to a fair trial ("equality of arms" guarantee). While it is possible to protect the identities of witnesses in certain situations, if the evidence is decisive for the guilt or innocence of the defendant, it may be required for the witness to give evidence in person.[78] The fear of danger to the witness must be objectively grounded; it is not sufficient for the head of the relevant unit conducting detective operations to state that there is a danger.[79] In addition, the requirements of Article 97 of the CPC (in particular paragraph 5) should be adhered to.

[78] *Al-Khawaja and Tahery v. United Kingdom*, judgment (Grand Chamber) of 20 January 2009, Application Nos. 26766/05 and 22228/06, at paragraph 147.
[79] *Ibid.* at paragraph 124.

Recommendation 35: Any reliance on the provisions of Article 24 paragraph 3 allowing the giving of evidence by the head of the relevant unit must be based on objectively grounded fears and conducted in compliance with Article 97 (in particular paragraph 5) of the CPC.

Article 31

5.53 Further to the conceptual comments and recommendation concerning the same set of safeguards and guarantees applicable to the intrusive actions and relevant procedural norms,[80] it is to be once more highlighted that the article lacks sufficiently detailed, specific references to the specific articles of the CPC.

5.54 Furthermore, the proposed draft obliges the authorities to report only what seems as statistical information about detective measures. There is a need for more transparency, accountability and democratic control, to give citizens confidence. The reporting should provide more detailed information (e.g. the volume and size of private electronic communications the authorities hold, the number of the type of the motions approved and the type of detective measures they entail (e.g. interception of communications, video surveillance, metadata or content data interception). The current form of public and parliamentary oversight does not provide for a procedure where the public can get sufficiently detailed information about the nature of the surveillance. Furthermore, there parliamentary control should be more proactive with a stronger mandate to oversee surveillance operations of respective authorities. If processing of personal data in law enforcement context falls within the jurisdiction of the Ukrainian Parliament Commissioner of Human Rights (Ombudsman), the proposed law or Data Protection Law needs to explicitly mention it (in this case Ombudsman serves as a general independent Supervising Authority).

Recommendation 36: If the Ombudsman lacks oversight powers concerning secret surveillance, there needs be an independent supervisory authority, outside the police sector which should be responsible for ensuring respect for data protection principles in law enforcement context (Principle 2.4 of Recommendation No.(87)15).[81] This oversight should be in addition to the prosecutorial and judicial oversight otherwise provided for, and could focus on systemic issues rather than on individual cases.

Section 7

5.55 The title of this section narrows the role attributed to the Public Prosecutor's Office by the Constitution (in Article 131) and the functions provided for throughout the draft Law, Articles 34-35, in particular. This supervision is not limited to legal compliance of detective operations and extends to organisational issues and providing guidance to them. Accordingly, the term "legal compliance" is not reflective of the actual role ascribed to the Public Prosecutor's Office and should be removed.

Recommendation 37: The term "legal compliance" should be omitted from the title of Section 7.

[80] See, for example, paragraphs 4.1 and 4.13 above.

[81] The ECtHR posits that it is preferable for a judge to be responsible to maintain oversight. This does not exclude that another body can be responsible, "as long as it is sufficiently independent from the executive" and "of the authorities carrying out the surveillance, and [is] vested with sufficient powers and competence to exercise an effective and continuous control". The ECtHR also "notes that it is essential that the supervisory body has access to all relevant documents, including closed materials". Finally, the ECtHR takes into account "whether the supervisory body's activities are open to public scrutiny."

Article 34

5.56 Article 34 paragraph 1 should be amended in line with the comments and recommendation as to the scope of prosecutorial oversight.[82]

Article 35

5.57 Reference is made to the comments and recommendations concerning this Article in the general comments section at paragraph 4.31 above.

5.58 For clarity, consideration should be given to outlining the role of the prosecutor when emergency applications are required, which may be of benefit to include in this Article and thus aligned to Article 250 of the CPC.

Article 38

5.59 It is encouraging to see that there is a legislative provision to enable inter-agency engagement, which may overcome potential barriers of inter-agency culture, different agencies working in isolation from each other, and promote and develop professional practice.

Article 39

5.60 This article provides a generic overview of the investigative powers that are available to investigators to consider as part of any criminal investigation. However, there is scope to increase the level of clarity of the terminology as it is currently ambiguous, e.g. at sections 1, paragraphs 1 and 2, 'audio control' or 'video control'. It is not entirely clear whether these terms refer to 'audio surveillance of a person' and 'video surveillance of a person' as defined in the Terms and Conditions at the start of the draft Law. It is important that the terminology used in the draft Law is consistent throughout it.

5.61 Reference is also made to the comments and recommendations concerning this Article in the general comments section at paragraph 4.11 and 4.18, and recommendations 1 and 5 above.

Article 40

Recommendation 38: Article 40 paragraph 1 should be brought into compliance with Article 41 of the CPC by specifying the written format of formulating an assignment to conduct a detective activity.

Article 41

5.62 This Article relates to the powers that refer to the recruitment and tasking of an informant/agent or CHIS to covertly collect intelligence relating to the investigation. It states in paragraph 1 that this is on a 'permanent basis'. This term is potentially ambiguous, as it could refer to a long term penetration agent, or to an individual who is recruited and tasked for the duration of a specific operation. It is suggested that this term be clarified.

5.63 Paragraphs 2 and 3 appear simplistic, given the complexity and risks where CHIS are authorised and tasked in the course of a detective action. Article 275 of the CPC provides a

[82] See paragraph 4.12 and recommendation 3 above.

framework on using confidential cooperation, including restrictions as to involving specific categories of persons, and should be referred to and quoted accordingly.

5.64 There is also a need for practical guidance to be available in order to ensure that the rights of a CHIS are protected. In particular, if there is any foreseeable likelihood that the CHIS's role or information obtained via it will become relevant in any subsequent pre-trial investigation, careful consideration and risk management is needed. This may be an area for further consideration, as well as developing appropriate provisions that enable the effective recruitment and tasking of a CHIS. It could be done through the development of a Rulebook or other appropriate administrative document.

Recommendation 39: The term "permanent basis" should be clarified.

Recommendation 40: Reference should be made to Article 275 of the CPC and its provisions incorporated. Consideration should be given to the development of practical guidance governing the procedure to be followed in the event that the role of a confidential informant (CHIS) is potentially going to be revealed in any subsequent pre-trial investigation.

Article 42

5.65 Article 254 of the CPC provides for the measures to protect and use of information obtained through covert investigative (detective) actions, and should be referred to and quoted accordingly.

Recommendation 41: Reference should be made to Article 254 of the CPC and its provisions incorporated.

List of Recommendations

Recommendation 1: It is recommended that Article 12 paragraph 3 and Article 39 paragraphs 3 and 4 are specifically subjugated to the requirement in Article 214 of the CPC concerning the entry of information about actual or likely crimes within a 24-hour period. In addition, the conduct of any detective operations beyond that period should be prohibited without approval as required for the specific operation as set out in the draft Law. Finally, the conduct of any unauthorised activities by detective officers should be expressly prohibited and provision made for specific procedures for obtaining instructions from the investigative authority or prosecutor, to be issued in accordance with Article 41 of the CPC.

Recommendation 2: In order to reduce the scope for confusion as to the meaning of a number of terms used both in the draft Law and in the CPC, it would be advisable for them to be given the same definition in both laws.

Recommendation 3: the draft Law should contain a specific and explicit requirement that the same level of procedural safeguards as are set out in the CPC, in particular prosecutorial and judicial oversight, is incorporated into the draft Law.

Recommendation 4: the draft Law should provide, in terms analogous to those set out in Articles 253 and 254 of the CPC, that once detective operations are concluded those affected by them should be notified where it is possible to do so.

Recommendation 5: The thresholds for arrest in Article 10 paragraph 6 sub-paragraph 2 and Article 39 paragraph 3 should be harmonised with Article 207 of the CPC.

Recommendation 6: The draft Law should follow the approach adopted in the CPC and require that inspections of financial statements etc. of companies, as provided for in Article 10 paragraph 2 sub-paragraph 19, can only be done in the course of individual overt or covert investigative activities.

Recommendation 7: It would be advisable that Article 9 of the draft Law states that, if a crime has been committed (*corpus delicti*), whether consummated or unconsummated,[83] or where specific measures of restraint have not been complied with, any further actions should be of an investigative, conducted under the applicable provisions of the CPC.

Recommendation 8: Article 9 paragraph 1 sub-paragraph 3 should require that a basis for the specific detective action is present. Sub-paragraph 4 should require that there are sufficient grounds to suspect that there are individual acts involving or potentially involving criminal activities concerned with individual or systemic acts of money-laundering or financing of terrorism, etc.

Recommendation 9: The terms contained in Article 10 paragraph 2 sub-paragraphs 20, 21 and 22 should be defined more specifically.

Recommendation 10: The draft Law should specifically incorporate the provisions of Article 250 of the CPC, either directly or by specific reference to the requirements of that Article.

[83] As defined in Article 13 of the Criminal Code of Ukraine.

Recommendation 11: The draft Law should require that all detective operations are registered appropriately, including a requirement that all information related to them, including information obtained, is included.

Recommendation 12: The draft Law should include a table setting out the amendments to other legislation which it would require.

Recommendation 13: The draft law should address data protection aspects within law enforcement context more systematically (e.g. by introducing a detailed sub-section or adopting a specific data protection law covering LEAs).

Recommendation 14: The definition of "audio surveillance of a person" in the draft Law should distinguish between the various forms of audio surveillance it permits, in particular between the use of eavesdropping devices and telephone interception, and should also distinguish between actions depending on the location in which they occur.

Recommendation 15: The draft Law should make specific reference to the fact that any actions related to juveniles should have as their primary aim the protection of the best interests of the child.

Recommendation 16: The draft Law should either incorporate further regulations governing the use of polygraph testing, or a specific reference to the relevant legislation.

Recommendation 17: Consideration should be given to the removal of Article 2 paragraph 2.

Recommendation 18: The scope of Article 2 paragraph 3 should be reviewed in order to prevent any extensive interpretation and unauthorised application of detective activities, as well as to ensure that it does not allow for the processing of personal data in an unduly broad set of circumstances.

Recommendation 19: In order to ensure coherence with the Convention and the case-law of the ECtHR, Article 4 of the draft Law should include as a principle of detective operations *necessity in a democratic society and interests of national security, public safety, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms.* This should be adopted also in Article 6 paragraph 2.

Recommendation 20: The draft Law should make provision for the management of information collected during the course of detective operations which concerns persons who are not suspected of involvement in any wrongdoing.

Recommendation 21: there should be provision in Article 6 paragraph 2 for a judicial remedy regarding compensation in appropriate cases.

Recommendation 22: Article 6 paragraph 3 should prescribe the exact manner in which the right to be informed of having been subject to detective operations is to be realised in practice. Any limitations on this right required by the need to maintain the secrecy of the organisation and tactics of detective operations should be the minimum necessary to protect them and should not unduly undermine the enjoyment of the right.

Recommendation 23: Article 7 paragraph 2 should provide for disclosure of the identity of CHIS where this is necessary for the protection of their vital interests.

Recommendation 24: If deployment of a CHIS is not allowed as an element of an action specified in Article 10 paragraph 2, specific provision for such deployment should be made.

Recommendation 25: The detective measures listed in Article 10 paragraph 2 sub-paragraphs 15 ("surveillance of a thing or place") and 22 ("signals intelligence") should be added to the group of detective measures referred to in sub-paragraphs 1-11, which require additional procedural safeguards.

Recommendation 26: Article 13 paragraph 14 should contain an express requirement that any use of physical coercive measures should be the minimum necessary to achieve the lawful objective being pursued.

Recommendation 27: The compliance of Article 13 paragraph 8 of the draft Law with Article 269 of the CPC should be examined carefully.

Recommendation 28: A review should be undertaken of whether under Ukrainian law public communications networks are obliged to retain data relating to a person's life and to his/her communications and whether such data retention obligations are within what is "strictly necessary".

Recommendation 29: Consideration should be given to whether the word "securely" should be inserted in paragraph 2, so that the text would read as follows: "Information shall be recorded and securely kept in files and catalogues and on digital carriers".

Recommendation 30: The proposed law should include processes and procedures for data erasure. If there is a domestic law or other binding regulation for processing intercepted data, the proposed law should contain an explicit reference to this law.

Recommendation 31: Technical measures to ensure the proper destruction of data should be a requirement under the draft Law.

Recommendation 32: If not otherwise provided by Ukrainian law, it is recommended to include a provision mirroring the language of Principle 2.4 of Recommendation No.(87)15 on collection and processing of sensitive data in law enforcement context.

Recommendation 33: The processing data relating to children needs special consideration and should be subjected to strengthened safeguards, such as routine review of the effectiveness of such data processing and stricter storage periods.

Recommendation 34: In order to ensure convergence with European data protection standards, a distinction should be made between the different categories of data subjects (e.g. processing of data of individuals who are not suspects).

Recommendation 35: Any reliance on the provisions of Article 24 paragraph 3 allowing the giving of evidence by the head of the relevant unit must be based on objectively grounded fears and conducted in compliance with Article 97 (in particular paragraph 5) of the CPC.

Recommendation 36: If the Ombudsman lacks oversight powers concerning secret surveillance, there needs be an independent supervisory authority, outside the police sector which should be responsible for ensuring respect for data protection principles in law enforcement context (Principle 2.4 of Recommendation No.(87)15). This oversight should be in addition to the prosecutorial and

judicial oversight otherwise provided for, and could focus on systemic issues rather than on individual cases.

Recommendation 37: The term "legal compliance" should be omitted from the title of Section 7.

Recommendation 38: Article 40 paragraph 1 should be brought into compliance with Article 41 of the CPC by specifying the written format of formulating an assignment to conduct a detective activity.

Recommendation 39: The term "permanent basis" should be clarified.

Recommendation 40: Reference should be made to Article 275 of the CPC and its provisions incorporated. Consideration should be given to the development of practical guidance governing the procedure to be followed in the event that the role of a confidential informant (CHIS) is potentially going to be revealed in any subsequent pre-trial investigation.

Recommendation 41: Reference should be made to Article 254 of the CPC and its provisions incorporated.