E-ISSN 3008-6299

THE CRIMINAL SCIENCES JOURNAL
TCSJ
"AL.I. CUZA" POLICE ACADEMY

SOME CONSIDERATIONS REGARDING SPECIAL METHODS OF SURVEILLANCE OR INVESTIGATION OF AN INFORMATION SYSTEM

Gianina-Anemona Radu[1]
Marius Popa[2]

Abstract: *In the digital age, criminal activities often leave a trail of electronic evidence, necessitating sophisticated methods of surveillance and investigation within computer systems. As technology advances, criminals adapt, making it imperative for law enforcement agencies to employ cutting-edge techniques. This research explores the methods employed in the surveillance and investigation of computer systems in the context of criminal investigations, examining their significance and challenges.*

The administration of evidence in the field of investigating corruption offenses and offenses assimilated to corruption presents specific particularities, which has caused the classic investigative procedures used by law enforcement authorities to become effectively inefficient, inappropriate, and even unrealistic.

The present study aims to identify the main characteristics of surveillance measures and analyze their role in the criminal process, as well as the limitations in their practical application, both in terms of legislation and their inadequate understanding by authorities. Another element the analysis focuses on is the practical aspects involved in implementing such measures, the means that state authorities can use to obtain data, and the rules regarding the security, maintenance, and certification of data authenticity.

This aspect has been identified and appreciated in the sense of the state's incapacity in the face of the multiplication and instantaneity of fraudulent financial transactions. For this reason, it has been considered that for specific forms of criminality, it is necessary to act with special means of investigation.

Taking into account this aspect, investigating and researching such offenses is very difficult, requiring ingenious methods, creativity, and inventiveness from law enforcement authorities. It necessitates the use of special surveillance or investigative methods, such as: intercepting communications and any type of remote communication, video or audio surveillance, photography, technical means for location or tracking, the use of undercover investigators and collaborators, as well as authorized participation in certain activities.

Keywords: *monitoring; computer system; surveillance; investigation; electronic evidence*

Overview

In our increasingly interconnected world, the effective functioning of information systems is critical for various aspects of daily life, ranging from communication and commerce to national security. However, the rise of cyber threats has necessitated the development and application of special methods of surveillance and investigation to safeguard these systems.

[1] Lecturer, PhD, Police Faculty, "Alexandru Ioan Cuza" Police Academy, Bucharest, 1-3 Aleea Privighetorilor, District 1, Bucharest, email: gianina.radu@academiadepolitie.ro.
[2] Prosecutor, PhD, National Anticoruption Directorate, Bucharest, 79-81 Știrbei Vodă Street, 010106, email: popa_marius_petrica@mpublic.ro

Copyright: © 2023 by the authors.
Open access publication under the terms and conditions of the
Creative Commons Attribution (CC BY) license
(https://creativecommons.org/licenses/by/4.0/)

One fundamental consideration in employing special methods of surveillance or investigation is the establishment of a robust legal framework. Adherence to existing laws is essential to safeguard individual rights to privacy and ensure due process. Authorities must obtain proper authorization before employing these methods, and oversight mechanisms should be in place to prevent misuse and guarantee lawful implementation.

The principle of necessity and proportionality is paramount in justifying the use of special methods. These techniques should only be employed when absolutely necessary to achieve a legitimate objective, and their application should be proportionate to the level of threat or risk being addressed. Striking a balance between the need for security and protecting individual privacy is crucial for ethical and legal considerations.

A transparent approach to the application of special methods fosters public trust and ensures accountability. While national security concerns may limit the extent of transparency, efforts should be made to provide information on the purpose, scope, and limitations of these methods. Transparency helps maintain a delicate equilibrium between safeguarding sensitive information and maintaining public confidence in the actions of those responsible for surveillance.

As special methods involve the collection and analysis of sensitive data, robust data protection measures are imperative. Safeguarding the confidentiality, integrity, and availability of information ensures that individuals' privacy is respected and that the data collected is used solely for its intended purpose. Striking the right balance between security and privacy requires a meticulous approach to data protection.

Given the transnational nature of cyber threats, international cooperation is essential in effectively countering them. Collaborative efforts between nations can enhance the capabilities of special methods while respecting the sovereignty and legal frameworks of each involved party. Shared intelligence and best practices contribute to a more comprehensive and effective global cyber security strategy.

The individuals involved in conducting special methods must possess a high level of technical expertise. Understanding the intricacies of information systems, encryption, and other relevant technologies is vital for the successful and responsible implementation of these methods. Ongoing training and development are necessary to keep pace with evolving technological landscapes.

Efforts should be made to minimize the impact on individuals not implicated in the investigation. Limiting the scope of surveillance and ensuring that only necessary information is collected and retained are crucial steps in preventing undue intrusion into the lives of innocent parties. Striking a balance between the investigative needs and the protection of individual rights minimizes collateral damage.

The use of special methods should be subject to periodic review to assess its effectiveness, legality, and impact. These reviews provide an opportunity for adjustments and improvements based on lessons learned. Regular evaluations contribute to the refinement of methods, ensuring they remain aligned with ethical and legal standards.

At the core of any decision to employ special methods is a consideration of ethical principles. The potential benefits of enhanced security must be weighed against the potential harm to individuals' rights and freedoms. Ethical considerations guide decision-makers in navigating the complexities of surveillance and investigation, ensuring that the methods chosen are justifiable and morally sound.

General Aspects Regarding the Special Method of Monitoring Access to an Information System

The management of evidence in the field of investigating corruption offenses and offenses related to corruption presents specific particularities, which have rendered the classical investigative procedures used by law enforcement agencies effectively inefficient, inappropriate, and even unrealistic.

This aspect has been identified and recognized in the sense of the state's inability to cope with the proliferation and immediacy of fraudulent financial affairs. For this reason, it has been considered necessary to employ special means of investigation for these special forms of criminality.

The specificity of corruption offenses also stems from the fact that, most often, they are committed in total secrecy, in a covert manner. The only individuals aware of their commission are typically the perpetrator of the bribery/influence trafficking offense and the perpetrator of the correlative offense/purchase of influence, conditioned, of course, by the special status of the offender, who must be a "public official" (Article 175 of the Criminal Code) or a "private official" (Article 308 of the Criminal Code), (Croitoru, S., 2020)[1].

Given this aspect, the investigation and research of such offenses are very challenging, requiring ingenious methods, creativity, and inventiveness on the part of law enforcement agencies. This involves the use of special methods of surveillance or investigation, such as: intercepting communications and any type of remote communication, video or audio surveillance, photography, location or tracking through technical means, the use of undercover investigators and collaborators, as well as authorized participation in certain activities.

The Code of Criminal Procedure has regulated certain evidentiary procedures in Article 138, and these can be divided into two categories:

- a) Surveillance methods - those provided for in Article 138 paragraph (1) letters a)-e);
- b) Investigation methods - those provided for in Article 138 paragraph (1) letters f)-j).

The fundamental difference between the two categories - surveillance and investigation - lies in the fact that the former are carried out in real-time; law enforcement agencies must receive information while the activities are ongoing. This fact is reinforced by the verbs used to define the activity: interception, access, surveillance, location, tracking, as well as obtaining.

On the other hand, investigation methods are evidentiary procedures through which law enforcement agencies receive information about activities after they have taken place, having, in some cases, the possibility to examine the material object - for example, postal referrals, obtaining data generated or processed by providers of public electronic communications networks or providers of electronic communications services intended for the public (Volonciu, N. 2015)[2].

Aspects encountered in judicial practice

I. In the Criminal Procedure Code, the special method of monitoring access to an information system is regulated.

Relevant legal provisions: Law no. 135/2010 regarding the Criminal Procedure Code

Article 138.

General provisions

[1] Croitoru Sandina Mariana, *Some special measures and methods of investigation applicable in the case of offenses related to corruption*, Romanian Journal of Jurisprudence, Issue 5, 2020;

[2] Nicolae Volonciu, The New Criminal Procedure Code Commented, Second Edition, Hamangiu Publishing House, 2015, Article 139.

"(1) The following are special methods of surveillance or investigation: (...); b) access to an information system;

(...).

(3) Access to an information system means the penetration into an information system or data storage medium either directly or remotely, through specialized programs or through a network, for the purpose of identifying evidence.

(4) An information system means any device or set of interconnected devices or devices in a functional relationship, of which one or more ensures the automatic processing of data, with the help of a computer program.

(5) Information data means any representation of facts, information, or concepts in a form suitable for processing in an information system, including a program capable of causing a system to perform a function."

In judicial practice[1], the question has arisen as to whether the evidentiary procedure of accessing an information system can be used when (i) the information support is physically held by the law enforcement body, or if this evidentiary procedure only allows for (ii) remote penetration into such a system for monitoring/surveillance purposes.

We believe that the evidentiary procedure of accessing an information system can be used in both situations, where the information support is physically held by the law enforcement body and when remote penetration into such a system occurs, for the following reasons:

From the analysis of the provisions of Article 138 paragraph (1) letter b) of the Criminal Procedure Code, it is evident that access to an information system is a special surveillance method that allows both remote access and direct, immediate access to the information system[2].

Access involves examining the resources of the information system to discover information existing therein or those generated during technical surveillance or to obtain a representation of the system. Penetration can be carried out either directly – physical contact directly with the information system or the data storage medium – or remotely (through an internet connection or by accessing a wireless network, under conditions of confidentiality). Physical access takes place where the information system or the data storage medium is located (Udroiu, M., 2018)[3].

Therefore, given that, by law, reference is made, on the one hand, to remote access and, on the other hand, to direct, immediate access, a restriction of the scope of application of this surveillance measure is not possible. The legislator does not distinguish within the provisions of Article 138 paragraph (3) of the Criminal Procedure Code, whether the information support is in the possession of the law enforcement body or at a distance, and any other interpretation would mean adding to the law.

According to the provisions of Article 168 paragraph (1) of the Criminal Procedure Code, digital search represents the procedure for investigating, discovering, identifying, and gathering evidence stored in an information system or data storage medium, carried out through technical means and appropriate procedures to ensure the integrity of the information contained therein. According to Article 168 paragraph (2) of the Criminal Procedure Code, a digital

[1] The Court of Appeal Pitești - Penal Section and for Cases Involving Minors and Family in Case No. 2485/90/2022/a1.

[2] This conclusion arises from reading Article 138 paragraph 1 letter b), which defines access to an information system as the penetration into an information system (any device or set of interconnected devices or devices in a functional relationship, of which one or more ensures the automatic processing of data) or a data storage medium, either directly or remotely, through specialized programs or through a network, for the purpose of identifying evidence.

[3] Mihai Udroiu, *Criminal Procedure, General Part*, C.H. Beck Publishing House, Bucharest, 2018, p. 447.

search is ordered in all cases where the investigation of an information system or a data storage medium is necessary for the discovery and collection of evidence.

Thus, while digital searches are used to obtain pre-existing data located in an information system already in the custody and under the control of the judicial authority, in the case of information represented by the content of email or VoIP messages stored on information systems not in the possession of judicial authorities, the evidentiary procedure to obtain this data is represented by access to an information system. In this situation as well, the issuance of a warrant by the judge for rights and freedoms is necessary, with the data being obtained using specific technical means, with or without the assistance of internet or communications service providers. What differentiates access to an information system from a digital search is that, while in the case of a digital search, the information is already present in the searched information system, referring to data from the past in relation to the date of issuing the digital search warrant, through access to an information system, both data on communications carried out before the date of issuing the technical surveillance warrant and data on communications after that date, made between the moment of issuing the technical surveillance warrant and the expiration date, can be obtained[1].

In conclusion, we believe that a clear distinction must be made between the two evidentiary procedures, digital search and access to an information system. These procedures are subject to different rules that determine different ways of action by judicial authorities. While a digital search requires physical contact with the information system being searched, access to an information system can be carried out both in the presence and absence of the system.

We also want to emphasize that we cannot consider technical surveillance in the form of access to an information system and digital search as alternative tools of criminal investigation that a prosecutor can access. This is because technical surveillance in the form of access to an information system is a secret investigative method, and a digital search does not possess this characteristic.

II. Another issue raised in judicial practice was the following: to what extent can data generated or processed by Facebook or other social networks be requested under Article 152 paragraphs (1)-(3), referring to Article 138 paragraph (1) letter j) of the Criminal Procedure Code?

We believe that such a request is not permissible because the social network is not a provider of publicly available communication services[2] or a provider of public electronic

[1] Decision no. 56/2023, High Court of Cassation and Justice, Bucharest, www.iccj.ro

[2] In Government Emergency Ordinance No. 111/2011, Article 4, point 9, the electronic communications service is defined as: a service, usually provided for a fee, through electronic communications networks, which includes the following types of services: a) internet access service, as defined in Article 2 paragraph 2 point 2 of Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 on measures to ensure open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, and Regulation (EU) No 531/2012 on roaming on public mobile communication networks within the Union, published in the Official Journal of the European Union, Series L, No 310 of 26 November 2015, with subsequent amendments and supplements; b) interpersonal communication service; and c) any other services that consist entirely or mainly of the transmission of signals through electronic communications networks, such as transmission services used for providing services between devices, machine-to-machine, and for the transmission of audiovisual media services.
Services through which the content of information transmitted through networks or electronic communications services is provided or editorial control over this content is exercised, and information society services, as defined in Article 1 point 1 of Law No. 365/2002 on electronic commerce, republished, with subsequent modifications, which do not consist entirely or mainly of the transmission of signals through electronic communications networks, are not considered electronic communications services.-to-machine, and for the transmission of audiovisual media services.

communication networks[1]. It only offers services where the content of the information comes from a third party and is delivered by the producer through an internet service provider, which is not responsible for the content of the information, nor capable of controlling the display of content, compliance with copyright, and redistribution of content.

On the other hand, the retention of information data, as provided by Article 154 of the Criminal Procedure Code, applies to information data, including data related to informational traffic, stored through an information system that is in the possession or under the control of other individuals, not just providers of public electronic communication networks or providers of publicly available communication services. This latter category includes social networks such as Facebook. Consequently, the prosecutor, through an ordinance, will order the retention of information data, and subsequently, with the authorization of the judge for rights and freedoms, will request the transmission of the retained data in accordance with the law [Article 154 paragraph (6) of the Criminal Procedure Code].

To the extent that law enforcement authorities wish to request certain data exclusively held by Facebook (date of account opening) using mechanisms of judicial cooperation in criminal matters, we believe that the approval of the initiative by a judge for rights and freedoms is required. This is because the use of the European Investigation Order mechanism entails compliance with the procedure provided by the law of the requesting state to obtain the respective evidence, specifically the authorization of the judge for rights and freedoms.

In the case where the data is made available to the public by the account holder, no authorization is required for the probative exploitation of this data, a situation similar to accessing a website. Thus, it is sufficient to draw up an official record to which a screenshot of the computer screen will be attached.

Additionally, we consider that the provisions of Article 154 of the Criminal Procedure Code do not cover the real-time monitoring of a Facebook account; for such an operation, authorization to access an information system is required [Article 138 paragraph (1) letter b) of the Criminal Procedure Code][2].

The applicable sanction in the case of evidence administration with a violation of the above-mentioned aspects

Doctrine is almost unanimous regarding the sanction that applies in the case of excluding evidence obtained illegally, in that it involves absolute nullity as regulated in the provisions of Article 281 of the Criminal Procedure Code.

We align ourselves with the opinion that the only true sanction is nullity, with other sanctions (forfeiture, inadmissibility, exclusion) having a specific nature; one could even argue that exclusion complements nullity. In this regard, other authors have pointed out that the sanction of exclusion is derived from the sanction of nullity, and its applicability is limited to establishing the existence of a case of express absolute nullity (Article 281 of the Criminal Procedure Code) or meeting the cumulative conditions of relative nullity (Article 282 of the Criminal Procedure Code).

Therefore, in the procedure for verifying the legality of evidence in a corruption-related criminal case, a procedure provided for in Article 342 of the Criminal Procedure Code, the

[1] Provider of electronic communications services - a person whose activity consists, wholly or in part, in providing an electronic communications service; public electronic communications network - an electronic communications network that is used, entirely or mainly, for the provision of publicly available electronic communications services and allows the transfer of information between the network's terminal points; - both definitions are found in Government Emergency Ordinance No. 111/2011, Article 4, points 94 and 10.

[2] High Court of Cassation and Justice, Minutes of the Meeting of the Presidents of the Criminal Sections of the High Court of Cassation and Justice and the Courts of Appeal, Bucharest, May 16-17, 2019, Pandectele Române no 6/2020, www.inm-lex.ro

judge has the obligation to sanction, in all cases where a violation of the law in the ordering, obtaining, and administration of evidence is found, the manner in which the chosen evidentiary procedures by investigators were administered. The sole sanction is nullity, resulting in the physical exclusion of all illegally administered means of proof.

Conclusions

The effective deployment of special surveillance or investigation methods requires a solid legal framework. Clear and comprehensive legal provisions are essential to delineate the scope, limitations, and procedural safeguards, ensuring the methods are applied within the bounds of the law.

Striking a delicate balance between the legitimate need for security and the protection of individuals' privacy is paramount. Any use of special methods must be guided by a commitment to respecting individual rights, and robust privacy safeguards should be in place to prevent unwarranted intrusion.

Given the rapid pace of technological advancements, law enforcement agencies must continuously adapt their surveillance methods. Staying abreast of changes in information systems is crucial for the effective investigation of cyber threats and criminal activities.

Maintaining the integrity of evidence collected through special methods is essential for legal proceedings. Stringent protocols and practices should be in place to guarantee that the evidence is reliable, untampered, and admissible in court.

The successful application of special methods requires law enforcement personnel to undergo specialized training. Proficiency in understanding the intricacies of information systems is crucial to conducting lawful and effective investigations.

Judicial oversight serves as a crucial safeguard against abuse. Requiring authorization from a judicial authority before employing special methods ensures accountability and prevents unwarranted intrusion into individuals' privacy.

Cyber threats often transcend national borders. Effective investigation of information systems requires international collaboration and cooperation to address challenges associated with jurisdictional boundaries and the global nature of cybercrime.

The dynamic nature of cyber threats demands an agile and adaptable response. Special surveillance methods should be flexible enough to address emerging threats, and law enforcement agencies should continuously update their strategies to effectively combat evolving cybercriminal tactics.

REFERENCE

Croitoru Sandina Mariana, *Some special measures and methods of investigation applicable in the case of offenses related to corruption*, Romanian Journal of Jurisprudence, Issue 5, 2020;

Mihai Udroiu, *Criminal Procedure, General Part*, C.H. Beck Publishing House, Bucharest, 2018;

Nicolae Volonciu, *The New Criminal Procedure Code Commented*, Second Edition, Hamangiu Publishing House, 2015