Tornike Khidesheli*

Production Order in Georgian Legislation and its compliance with the Convention on Cybercrime

The letter addresses a topical issue such as Production Order in Georgian legislation and its compliance with the Convention on Cybercrime. The investigative action is considerable for obtaining content or traffic data, including subscriber data, etc. A well-established national legal framework that is in line with International Law is crucial. Thus, the paper aims to consider the compliance of Article 136 of GECPC with the Budapest Convention, to expose any inaccuracies and thoroughly analyze them.

Keywords: *Computer system, computer data, digital evidence, electronic evidence.*

1. Introduction

In the modern world, cybercrime poses a real threat to individuals, businesses, and government agencies.[1] The development of technology has given rise to different forms of crime and has had an impact on traditional crime too. Given the existing reality, it's obvious that digital evidence is everywhere. The world is becoming increasingly interconnected and hard to imagine daily lives without a device. In parallel, the value of digital evidence increases for any criminal investigation[2] whether it is petty crimes, cybercrime, or even organized crime.[3]

Due to the volume, dynamic and volatile nature of electronic evidence the availability of appropriate tools are required. Cybercrime makes clear the need for their existence. Especially, when cybercriminals conduct sophisticated attacks on a computer, resulting in the disclosure of a vast amount of personal data, including usernames, date of birth, addresses, etc.[4] Under such cases, the major challenge is in identifying the perpetrator and assessing the extent and impact of the criminal act. Therefore, immediate and sometimes covert investigations are vital.[5]

Fortunately, through the Convention on Cybercrime, the Council of Europe is successfully tackling the challenges[6] and offering a range of procedural powers including Production Order. It promotes the state to ensure its positive obligation to protect individuals from crime and conduct the investigation with respect to human rights and fundamental freedoms.

Respectively, Convention covers substantive and procedural criminal law as well conditions and safeguards. The state must take these requirements into account while implementing the special procedural power in national legislation. Whereas article 136 of GECPC, the so-called "Request for document or information" is corresponding to article 18 of the Convention and at the same time it's an effective domestic measure for obtaining stored electronic data, its compliance with international

* Phd Student, Visiting Lecturer at Ivane Javakhishvili Tbilisi State University Faculty of Law.

1 *Schwerha J.J,* Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers" France, 2010, 4.

2 *Kerr S.O.,* Searches and Seizures in Digital World, Harvard Law Review, Vol. 119, USA, 2006, 1.

3 *Arnes A. (ed.),* Forensic Science, Digital Forensics, Norway, 2018, 1.

4 *Flaglien O. A.,* The Digital Forensics Process, Digital Forensics, *Arnes A. (eds.),* Norway, 2018, 13.

5 Explanatory Report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 21.

6 *Schwerha J.J,* Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers" France, 2010, 4.

law is meaningful. That's why this article will focus on the requirements of the Convention on Cybercrime itself and as well as on the compliance of article 136 of GECPC with them.

2. Conditions of Convention on Cybercrime

2.1. Implementing the Procedural Power

The purpose of Production Order is to empower law enforcement agencies to collect any type of computer data, including subscriber data. Looking from the perspective of Article 15, this is an alternative investigative power among coercive measures that provide a less intrusive means of obtaining digital evidence relevant to criminal investigations.[7] In particular, when data holders are prepared to cooperate with law enforcement agencies and they need to operate based on clear legal duties and within the foreseeable legal framework.[8] Therefore, several requirements should be taken into account before implementing a "Production Order" in national legislation. In particular: **1. Whether "Production Order" is implemented as standalone procedural power; 2. Whether national law is precise and foreseeable; 3. Whether national law contains safeguards against the arbitrary application**.[9]

Besides, the production of privileged data may be excluded. For example, privileged communication between lawyers and clients, etc.[10] And, judicial or other independent supervision is appropriate for the exercise of power, but this should be decided individually for each type of data.

2.2. Scope of Procedural Provisions

The scope of investigative methods, including the production order, is specified in article 14 of the Cybercrime Convention. The powers can be applied a) to criminal offences established under the Convention itself; b) to criminal offences committed by the means of a computer system, and c) to the collection of evidence in electronic form of any criminal offence. [11] Such a broad definition of the scope is an attempt to ensure the competent authorities with an equivalent capability for obtaining digital evidence as exists under traditional powers and procedures. Herewith, it is proof that electronic data can be used as evidence before a court in criminal proceedings, irrespective of the nature of the offence is prosecuted.[12]

Despite the general and wide interpretation of scope, the Convention still limits it. For example, interception of content data should be limited to a range of "serious offences". This is conditioned by its covert nature and high intrusiveness into privacy. Regarding the definition of

---

7 Explanatory Report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 29.

8 Ibid.

9 Conditions and Safeguards under Article 15 of the Convention on Cybercrime in the Eastern Partnership, Council of Europe, 2018, 9, <https://rm.coe.int/conditions-and-safeguards-under-article-15-of-the-convention-on-cyberc/16808f1e39> [08.03.22].

10 Explanatory Report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 30.

11 General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership, Council of Europe, Cybercrime EAP, 2017, 7, <https://rm.coe.int/general-report-on-mapping-the-current-strengths-weaknesses-opportuniti/16808f1e1b> [08.03.2022].

12 Explanatory Report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 22.

"serious crime" the Convention maintains a neutral position and the states are eligible to determine it as it is defined in their domestic law.[13] However, this does not preclude the possibility of states to determine the list of crimes and the scope of measure on their own.

The requirement to limit the scope of interception of content data is imperative, but not in the case of traffic data. Signatory states are independent in imposing restrictions with an interception of traffic data. We may not obtain the content of the communication during the collection of traffic data and it may not be equivalent in terms of privacy and degree of intrusiveness, but it can help trace the source and destination of communication, thus identifying the person. So the state has the discretion whether limit the scope of the real-time collection of traffic data or not. However, when restricting, an imperative requirement should be considered that the range of offences will not be more restricted than to offences to which "real-time collection of content data" applies.[14]

To sum up, litra "a" of article 14(2) specifies a list of criminal offences, but litra "b" and "c" are more broadly construed that the investigative measures can be applied to every criminal offence.[15] The only imperative request to limit the scope of procedural powers with the range of serious offences is in case of real-time collection of content data, but not with an interception of traffic data or production order. Besides, according to the explanatory report to the Convention on Cybercrime, to facilitate tracing the source or destination of electronic communication, limiting the scope collection of traffic data is not recommended.[16] Except for the interception of content data, a broad definition of the scope of procedural provisions is appropriate. The existence of an offence has limited deterrent effects if there is no means to identify the actual offender and bring him to justice.[17] Herewith, the convention does not limit the investigation methods to any phases, as long as the probable cause is fulfilled.[18]

2.3. Conditions and Safeguards

Production Order, an adapted traditional "search and seizure" to the new technological environment, expedited preservation of stored computer data, real-time collection of content and traffic data, each of them is coercive investigation methods. So the coercive measures often interfere with the right to private life, liberty, freedom of expression, property rights, and can be applied without the consent of the person who is subject to it.[19] Therefore, article 15 of the Convention stipulates the obligation to protect fundamental human rights while making use of the investigation methods. To ensure adequate protection of human rights, it is essential: a) to respect for obligations undertaken under international human rights instruments; b) reliance on grounds justifying application; c) adherence to the principle of proportionality; d) limitation of the duration

---

13 Explanatory Report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 22.
14 Ibid., 23.
15 *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (ed.)*, Norway, 2018, 100.
16 Explanatory Report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 22-23.
17 K. U. v. Finland, [2009], ECHR, №2872/02. §46.
18 *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, 2018, 100.
19 Ibid., 61.

and scope of the powers; e) judicial or other independent supervision;[20] f) considerations relating to third parties.[21] Let's consider each of them:

a)Respect for obligations undertaken under international human rights instruments – It is hard to imagine a human rights system being strengthened without proper respect for international treaties. As a rule, they had a great impact on national legislation and case law. In the case of Georgia, such are the European Convention on Human Rights 1950 and ECHR judgements. Accordingly, the Convention calls on the signatory parties to comply with their obligations under international instruments. Particularly, rights to liberty and security (article 5), fair trial right (article 6), the principle of no punishment without law ((nulla poena sine lege) (article 7), and the right to privacy (article 8).[22]

b) Reliance on grounds justifying application - As we mentioned above, the application of any of the procedural methods available under the Cybercrime Convention represents, to one degree or another, interference into the private life of persons. Therefore, the use of such powers should be sufficiently justified by applicable facts and based on some external findings. Moreover, such grounds must be presented and available before the actual exercise of procedural powers.[23] To some extent, it precludes an arbitrary interference into the right and misuse of state resources.[24] Herewith, "ongoing investigation" is another precondition for the application of an investigative measure.

c)The principle of proportionality – if we look at the sequence of investigative measures we will see that they are arranged in a certain order. And the criterion is the intensity of intrusiveness of human rights. The procedural provisions begin with "expedited preservation of computer data, which is a less intrusive investigative measure and ends with very intrusive means such as a real-time collection of content data. We may say, that this is a kind of indicator to protect the principle of proportionality. If it is possible to achieve the goal with the application of less intrusive procedural powers, using the "heavier" options are not allowed. The choice of procedural powers should be proportional to the nature of the offence and the circumstances of the case.[25] Herewith, article 21(1) indicates to proportionality that the interception of content data should be used only for investigation and prosecution of a limited number of criminal offences. [26]

---

[20] General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership, Council of Europe, Cybercrime EAP, 2017, 7, <https://rm.coe.int/general-report-on-mapping-the-current-strengths-weaknesses-opportuniti/16808f1e1b> [08.03.2022].

[21] Convention on Cybercrime, Budapest, 23.11.2001, Article 15(3).

[22] *Dragicevic D., Juric M.,* Article-15 – Safeguards in the Eastern Partnership region, Council of Europe, 2013, 11.

[23] General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership, Council of Europe, Cybercrime EAP, 2017, 8, <https://rm.coe.int/general-report-on-mapping-the-current-strengths-weaknesses-opportuniti/16808f1e1b> [08.03.2022].

[24] *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, 2018, 99.

[25] General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership, Council of Europe, Cybercrime EAP, 2017, 13, <https://rm.coe.int/general-report-on-mapping-the-current-strengths-weaknesses-opportuniti/16808f1e1b> [08.03.2022].

[26] *Dragicevic D., Juric M.,* Article-15 – Safeguards in the Eastern Partnership region, Council of Europe, 2013, 11.

d) Limitation of the duration and scope of the powers – this safeguard has a big impact on in case of interception of content data. Except for the fact that the scope of the real-time collection of content data (imperative) and traffic data should be limited with "serious crimes", the limitation of the duration of their application is essential too. But after the expiration of the warrant, it can be reviewed and prolonged.[27]

e) Judicial or other independent supervision[28] **–** one of the major safeguards against violations of a right to privacy and a fair trial. When discussing supervision, we assume an individual must be functionally independent and not formally from parties to the criminal proceedings. Except for the judge, such may be the data protection authorities, parliamentary or ad hoc commissions, etc.[29]

f) Considerations relating to third parties – According to article 15(3) of the Convention, in the interests of the administration of justice states must consider the impact of the powers and procedures upon the rights and legitimate interests of third parties. The individuals who are not related to the crime, but may be affected by the investigation. It is noteworthy that the Convention only requests the parties to be aware of it, without prescribing a concrete solution.[30] The legal interests of third parties are practical. For example, in January 2012, the website www.megaupload.com was seized and shut down by the US Department of Justice, charged with criminal copyright infringement and racketeering. The web had more than 66 million users, whose accounts thus became inaccessible.[31] Even though the investigation was directed against only some people, still, millions of users were affected by the measure.

Production order serves to strengthen the legitimate interests of third parties. Except for the fact that it is a less intrusive means of obtaining relevant information to the criminal investigation, the implementation of such measure will be beneficial to third parties, especially for ISP. It provides them with a legal basis to assist law enforcement agencies and as a result excludes their possibility to provide competent authorities with personal data voluntarily.[32] Especially when, the subscriber data and content of communication are confidential.[33]

To summarize, the above-mentioned conditions and safeguards are a non-exhaustive list for the complete protection of human rights and fundamental freedoms. However, they are basic prerequisites for implementing the procedural provisions into the national legislation. In addition, the protection of other safeguards is crucial. For instance, the presumption of innocence, right to liberty and security of a person, right to a fair trial, freedom of expression, double jeopardy clause,

---

27 General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership, Council of Europe, Cybercrime EAP, 2017, 8, <https://rm.coe.int/general-report-on-mapping-the-current-strengths-weaknesses-opportuniti/16808f1e1b> [08.03.2022].

28 *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, 2018, 101.

29 General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership, Council of Europe, Cybercrime EAP, 2017, 8, <https://rm.coe.int/general-report-on-mapping-the-current-strengths-weaknesses-opportuniti/16808f1e1b> [08.03.2022].

30 *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, 2018, 102.

31 United States of America v. Kim Dotcom, (2012*),* US, №1:12CR3.

32 Explanatory Report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 29.

33 Law of Georgia on Electronic Communications, LHG, 02/06/2005, 8(2).

etc.[34] Maintaining a balance between the application of powers and respect for the rights of individuals is decisive for the admissibility of evidence before the court.[35]

3. Obtaining Computer Data in Georgian Criminal Procedure

According to the Criminal Procedure Code of Georgia, production order, an investigative measure provided for in article 18 of the Convention on Cybercrime, is known as the "request for a document or information".[36] Of course, the words "information and document" in the provision cover not every type of data, but only digital.

Under the first paragraph of 136 of the GECPC, "if there is a probable cause that the information or document important for the criminal case is stored in a computer system or on a computer data carrier, the prosecutor (a defence lawyer)[37] is authorized to file a motion with a court having jurisdiction over the investigative place, to issue an order requesting relevant information or document". The first part of this article deals with the production order for computer data in general. Herewith, it does not differentiate the types of data, which means the scope of the article is wide too. Therefore, the prosecutor and the defence attorney are eligible to order an individual in its territory to submit specified computer data stored in a computer system or data carrier that is in that person's possession or under the control.[38]

Regarding article 136(2), the computer data belongs to the service provider[39] and for a prosecutor to file a motion with a court, there must be probable cause that a person committed a crime through a computer system. As it seems, the second paragraph of the article is more specific and its scope limited. Particularly, the only authorized person to obtain subscriber data[40] is the prosecutor, but if he does not prove before the court that an individual uses a computer to commit a crime, he is not eligible to file a motion with a court for obtaining data.

The fourth paragraph of article 136 is critical. It specifies that the request for a document or information is subject to the same procedures that apply to covert investigative actions. First and foremost, it implies the limitation of its scope. To carry out the covert investigative actions an investigation should be initiated or criminal prosecution conducted due to an intentionally serious and/or particularly serious offence or to any of the offences defined in some articles of the

---

34 General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership, Council of Europe, Cybercrime EAP, 2017, 8, <https://rm.coe.int/general-report-on-mapping-the-current-strengths-weaknesses-opportuniti/16808f1e1b> [08.03.2022].

35 Ibid.

36 Criminal Procedure Code of Georgia, LHG, 09/10/2009.

37 The decision of the Constitutional Court of Georgia of January 27, 2017, on the case of Nadia Khurtsidze and Dimitri Lomidze v. Parliament of Georgia, №1/1/650,699 (in Georgian).

38 Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 29.

39 The term "service provider" encompasses a broad category of persons. It covers public and private entities which provide users the ability to communicate with one another. Also, the entities, who store or otherwise process data on behalf of the persons. It is not relevant whether the service is public or not, whether free of charge or for a fee. The term also includes closed communication systems.

40 Subscriber data - means any information, other than traffic or content data, by which can be established the type of communication service used, the technical provisions related thereto, and the period of time during which the person subscribed to the service, the identity of a user, mail or residential address, phone numbers, information on accounts and taxes, the location of the installed communications equipment, which is available based on a service contract or agreement.

Criminal Code of Georgia.[41] It is a different issue whether the production order is a covert investtigative action or not and if it has any sudden effect for the person,[42] but this notion of legislation is not in line with either the Convention on Cybercrime or international experience.[43]

To sum up, a production order has two dimensions. The first paragraph of article 136 enables both parties to compel a person in its territory to provide specified stored computer data, whereas the second paragraph of the article, enables the prosecutor to compel the service provider to submit subscriber data. Except for the fact that ongoing investigation and prosecution are essential conditions to use the investigative power, for obtaining subscriber data, the prosecutor must prove before the court that an individual uses a computer for committing a crime, otherwise he is not eligible to file a motion with a court for obtaining data.

Accordingly, it further limits the scope of article 136 of GECPC. So later we discuss the compliance issue of Georgian legislation to the Convention on Cybercrime based on its conditions and safeguards.

4. Compliance of Article 136 of GECPC with the Requirements of the Convention

We have discussed on requirements of the Convention and the legislation of Georgian criminal procedure. So now it is important to summarize some major issues. Primarily, if article 136 of GECPC is in-line with the Convention on Cybercrime, in particular with the scope of investigative measures and the conditions and safeguards necessary for the protection of fundamental human rights and freedoms. Article 14(2) of the Convention is formulated in such a way that the procedural powers, including production order, can be applied in the investigation of any crime. The only imperative request to limit the scope of procedural powers with the range of serious offences is in the case of real-time collection of content data, which presents the covert investigative action and highly interferes with the right to privacy. And regarding the production order which creates a legal basis for cooperation between LEA and individuals or service providers and represents an alternative and viable measure to lengthy or even disruptive search and seizure, limiting its scope with the range of offences is unjustified.

According to the above-mentioned limiting the scope of article 136 of GECPC is not only inconsistent with the requirements of the Convention, but also differs from the legislation of other states.[44] The scope of the provision is further limited by the reservation of an article of 136(2) "which can be applied only to crimes committed through a computer system". That's why, the Eastern Partnership recommended Georgia broaden the scope of article 136(2) to enable the collection of electronic evidence, including Subscriber data of any crime.[45] However, no relevant changes have been made in the legislation so far.

---

41 Criminal Procedure Code of Georgia, LHG, 143^3 (2a), 09/10/2009.

42 The Decision of the Investigative Collegium of the Tbilisi Court of Appeals of May 6, 2020, №1g/633-20, 3 (in Georgian).

43 Rules on Obtaining Subscriber Information, Adopted by T-CY at its 12th Plenary, 2014, France, 16-18, <https://rm.coe.int/16802e7ad1> [08.03.22].

44 *Marion L., Degani M.,* Making the Most of Your Statutory Electronic Evidence Toolbox, *Donovan J. (eds.),* Cyber Misbehavior, USA, 2016, 58-60. Criminal Procedure Code of Austria, 30.12.1975, Art. 76a, 90(7); Telecommunications Act 2003, 19.08.2003, Art. 92(3); German Code of Criminal Procedure, 07/04/1987, Art. 100j; Telecommunications Act (TKG), 06/22/2004, Art. 113(3).

45 *Dragicevic D., Juric M.,* Article 15 – Safeguards in the Eastern Partnership Region Prepared under the Cybercrime EAP, 2013, 44.

Also, it is important if national legislation, including article 136 of GECPC provides essential safeguards to protect individuals against arbitrary interference into the right and is consistent with the requirements of the Convention on Cybercrime. Under the national legislation, such safeguards are meeting formal and substantive prerequisites for obtaining stored computer data.[46] In particular, ongoing investigation of a criminal case, to file a motion under the probable cause,[47] Ex ante and Ex post (in case of the prosecutor) judicial supervision,[48] and the supervision of Personal Data Protection Service.[49] All of the above mentioned provide a solid guarantee for the proper protection of human rights.

Based on examining different issues, it became clear that in terms of protection of human rights, article 136 of GECPC is absolutely in compliance with the imperatives of international law. We find inconsistency in the scope of its operation, which evokes a significant barrier in practice.[50] Particularly with subscriber information, which plays a decisive role in crime detection worldwide, and should be subject to a wider scope than the interception of traffic and content data.[51] At the same time, it will be expedient to differentiate the types of data[52] for Article 136 and apply a distinct legal regime to them and determine the authorized persons for each of them. Moreover, the motions should be considered by the court by the procedure established by Article 112 of the present Code.

5. Conclusion

In the modern age, it is hard to imagine a crime that does not have a digital dimension.[53] Criminals often use technology and computer systems to commit crimes, communicate, launder money, attack criminal infrastructure, etc.[54] Traditional crime has also moved into the online. Illegal products are traded on the online black market. Sexual offences happen in front of a camera and then spread on the internet.[55]

---

46 The Decision of the Investigative Collegium of the Tbilisi Court of Appeals of May 6, 2020, №1g/633-20, 3 (in Georgian).

47 *Dragicevic D., Juric M.,* Article 15 – Safeguards in the Eastern Partnership Region Prepared under the Cybercrime EAP, Council of Europe, 2013, 38.

48 Conditions and Safeguards under Article 15 of the Convention on Cybercrime in the Eastern Partnership, Council of Europe, 2018, 44 <https://rm.coe.int/conditions-and-safeguards-under-article-15-of-the-convention-on-cyberc/16808f1e39> [08.03.22].

49 By the Decision of the Parliament of Georgia, the State Inspector's Service has been abolished from March 1, 2022. Instead, two agencies – The Special Investigation Service and The Personal Data Protection Service will be available.

50 The Decision of the Investigative Collegium of the Tbilisi Court of Appeals of October 20, 2016, №1g/1614-16, 9 (in Georgian). See also, The decision of the Investigative collegium of the Tbilisi Court of Appeals of December 25, 2019, №1g/2110-19, 4-5 (in Georgian); The Decision of the Investigative Collegium of the Tbilisi Court of Appeals of December 26, 2019, №1g/2133-19 (in Georgian).

51 Cybercrime Strategies, Procedural Powers and Specialized institutions in the Eastern Partnership Region – State of Play, Council of Europe, Bucharest, 2017, 18.

52 Electronically stored data can be: stored content data, traffic data, subscriber data, privileged data and etc.

53 *Casey E*., Foundations of Digital Forensics, Digital Evidence and Computer Crime, 3rd ed., USA, 2011, 3.

54 Ibid., 3-4.

55 The Internet Organised Crime Threat Assessment (IOCTA), Europol, 2015, 29. <https://www.europol.europa.eu/iocta/2015/resources/iocta-2015.pdf> [08.03.2022].

There is a positive aspect to the increasing use of technology by criminals, the involvement of computers in crime has resulted in an abundance of digital evidence that can be used to apprehend and prosecute offenders.[56] And since the main activity performed in the investigation is the collection of evidence to identify the suspect,[57] without effective, adapted, and developed procedural powers is impossible. So such kind of procedural measure for obtaining electronically stored data on a computer system, data storage medium, or cloud storage, is "Production Order", provided in Article 136 of GECPC. Therefore, to ensure its effectiveness, it is vital to bring the legal framework in line with International Law. An analysis of provisions of the Convention, domestic legislation, and their comparative analysis showed us that adequate protection of human rights is ensured while using the Production Order. Article 18 of the Convention is adequately implemented in national law. For example, it is implemented as a standalone procedural power, the national is law is precise and foreseeable and it contains safeguards against the arbitrary application.

However, the only requirement which Article 136 of GECPC does not meet is its scope, whereas Article 14(2) of the Convention is formulated in such a way that electronically stored data can be obtained in the investigation of any crime. And, under national law, its scope is limited by the range of offences.[58] Access to Subscriber Data is also limited, whereas, under the Convention for obtaining such data, a person doesn't need to commit a crime using a computer system.

According to the above-mentioned, to provide full compliance with the Convention on Cybercrime, it is essential to amend the law. In particular, to abolish procedures of covert investigative actions. And the court should consider the motion by the procedure established by Article 112 of GECPC. It will automatically expand its scope and electronically stored data will be available in the investigation of any crime. Moreover, the content of Article 136(2) should be broadened too and Subscriber Data must become available despite the fact a person commits the crime through a computer system or not. Except for the compliance with the requirements of International Law, it will improve the sound administration of Justice too.

Bibliography:

1. Criminal Procedure Code of Georgia, LHG, 09/10/2009.
2. Law on Electronic Communications, LHG, 02/06/2005.
3. Telecommunications Act (TKG), 06/22/2004.
4. Telecommunications Act 2003, 19.08.2003.
5. Convention on Cybercrime, Budapest, 23.11.2001.
6. Explanatory Report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001.
7. German Code of Criminal Procedure, 07/04/1987.
8. Criminal Procedure Code of Austria, 30.12.1975.
9. *Arnes A. (ed.),* Forensic Science, Digital Forensics, Norway, 2018, 1.
10. *Casey E*., Foundations of Digital Forensics, Digital Evidence and Computer Crime, 3rd ed., USA, 2011, 3-5, 29.

[56] *Casey E*., Foundations of Digital Forensics, Digital Evidence and Computer Crime, 3rd ed., USA, 2011, 5.

[57] *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (ed.)*, Norway, 2018, 95.

[58] Criminal Procedure Code of Georgia, LHG, 143^3 (2a), 09/10/2009.

11. *Dragicevic D., Juric M.,* Article-15 – Safeguards in the Eastern Partnership region, Council of Europe, 2013, 11, 38, 44.
12. *Flaglien O. A.,* The Digital Forensics Process, Digital Forensics, *Arnes A. (ed.),* Norway, 2018, 13.
13. *Kerr S.O.,* Searches and Seizures in Digital World, Harvard Law Review, Vol. 119, USA, 2006, 1.
14. *Marion L., Degani M.,* Making the Most of Your Statutory Electronic Evidence Toolbox, *Donovan J. (ed.),* Cyber Misbehavior, USA, 2016, 58-60.
15. *Schwerha J.J,* Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers" France, 2010, 4.
16. *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (ed.)*, Norway, 2018, 95, 99, 100-102.
17. Conditions and Safeguards under Article 15 of the Convention on Cybercrime in the Eastern Partnership, Council of Europe, 2018, 9, 44. <https://rm.coe.int/conditions-and-safeguards-under-article-15-of-the-convention-on-cyberc/16808f1e39> [08.03.22].
18. Cybercrime Strategies, Procedural Powers and Specialized institutions in the Eastern Partnership Region – State of Play, Council of Europe, Bucharest, 2017, 18.
19. General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership, Council of Europe, Cybercrime EAP, 2017, 7, 8, 13, <https://rm.coe.int/general-report-on-mapping-the-current-strengths-weaknesses-opportuniti/16808f1e1b> [08.03.22].
20. The Internet Organised Crime Threat Assessment (IOCTA), Europol, 2015, 29 <ttps://www.europol.europa.eu/iocta/2015/resources/iocta-2015.pdf> [08.03.22].
21. Rules on Obtaining Subscriber Information, Adopted by T-CY at its 12th Plenary, France, 2014, 16-18, <https://rm.coe.int/16802e7ad1> [08.03.22].
22. The Decision of the Investigative Collegium of the Tbilisi Court of Appeals of May 6, 2020, №1g/633-20 (in Georgian).
23. The Decision of the Investigative Collegium of the Tbilisi Court of Appeals of February 28, 2020, №1g/363-20 (in Georgian).
24. The Decision of the Investigative Collegium of the Tbilisi Court of Appeals of December 26, 2019, №1g/2133-19 (in Georgian).
25. The Decision of the Investigative Collegium of the Tbilisi Court of Appeals of December 25, 2019, №1g/2110-19 (in Georgian).
26. The Decision of the Constitutional Court of Georgia of January 27, 2017, on the case of Nadia Khurtsidze and Dimitri Lomidze v. Parliament of Georgia, №1/1/650,699 (in Georgian).
27. The Decision of the Investigative Collegium of the Tbilisi Court of Appeals of October 20, 2016, №1g/1614-16 (in Georgian).
28. United States of America v. Kim Dotcom, (2012), US, №1:12CR3.
29. K. U. v. Finland, [2009], ECHR, №2872/02.