https://doi.org/10.25143/socr.18.2020.3.081-088

Restrictions of Criminal Intelligence Measures in Law Enforcement Directive and Law on Criminal Intelligence of Lithuania

Ph.D. candidate ***Edgaras Markevičius***
Mykolas Romeris University, Lithuania
Public Procurement Department at Vilnius University, Lithuania
e.markeviciui@gmail.com

Abstract

Increasing use of technologies in the last decades has created an unprecedented opportunity to systematically collect and use a wide variety of data (including personal data) for different purposes. Information and data collected and processed with the help of new technologies is used not only for the purposes of natural and legal persons but also for various other purposes.

Intelligence services that ensure prevention of crime must perform their functions to ensure safety of public. When doing so, they use various means and methods of information collection, which help them to reach their goals. However, the means applied undermine and intensively restrict a person's right to private life.

Given that two legal interests compete during the application of criminal intelligence measures, i.e. the individual's right to privacy and ensuring of public security, the Author seeks to analyse their points of contact – restrictions of application of criminal intelligence measures, which in theory are designed to ensure the person's right to private life.

In this article, the Author analyses the restrictions on the application of criminal intelligence measures, which are present in international, Lithuanian legislation and compares them with relevant requirements set forth in the practice of European Union Court of Justice.

Keywords: criminal intelligence, right to private life, privacy, criminal intelligence measures, restrictions of criminal intelligence measures, Directive No. 2016/680.

Introduction

The last decades have been marked by extremely rapid technological progress that has affected numerous areas of our daily lives. One of the most affected areas is the social life of individuals – the means of working together, communicating with each other have changed dramatically. It is common to hold teleconferences rather than *live* meetings; make calls not via GSM, but video calls (using *Viber*, *Messenger*, *FaceTime* apps), etc.

The increasing use of technologies leads to an unprecedented opportunity to systematically collect and use a wide variety of data (including personal data) for different purposes. Information and data collected and processed with the help of new technologies is used not only for the purposes of natural and legal persons, but also for various other purposes.

These other purposes cover a wide range of societal priorities, ranging from crime prevention and pre-trial investigation to the provision of public administrative services by electronic means.

In the context of the widespread collection and use of personal data, ensuring the right to privacy becomes problematic. Even though individuals are guaranteed a right to privacy, it is necessary to bear in mind that the society also has a collective security interest.

Intelligence services that ensure the prevention of crime must perform their functions to ensure the safety of public. When doing so, they use the means and methods of information collection established in the Law on Criminal Intelligence of the Republic of Lithuania (hereinafter – the Law on Criminal Intelligence) [1], which help them to reach their goals. However, the means applied undermine and intensively restrict a person's right to private life [12, *902*].

It should be emphasised that secrecy is one of the essential principles of criminal intelligence [1, *Art. 3*, *p. 2*] and presumably a precondition for their successful operation. It is widely acknowledged that the effectiveness of criminal intelligence is inseparable from the secrecy of such actions and the fact that the data subject is not, in principle, aware that his or her personal data is being processed [14].

Therefore, two interests that are protected by law and extremely important for the society – the individual's right to private life and the public's common interest of safety – collide [10, *79*]. Although the right to privacy of individuals is significantly restricted by the use of the measures established by the Law on Criminal Intelligence by criminal intelligence institutions, the legislator also recognised the need to protect the rights of natural persons' (i.e. objects of criminal intelligence) in this process. To this end, the Law on Criminal Intelligence also *expressis verbis* establishes the obligation of criminal intelligence institutions to ensure the protection of individual's rights and legitimate interests [1, *Art. 3*, *p. 2*].

In order to prevent possible arbitrariness and disproportionate restrictions of the rights of persons (*inter alia* the right to private life) by criminal intelligence institutions,

the Constitution of the Republic of Lithuania [2], the Law on Criminal Intelligence and other legal acts establish restrictions on the application of criminal intelligence measures.

Given that two legal interests compete during the application of criminal intelligence measures, i.e. the individual's right to privacy and ensuring of public security, the Author seeks to analyse their points of contact – restrictions of application of criminal intelligence measures.

Therefore, in this article restrictions on the application of criminal intelligence measures, present in international and Lithuanian legislation have been analysed and compared with relevant requirements set forth in the practice of European Union Court of Justice (hereinafter – CJEU).

Restrictions on the use of criminal intelligence measures

The question of who has access to mass amounts of data collected and how they are to be used has become a central theme in the debate over transparency *vs* secrecy [13, *5*]. The Law on Criminal Intelligence entitles criminal intelligence entities to obtain information from any entity, to perform secret inspection of postal items and their documents, control and seize postal items, secret control of correspondence and other communications, access to personal accommodation, offices and other premises, closed areas, vehicles, as well as to inspect them [1, *Art. 6*, *p. 3*] etc.

Thus, criminal intelligence entities have the right not only to follow a person or listen on his or her conversations, but in principle to obtain information of interest to them from any entity by any available technical means. The legal doctrine confirms the position that the Law on Criminal Intelligence provides for a very wide range of different non-public investigative measures [7, *p. 275*].

Criminal intelligence activities and the exercise of these rights undoubtedly significantly interferes with the privacy of individuals, so the application of specific criminal intelligence measures cannot be left to discretion of criminal intelligence entities themselves.

The CJEU, in interpreting the right of law enforcement authorities to invade private life, has stated that "in order to ensure that access of the competent national authorities to retained data is limited to what is strictly necessary, it is, indeed, for national law to determine the conditions under which the providers of electronic communications services must grant such access. […] That national legislation must also lay down the substantive and procedural conditions governing the access of the competent national authorities to the retained data" [4, *para. 118*].

Thus, the case law of the CJEU and the legal doctrine [11, *2*] confirms that national law must provide procedural mechanisms to limit discretion of criminal intelligence entities. These mechanisms should enable to verify whether access to personal data is proportionate (i. e. strictly necessary). Therefore, the following provides analysis of

the Law on Criminal Intelligence, the Law Enforcement Directive [2], which reveals whether the legislation provides for significant procedural measures to ensure the balance between the right to privacy of individuals and the objective of criminal intelligence entities to prevent criminal activities.

First, data protection/national security laws as well as case law place special emphasis on independent oversight and transparency [8, *72*].

Constitution of the Republic of Lithuania [2, *Art. 22*, *para. 3*] provides that "information on the private life of a person may be collected only by a reasoned court decision and only in accordance with law". The same mandatory procedural requirement of prior administrative control has been established in case law by the CJEU, which states that access to retained data by competent national authorities must be subject to review "by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions" [5].

In this respect, it should be noted in particular that, although the Directive was adopted in 2016 (i.e. relatively recently), it does not implement the rulings in the abovementioned judgment of the CJEU [5], concerning mandatory prior control by a court or an independent administrative entity.

Article 28 para 1 of the Directive [3] specifies a mandatory procedure for *prior consultation* of the supervisory authority, the grounds of application of which are subjective. Furthermore, Article 47 para 3 of the Directive [3] governs the "effective *advisory* powers of those supervisory authorities to provide *advice to* the controller in accordance with the prior consultation procedure referred to in Article 28". Therefore, the "prior consultation" procedure specified in the Article 28 of the Directive [3] cannot be considered as a measure of prior control carried out by an independent entity, in the context of the CJEU case No. C-293/12 and C-594/12 [11, *15*].

The Law on Criminal Intelligence provides for a procedural restriction on application of criminal intelligence measures in Articles 9, 10 and 11. In Article 9 para. 1 of the Law on Criminal Intelligence it is established that the chairperson of a district court or a judge authorised by him or her shall make a ruling on motivated submissions of heads of criminal intelligence entities or their authorised deputies regarding receipt of information from economic entities, including electronic communications networks and/or service providers, the Bank of Lithuania, financial companies and credit institutions, etc. Meanwhile, Articles 10 and 11 of the Law on Criminal Intelligence establish that the chairpersons of regional courts or their authorised judges approve the use of technical means in a special manner, secret inspection of postal items and their documents, control and seizure of postal items, secret control of correspondence and other communications [1, *Art. 10*] and secret access to personal data, housing, official and other premises, closed territories, vehicles etc. [1, *Art. 11*].

Therefore, the Directive itself does not entail measures of prior independent control of application of criminal intelligence measures. However, Law on Criminal Intelligence provides for measures of prior administrative control of criminal intelligence measures [10, *13*], as required by the Article 22 of the Constitution and in line with the case law of the Court of Justice of the European Union.

Second, the Law on Criminal Intelligence provides for restrictions on the duration of criminal intelligence measures. Criminal intelligence measures which, by their nature, are continuous, e.g. tracking people, controlling the content of conversations etc., must be sanctioned for a specific time limit.

The European Court of Human Rights has held that it is reasonable for the relevant national authorities to regulate the overall duration of the interception, which are competent to issue and renew decisions, but only on condition that adequate safeguards are in place, such as (1) a period after which the measures authorised become obsolete, (2) the conditions under which the authorisation may be renewed and (3) the circumstances in which the authorisation is to be revoked [6, *para 250*].

Directive does not entail any regulation with regard to the maximum possible duration of the applied criminal intelligence measures. Art. 22 para. 3 of the Directive regulates that member states are free to set out the subject-matter and duration of the processing (i. e. application of criminal intelligence measures and duration thereof). This may be interpreted as respecting exclusivity and freedom of each EU member state; however, it fails to set even a low standard of protection of the right to privacy.

Art. 10 and 11 of the Law on Criminal Intelligence provide that specific criminal intelligence measures may be applied for a period not exceeding 3 months, but both articles entail the possibility of the duration extension of those criminal intelligence measures. In the first case, criminal intelligence tools can be renewed an unlimited number of times, each consisting of no more than 3 months, under the same conditions as they were granted, and in the second case, they may be extended for no more than 12 months (with certain exceptions).

Therefore, Articles 10 and 11 of the Law on Criminal Intelligence entail procedural restrictions on the duration of criminal intelligence measures, which in principle comply with the requirements of the legality of criminal intelligence periods established in the case law of the European Court of Human Rights (except for determining the circumstances in which applied criminal intelligence measures must be revoked). However, they can be easily manipulated by applying the extension period.

Thirdly, in accordance with the above-mentioned case law of the CJEU, criminal intelligence measures must be limited to what is strictly necessary to achieve the objective pursued [6, *para. 250*]. Therefore, the independent sanctioning of criminal intelligence (by courts or other independent bodies) must be aimed *inter alia* at verifying the proportionality of criminal intelligence.

The requirement of proportionality of the criminal intelligence measures applied is also directly enshrined in para 26 of the Directive preamble, which stipulates that

criminal intelligence activities must be a *proportionate* measure of a democratic society and Article 8 para. 1, which states that the processing of data [for the purposes of criminal intelligence] is lawful only if it is necessary and to the extent necessary for the competent authority to carry out its task under Article 1 para. 1 of the Directive.

Law on Criminal Intelligence set forth that each submission for the application of criminal intelligence measures to a district or regional court must indicate the *data and/or reasons* justifying the necessity to perform the specified actions and/or obtain the requested data and indicate the desired result [1, *Art. 9, p. 4, sp. 2*; *Art. 10, p. 4, sp. 3*; *Art. 11, p. 4, sp. 3*]. Given that the courts must make *justified* decisions [1, *Art. 9, p. 3*; *Art. 10, p. 3*], they ought to assess the measures and/or the information requested by the criminal intelligence subject, decide if it is objectively necessary and if the restriction to a person's privacy is applied proportionately.

Therefore, the Law on Criminal Intelligence does not directly establish the requirement of proportionality with reference to the criminal intelligence measures applied. However, bearing in mind (1) the obligation of criminal intelligence subjects to ensure the protection of individual rights and legitimate interests, (2) to state reasons for the criminal intelligence measures requests, and (3) the duty of courts to state reasons for orders granting such requests, the Criminal Intelligence Act should be considered to provide for measures aimed at ensuring the proportionality and necessity of applicable criminal intelligence.

Summarising the arguments given, it can be concluded that the Law on Criminal Intelligence provides for restrictions on the application of criminal intelligence measures, which in principle correspond to the restrictions established in the case law of the CJEU and the European Court of Human Rights. This sketches the current situation, where criminal law no longer communicates with its citizens, but rather threatens its enemies [9, *107*].

Conclusions

The case law of the CJEU confirms that national law must provide procedural mechanisms to limit discretion of criminal intelligence entities. Having analysed Directive and Law on Criminal Intelligence, a general conclusion can be drawn that the balance of the right to private life and the right to apply measures of criminal intelligence is tilted in favour of criminal intelligence subjects.

More detailed conclusions can be drawn:

1) the Directive does not entail measures of prior independent control of application of criminal intelligence measures; however, the Law on Criminal Intelligence provides for measures of prior administrative control of criminal intelligence measures;
2) the Directive does not entail restrictions on the duration of the criminal intelligence measures, whereas the Law on Criminal Intelligence does entail procedural

restrictions on the duration of criminal intelligence measures, which in principle comply with the requirements developed in the practice of the ECHR. However, they can be easily manipulated by the applying the extension period;

3) the Law on Criminal Intelligence and the Directive do not directly establish the requirement of proportionality with reference to the criminal intelligence measures applied. However, indirect references to the proportionality of the applied criminal intelligence measures are present in both legal acts and they may be aimed at ensuring the proportionality and necessity of applicable measures of criminal intelligence.

Kriminālās izlūkošanas pasākumu ierobežojumi likuma izpildes direktīvā un Lietuvas kriminālās izlūkošanas likumā

Kopsavilkums

Pieaugošā tehnoloģiju izmantošana pēdējās desmitgadēs ir radījusi nepieredzētu iespēju sistemātiski ievākt un izmantot ļoti dažādus datus (ieskaitot personas datus) dažādiem mērķiem. Informācija un dati, kas ievākti un apstrādāti ar jauno tehnoloģiju palīdzību, tiek izmantoti ne tikai fizisko un juridisko personu vajadzībām, bet arī dažādiem citiem mērķiem.

Izlūkošanas dienestiem, kas nodrošina noziedzības novēršanu, jāveic savas funkcijas, lai nodrošinātu sabiedrības drošību. To darot, viņi izmanto dažādus informācijas vākšanas līdzekļus un metodes, kas viņiem palīdz sasniegt savus mērķus. Tomēr izmantotie līdzekļi nereti grauj un intensīvi ierobežo personu tiesības uz privāto dzīvi.

Tā kā krimināllizlūkošanas pasākumu piemērošanā sacenšas divas likumīgas intereses – personas tiesības uz privātumu un sabiedrības drošības nodrošināšana –, autore cenšas analizēt to saskares punktu – krimināllizlūkošanas pasākumu piemērošanas – ierobežojumus, kas teorētiski ir izstrādāti, lai nodrošinātu personas tiesības uz privāto dzīvi.

Šajā rakstā autore ir izvēlējusies analizēt krimināllizlūkošanas pasākumu piemērošanas ierobežojumus: (1) obligāta iepriekšēja kontrole (sankcija) noteiktam krimināllizlūkošanas pasākumam, ko veic tiesa vai neatkarīga administratīva vienība; (2) krimināllizlūkošanas pasākumu ilguma ierobežošana; (3) krimināllizlūkošanas pasākumu samērīgums.

Rakstā secināts, ka, kaut arī šie kriminālās izlūkošanas piemērošanas ierobežojumi likuma izpildes direktīvā parasti nepastāv, tie ir ietverti Lietuvas Republikas likumā par kriminālo izlūkošanu. Tomēr ar tiem var viegli manipulēt un tie nenodrošina tiesības uz privātās dzīves efektīvu aizsardzību.

Atslēgvārdi: kriminālā izlūkošana, kriminālās izmeklēšanas pasākumi, kriminālās izmeklēšanas pasākumu ierobežojumi, tiesības uz privāto dzīvi.

Literature

1. Law on Criminal Intelligence of the Republic of Lithuania (Žin., 2012, Nr. 122-6093).
2. Constitution of the Republic of Lithuania (Lietuvos Aidas, Nr. 220; 1992, Nr. 33-1014).
3. Directive No. 2016/680 of the European Parliament and of the Council of 27 April 2016 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, and repealing Council Framework Decision 2008/977/JHA.
4. Judgment of the Court of Justice of the European Union in 2016. December 21 decision in case No. C-203/15 and C-698/15 (*Tele2 Sverige* case).
5. Judgment of the Court of Justice of the European Union in 2014. April 8 decision in case No. C293/12 and C594/12 (*Digital Rights Ireland* case).
6. European Court of Human Rights decision of 2015 December 4 in case No. 47143/06 (*Roman Zakharov v. Russia*).
7. Ažubalytė, R. (2019). "Restricting the life of a Private Person by Secret Means: the Problem of (in) Quality Law". *Jurisprudence*, *26*(2).
8. Ryngaert, Cedric M. J., van Eijk, Nico A. N. M. (2019). "International cooperation by (European) security and intelligence services: reviewing the creation of a joint database in light of data protection guarantees", *International Data Privacy Law*, *9*(1).
9. Derencinovic D., Getos A. M. (2007). "Cooperation Of Law Enforcement And Intelligence Agencies In Prevention And Suppression Of Terrorism – European Perspective". *Revue Internationale de Droit Penal*, 2007, *78*(1).
10. Gutauskas, A. (2019). "Kriminalinė žvalgyba ir privatus žmogaus gyvenimas (Eng. Criminal intelligence and private human life)". *Teisė*, No.113.
11. Jasserand C. (2018). "Law Enforcement Access to personal Data Originally Collected by Private Parties: Missing Data Subjects' Safeguards in Directive 2016/680". *University of Groningen Faculty of Law Research Paper*, No. 25.
12. Villani, S. (2018). "Some Further Reflections on the Directive (EU) 2016/681 on PNR Data in the Light of the CJEU Opinion 1/15 of 26 July 2017". *Revista de Derecho Político*, No. 101.
13. Rittberger, B., Goetz, K. H. (2018). "Secrecy in Europe", *West European Politics*, February..
14. 2019 June 5th Hearing information of the Parliamentary Control Commission on Criminal Intelligence. (2019.06.05). Available from: http://www.infolex.lt/portal/start.asp?act=news&Tema=1&Str=66392.