DOI https://doi.org/10.30525/978-9934-26-686-7-1

THE CONSTITUTIONAL BOUNDARIES OF DIGITAL EVIDENCE: INTRUSIVE MEASURES, CYBERSECURITY AND NATIONAL SECURITY IN ROMANIA

Safta, M., Stanciu, C. A. M.

INTRODUCTION. THEORETICAL FRAMEWORK

In any legal system, evidence constitutes the cornerstone of the administration of justice. The establishment of truth represents the ultimate objective of jurisdictional proceedings, while the legitimacy of judicial decisions depends directly upon the legality and integrity of the methods employed in its ascertainment. From this perspective, evidentiary matters cannot be reduced merely to their effectiveness in proving factual circumstances; rather, they inherently engage considerations relating to the protection of fundamental rights and freedoms. Within a state governed by the rule of law, judicial truth cannot be pursued at any cost. Accordingly, evidentiary mechanisms must remain strictly subject to the principles of legality, necessity, and proportionality.

The rapid development of information and communication technologies has profoundly reshaped the law of evidence, positioning digital evidence at the core of contemporary procedural systems. As social and economic interactions increasingly unfold in digital environments, they inevitably leave behind informational traces–such as traffic, location, identification, and content data–that may be collected and processed by public authorities. This expanded technological capacity significantly enhances the state's ability to access intimate aspects of individual life, thereby requiring a careful constitutional reassessment of the limits of public intervention.

Within the framework of criminal proceedings, this issue finds its most profound expression through technical surveillance measures, which represent some of the most intrusive instruments available to criminal investigation bodies. The interception of communications, access to traffic and location data, or the use of technical infrastructure to collect information involve direct interferences with the right to intimate, family, and private life and the secrecy of correspondence, guaranteed by the Romanian Constitution under Article 26 and Article 28. The expansion of the state's technological capabilities thus generates a structural tension between the necessity of combating crime–including cybercrime–and the constitutional obligation to protect the substance of fundamental rights.

Beyond the sphere of criminal proceedings, however, the issue of digital evidence and technical surveillance transcends the strictly judicial framework, fitting into a broader dimension–that of cybersecurity and, implicitly, national security. In the context of hybrid threats, cyberattacks, and the vulnerabilities of critical infrastructures, the collection and processing of data acquire a strategic dimension, transforming surveillance from a procedural tool into a mechanism for protecting the fundamental interests of the state. This functional expansion, however, raises

additional concerns regarding the delimitation of the authorities' competences and the constitutional standards applicable to interferences with fundamental rights.

Within this framework, the present research seeks to analyse–by capitalizing on the evolution and chronological development of the case law of the Constitutional Court of Romania (CCR)–three distinct yet interconnected dimensions of the issue: the general dimension of digital evidence, its application in criminal proceedings through technical surveillance measures, and, finally, its extension into the field of national security. The analysis will highlight the manner in which constitutional case law has progressively developed a coherent set of standards concerning the legality, foreseeability, necessity, and proportionality of interferences, in a judicial dialogue with the case law of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR). In accordance with the relevant constitutional provisions–namely Articles 20 and 148–the research will further consider the interpretation of fundamental rights in harmony with the international treaties Romania is a party to and in compliance with the principle of the primacy of European Union law.

Without claiming to provide an exhaustive analysis of an issue characterized by growing normative density and technological dynamism, the proposed analysis seeks to outline the constitutional landmarks of surveillance in the digital age and to highlight the contribution of Romanian case law to the configuration of a genuine digital constitutionalism, situated at the intersection of fundamental rights protection and security imperatives in a democratic society.

I. Data Retention and Structural Surveillance. Constitutional and European Standards

1. The Unconstitutionality of the National Transposition of Directive 2006/24/EC ("Big Brother")

Without providing extensive detail on this case law within the current framework, given its comprehensive presentation in other studies[1], we mention it as a landmark not only at the national level but also at the level of the European Union (EU). This includes its role in the dialogue between constitutional courts and the subsequent effects regarding the shaping of fundamental rights protection standards.

From the perspective of EU law, this moment was one of tension between Romania's obligation to comply with the European legal order (the transposition of a directive) and the obligation to adhere to the fundamental rights protection standards enshrined in the Romanian Constitution. This tension arose from the intrusive nature of the measures established by the European act in question, namely Directive 2006/24/EC (the so-called "Big Brother Directive")[2]. Essentially, it imposed a

[1] C. F. Stoica, M. Safta, '*Theoretical and practical issues relating to the right to the protection of personal data*' (2015) 5(2), Juridical Tribune – Review of Comparative and International Law 88–10, available at https://www.tribunajuridica.eu/arhiva/An5v2/6%20Stoica.pdf.

[2] Directive 2006/24/EC (Data Retention Directive).

general obligation on Member States to store traffic and location data held by telephone and internet service providers for a specified period, for the purpose of combating serious crime and terrorism. However, the manner in which this obligation was regulated faced critical positions, both publicly and in legal literature, where it was argued that it permitted generalized and undifferentiated surveillance, establishing what Stefano Rodotà named "total surveillance," which alters the balance of power between the state and the individual. In his view, the functioning of the rule of law is based on a clear rule: state power must be transparent, while the individual's life must be opaque[3]–more precisely, the requirements of the right to privacy must be respected. The same thesis is developed in legal doctrine by Orla Lynskey, who states that generalized data retention policies undermine the foundation of liberal democracy, transforming citizens into subjects of constant monitoring[4]. The issue of undifferentiated data collection lies in the creation of an informational asymmetry between the state and the citizen. In the absence of robust safeguards, the state's control capacity is liable to exceed the requirements of the proportionality test. Lynskey emphasizes that data protection is more than an individual right, being a structural component of the rule of law.

The Directive in question was transposed in Romania through Law No 298/2008[5], which was challenged before the CCR and found unconstitutional by Decision No1.258/2009[6]. While the Constitutional Court acknowledged, in principle, "*the legislator's possibility to limit the exercise of certain fundamental rights and freedoms, as well as the necessity of regulating measures that provide law enforcement authorities with specific duties in criminal investigation with efficient and adequate instruments for preventing and uncovering terrorism-related crimes, in particular, as well as serious crimes*", it emphasized the imperative of respecting "*all the safeguards that such an interference requires*." Subsequently, the Romanian legislator adopted Law No 82/2012[7], attempting to remedy the identified unconstitutionality flaws and to establish new standards for the protection of personal data. However, this law was also found unconstitutional by Decision No 440/2014[8], which reaffirmed the necessity of real, not illusory, safeguards for the fundamental rights affected by the transposition of the directive. We shall briefly highlight below these safeguards as they emerge from the aforementioned decisions.

[3] S. Rodotà, *Technopolitics. Democracy and the New Communication Technologies*, 2nd Edition, Laterza Publishing, Rome-Bari, 2004, pp. 3–15.

[4] O. Lynskey, The Foundations of EU Data Protection Law, Oxford University Press, Oxford, 2015, pp. 175-180.

[5] Official Gazette no. 780 of 21 November 2008.

[6] Official Gazette no. 798 of 23 November 2009.

[7] Official Gazette no. 211 of 25 March 2014.

[8] Official Gazette no. 883 of 9 November 2014.

2. Constitutional Safeguards Governing Data Retention and Access

2.1. Quality of Law

The Court emphasized that the limitation of the exercise of fundamental rights (in this case, the right to intimate life, the secrecy of correspondence, and the freedom of expression) must occur in a clear, predictable, and unequivocal manner, so as to eliminate, as far as possible, the possibility of arbitrariness or abuse by the authorities in this field. However, "*the lack of precise legal regulation, which would exactly determine the scope of those data necessary for identifying natural or legal persons who are users, opens the possibility for abuses in the retention, processing, and use of data stored by providers of publicly available electronic communications services or public communications networks*". In the same logic, the Court held that the legislator does not define what is meant by "*threats to national security*"; thus, in the absence of precise delimitation criteria, various ordinary, routine actions, information, or activities of natural and legal persons can be arbitrarily and abusively assessed as being of the nature of such threats. Consequently, "*the subjects of the law may be included in the category of suspected persons without knowing this and without being able to prevent, through their conduct, the consequence of applying the rigors of the law*".

With reference to the same constitutional requirements, the Court sanctioned the ambiguous terminology, noting, *inter alia*, that Article 1 (2) of the law extended the retention obligation to "*related data necessary for identifying the subscriber*", without, however, providing a legal definition of this concept. In the absence of an explanation of what the legislator understands by "*related data*", the legal provision failed to establish with precision the scope of information subject to storage.

2.2. The State's Negative Obligation to Refrain from Interference with the Exercise of Rights or Freedoms

The Court found that the law established an obligation for providers of publicly available electronic communications services or public communications networks to retain data continuously for a period of 6 months from the moment of interception, thereby depriving the principle of personal data protection and confidentiality of its substance (enshrined at the legislative level by Law No 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data, as well as Law No 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector). The excessive nature of these limitations was further highlighted by invoking the provisions of Article 91^1 of the Code of Criminal Procedure, regarding which the Court held that it "*respects the exceptional nature of audio or video interceptions and recordings, as these are allowed under certain strict conditions, from the moment of obtaining a reasoned authorization from a judge, for a limited period of time which cannot exceed, in total, for the same person and the same act, 120 days*". The Court concluded that the regulation of a positive obligation concerning the continuous limitation of the exercise of the right to intimate life and the secrecy of correspondence "*causes the very essence of the right to disappear, by removing the safeguards regarding its exercise*".

2.3. Proportionality of the Interference

2.3.1. The Unconstitutionality of General and Continuous Data Retention

In essence, the Court emphasized that it is not the justified use, under the conditions regulated by Law No 298/2008, that in itself unacceptably prejudices the exercise of the right to intimate life or the freedom of expression, but rather the continuous, generally applicable legal obligation to store data–thus, an interference lacking proportionality. Storage affects the subjects of the law "*regardless of whether or not they have committed criminal acts or whether or not they are the subject of criminal investigations, which is likely to overturn the presumption of innocence and to transform a priori all users of electronic communications services or public communications networks into persons suspected of committing terrorism-related or serious crimes*".

2.3.2. Sanctioning the Absence of Effective Judicial Oversight of Access to Retained Data

While Decision No 1.258/2009 primarily examined the bulk collection of data, Decision No 440/2014[9]–which sanctioned a new attempt to transpose the same aforementioned Directive–focused particularly on the access to the collected information. The Court found that "*requests for access to retained data for the purpose of their use as provided by law, formulated by state authorities with duties in the field of national security, are not subject to authorization or approval by a court of law, thus lacking the guarantee of effective protection of the stored data against the risks of abuse as well as against any illicit access and use of such data. This circumstance is likely to constitute an interference with the fundamental rights to intimate, family, and private life and the secrecy of correspondence and, therefore, infringes the constitutional provisions that enshrine and protect these rights*".

The need for such review was reasoned by pointing out that in the case of retention and storage of electronic information, the interference with the fundamental rights regarding intimate, family, and private life, the secrecy of correspondence, and the freedom of expression is extensive and must be regarded as being particularly serious. Furthermore, the circumstance that the retention of data and their subsequent use are carried out without the subscriber or registered user being informed thereof is likely to generate for the persons concerned the feeling that their private life is the subject of constant surveillance. Likewise, the Court emphasized that the information which can be retained or stored by providers of electronic communications networks or services, although predominantly technical in nature, is likely to provide relevant information regarding the individual and their private life. These data aim at identifying subscribers or customers, namely the user and the recipient of information communicated electronically, the source, destination, date, time, and duration of a communication, the type of communication, the communication equipment or devices used by the user, the location of mobile communications equipment, the payment methods used by users, as well as the history of access logs with the corresponding timestamps for an IP address. Such data are likely to affect the free

[9] Official Gazette no. 653 of 4 September 2014.

exercise of the right to correspondence or freedom of expression, as well as the person's intimate, family, and private life; "*specifically, the data in question allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, conclusions which may concern daily habits, permanent or temporary places of residence, daily or other movements, activities carried out, personal interests, social relationships of those persons and the social environments attended by them*"[10].

Using the same reasoning, the Court held the lack of an effective control mechanism over the activity of communications providers–namely, the entities that actually stored the data. Although the law appointed supervisory authorities, it did not provide them with the necessary levers to effectively verify whether operators complied with security standards, making it impossible to carry out an actual verification of the manner in which data were stored, protected, or destroyed; furthermore, no transparent information was provided regarding the institutions permitted to access these data[11]. Additionally, the majority of the established violations were sanctioned with an administrative fine rather than a criminal one, leaving the citizen vulnerable to the risks of potential abuses. At the same time, the law only defined as a criminal offense the intentional access, alteration, or transfer of retained data without authorization, while all other illicit acts were considered administrative offenses[12]. According to the Court, the failure to regulate a real control mechanism over electronic communications service providers was tantamount to a lack of safeguards.

Moreover, at the time the Decision No 440/2014 was issued, the Court of Justice of the European Union (CJEU) had already invalidated Directive 2006/24/EC through its Judgment of 8 April 2014; consequently, the Constitutional Court of Romania (CCR) found Law No 82/2012–which transposed the Directive as unconstitutional. Simultaneously, the Court found that the activities of retaining and using data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks "*become devoid of legal basis, both from the perspective of European and national law*"[13].

2.4. Lack of Adequate Safeguards for the Protection of Fundamental Rights. "Undermining or Destroying Democracy on the Ground of Defending It"[14]

The aforementioned decisions of the Constitutional Court also established the infringements upon the exercise of the right to freedom of movement, the right to intimate, private, and family life, and the interference with the secrecy of correspondence and freedom of expression caused by Law No 298/2008. Referring to the case-law of the ECtHR in Case *Klass and Others v. Germany*[15] (1978) or

[10] Decision no. 440/2014, para. 56.
[11] Ibidem, para. 68.
[12] Ibidem.
[13] Ibidem., para. 78.
[14] ECtHR Judgment of 6 September 1978, *Klass and Others v. Germany*, Application no. 5029/71, para. 49.
[15] Ibidem

Dumitru Popescu v. Romania[16] (2007), the Court established, through Decision No 1.258/2009, that interferences with private life can only be justified by the existence of robust legal safeguards, aimed at ensuring effective protection against the risk of abuse by state authorities. In accordance with the principles enshrined in *Klass* Case, the Court found that the adoption of surveillance measures, in the absence of adequate and sufficient safeguards, risks leading to the very destruction of democracy under the alleged reason of defending it.

2.5. European Jurisprudential Coherence on Electronic Communications Surveillance

With reference to the aforementioned sequence of decisions and the interference of EU law, it should be noted that other Constitutional Courts have also sanctioned, using similar reasoning, the transposition of the directive, and that it was ultimately invalidated by the CJEU in the joined cases *Digital Rights Ireland* (C-293/12) and *Seitlinger and Others* (C-594/12). Among the arguments upheld by the Court was the fact that no distinction was made between the categories of collected data based on their potential usefulness in achieving the pursued objective or based on the persons concerned. Directive 2006/24/EC did not provide clear and precise rules governing the scope of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. Furthermore, the imposition of a storage period of at least six months and a maximum of 24 months, without specifying that the determination of the retention duration must be based on objective criteria to guarantee its limitation to what is strictly necessary, contravened constitutional standards[17].

The approach of constitutional judges–whether referring to national constitutional courts or the CJEU–was based on a common objective: ensuring the highest possible standard of protection for human rights in the context of electronic communications surveillance. This remains in recent constitutional history as a valuable endeavor to defend constitutional values against technology and the risks involved in its improperly controlled use. Regarding the actual judicial relations between the courts, there have also been criticisms raising from the fact that the CCR did not address the CJEU with a preliminary ruling request in that context. In this regard, we share the opinion that the dialogue between judges in the EU must be strengthened and the preliminary ruling mechanism utilized to its full potential[18].

[16] ECtHR, Judgment of 26 April 2007, *Dumitru Popescu v. Romania (no. 2)*, Application no. 71525/01.

[17] CJEU, Judgment of 8 April 2014, *Digital Rights Ireland Ltd*, joined cases C-293/12 and C-594/12, EU:C:2014:238, paras. 63-65.

[18] Ibidem.

II. Technical Surveillance in Criminal Proceedings: Constitutional Limits and Safeguards

1. The Legality of Technical Surveillance Measures[19] – Criteria and Remedies

Over time, a rich case-law of the CCR has emerged in response to criticisms brought against the provisions of Chapter IV, marginally titled "Special Surveillance Methods[20]", under Title IV, "Evidence, Means of Evidence, and Evidentiary Procedures", of the Code of Criminal Procedure. In its rulings, relying on the landmark case law of the ECtHR, the Court has specified and described the criteria for assessing the legality of surveillance measures, as well as the remedies that the law must provide to persons against whom technical surveillance measures have been ordered. Thus, the CCR held that, in analyzing compliance with the safeguards for the right to private life provided by Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, the ECtHR considers–besides the aspects regarding the definition of categories of persons subject to technical surveillance–the nature of the offenses (types of offenses), the duration of the measure's execution, the authorization procedure, the conditions for drafting the summary report of intercepted conversations (transcription procedures), the precautions taken to communicate intact and complete recordings for judicial review, and aspects concerning the circumstances under which such interceptions can or must be destroyed (referring, for example, to the Judgment of 24 April 1990, *Huvig v. France*, paragraph 34; the Judgment of 18 February 2003, *Prado Bugallo v. Spain*, paragraph 30; the Judgment of 4 December 2015, *Roman Zakharov v. Russia*, paragraph 231).

At the same time, the CCR has contributed to "*shaping*" the incident regulatory framework by delivering rulings that eliminated a series of unconstitutionality flaws. As will be seen in the following analysis, these rulings applied the standards already defined in the "*Big Brother*" case law, thus marking a jurisprudential continuity within the specific field of criminal procedure regulation.

2. Legislative Precision in Defining Competent Authorities Empowered to Execute Technical Surveillance Warrants

2.1. The Separation of Criminal Investigation and Intelligence Functions in the Execution of Technical Surveillance Warrants

Applying the standard of quality of law extensively developed in its case law–which involves rigorous requirements in criminal matters–the CCR sanctioned the criminal procedure provisions that established, in a vague and imprecise manner, the

[19] See also Gianina-Anemona Radu, 'Theoretical and Practical Aspects Regarding Technical Surveillance in the Criminal Trial' (2023) *Valahia University Law Study* SI 216–223 https://www.ceeol.com/search/article-detail?id=1353109

[20] For references see Mihail Udroiu, 'A posteriori control of the legality of technical surveillance in Romanian criminal proceedings' (Studia Universitatis Babeș-Bolyai Iurisprudentia, Vol 68 No 2, 23 Dec 2023) https://doi.org/10.24193/SUBBiur.68(2023).2.6

category of authorities competent to enforce technical surveillance warrants, thereby allowing their execution by authorities not expressly specified by law.

Having been called upon to rule on the provisions of Article 142 (1) of the Code of Criminal Procedure, according to which "*The prosecutor shall execute the technical surveillance or may order it to be carried out by the criminal investigation body or by specialized workers within the police or by other specialized state bodies*", the CCR found that the phrase "*or by other specialized state bodies*" is unconstitutional[21].

In the reasoning of its decision, the Court emphasized the inherently intrusive nature of technical surveillance measures, underscoring the necessity of a clear, precise, and foreseeable legal framework. Such regulation must provide sufficient safeguards not only for the individual subject to the measure, but also clear guidance for prosecutorial authorities and courts, thereby ensuring protection against arbitrary or abusive implementation and against unjustified interference with fundamental rights, including the right to private and family life and the confidentiality of communications. However, through the aforementioned general phrasing, the legislator included within Article 142 (1) of the Code of Criminal Procedure, in addition to the prosecutor, the criminal investigation body, and specialized workers within the police, other specialized state bodies, such as the Romanian Intelligence Service (SRI) referenced by the authors of the exception, other services with duties in the field of national security, or specialized state bodies with duties in various fields, such as the National Environmental Guard, the Forest Guards, the National Authority for Consumer Protection, the State Inspectorate in Construction, the Competition Council, or the Financial Supervisory Authority, none of which possess criminal investigation powers. According to the CCR, "*the legislator's option for the technical surveillance warrant to be executed by the prosecutor and the criminal investigation bodies, which are judicial bodies according to Article 30 of the Code of Criminal Procedure, as well as by specialized workers within the police–insofar as they may hold the certification of judicial police officers under Article 55 (5) of the Code of Criminal Procedure–is justified",* but *not that of other bodies whose scope is not specified*. With reference to the opinions regarding the involvement of the SRI in criminal investigations–a flashpoint of both legal and public debate–the opinions of the Venice Commission[22] are noteworthy, as is the distinction made in legal literature[23] between intelligence gathering for national security and criminal prosecution activities. Intelligence agencies have specific duties and different operational rules, which do not overlap with the procedural safeguards of the criminal process. By allowing their involvement in the execution of common law technical surveillance warrants without establishing a clear legal framework, the citizen has no guarantee that the digital evidence against them was obtained by a legally authorized body.

[21] Decision no. 51/2016, Official Gazette, Part I, no. 190 of 14 March 2016, para. 20.

[22] See Venice Commission, *Report on the Democratic Oversight of the Security Services* (CDL-AD(2007)016), Strasbourg, 11 June 2007, para. 199 et seq.

[23] Popa, A.-N., *CCR Case-law regarding the notion of "national security"*, published on Juridice.ro on 10.02.2020.

In addition to the constant reference to ECtHR standards, it is interesting to note the manner in which the Court correlates the national regulatory framework with that of the EU, by specifically referring to provisions of the codes of criminal procedure from other states; regarding these, it notes that "*when regulating technical surveillance activities and their execution, they do so through clear and predictable rules and target only judicial bodies. In this sense, national codes of criminal procedure expressly provide that technical surveillance activities are carried out by the investigating judge, prosecution bodies, and police bodies, and that, from a technical standpoint, legal entities in the field of telecommunications services or other fields expressly and limitedly provided for by the law of criminal procedure are obliged to collaborate, if necessary, in their implementation*"[24]. From this perspective, it can be stated that this decision also finds its place within the space of jurisdictional dialogue that contributes to the strengthening of the European architecture for the protection of fundamental rights.

2.2. Remedies in Case of Breach of Competence by Prosecution Bodies

In this context, given its importance from the perspective of remedies for the violation of fundamental rights (including within the complex context of technical surveillance), we mention Decision No 302/2017[25]. Through this ruling, the CCR found that the legislative solution contained in the provisions of Article 281 (1) letter b) of the Code of Criminal Procedure–which does not include the breach of provisions regarding the material competence and personal competence (*ratione personae*) of the prosecution body within the category of absolute nullities–is unconstitutional. In essence, the CCR held that proving an injury to a person's rights solely through the prosecution body's failure to comply with provisions regarding subject-matter or personal competence "*turns into a proof difficult to achieve by the interested party, which amounts, in fact, to a genuine probatio diabolica, and implicitly leads to a violation of the fundamental right to a fair trial*". It is therefore required that, in this situation, the procedural injury to be presumed *juris et de jure*.

The logical link between Decision No 51/2016 and Decision No 302/2017 regarding remedies is expressly mentioned in the subsequent case law of the CCR, to which we shall briefly refer in the following section[26].

3. Technical Surveillance Activities. The Unconstitutionality of Granting the Status of Special Criminal Investigation Body to the Romanian Intelligence Service (SRI)

Following the delivery of Decision No 51/2016, Government Emergency Ordinance no. 6/2016 was adopted, aiming to align the provisions of the Code of Criminal Procedure with this CCR decision. Thus, the phrase found unconstitutional was removed from the provisions of Article 142 (1) of the Code of Criminal Procedure. Furthermore, Article 57 (2) of the Code of Criminal Procedure was amended to specify that "*special criminal investigation bodies may, in the case of*

[24] Decision no. 51/2016, para. 36.
[25] Official Gazette no. 566 of 17 July 2017.
[26] Official Gazette no. 193 of 12 March 2019.

offenses against national security provided for in Title X of the Criminal Code and terrorism offenses, upon the prosecutor's order, implement technical surveillance warrants" *(Article I point 1)*. Additionally, Article 13 of Law No 14/1992 on the organization and functioning of the SRI was amended to state that "*SRI bodies cannot perform criminal investigation acts, cannot take the measure of detention or preventive arrest, nor have their own arrest facilities. By way of exception, SRI bodies may be designated as special criminal investigation bodies according to Article 55 (5) and (6) of the Code of Criminal Procedure for the execution of technical surveillance warrants, in accordance with the provisions of Article 57 (2) final thesis of the Code of Criminal Procedure*" *(Article IV point 2)*. Through the same normative act, the role of the National Center for Communications Interception (CNIC) within the Romanian Intelligence Service (SRI) was established as a mandatory infrastructure for prosecution bodies in order to conduct technical surveillance activities[27].

Reiterating the reasoning that grounded its case-law in this matter and placing its analysis within a broad framework of European law, the CCR found that granting the status of special criminal investigation body to the SRI violates the constitutional provisions. The Court noted, *inter alia*, the aspects highlighted by the European Union Agency for Fundamental Rights, according to which "*an organizational separation between secret services and law enforcement authorities is usually considered a safeguard against the concentration of powers in a single service and the risk of arbitrary use of information obtained in secret*"[28].

Regarding the aforementioned technical structure, the Court held that the provisions concerning the execution of technical surveillance warrants through the C.N.I.C. are norms adopted to regulate a transitional situation in the period immediately following the publication of Decision No 51 of 16 February 2016, with the aim of adopting a precise regulation in the field that complies with constitutional requirements. Although six years have passed since the adoption of Government Emergency Ordinance no. 6/2016, the legislator, through its approval law, limited itself to approving the "*emergency solution*" without regulating a procedure compliant with constitutional norms, and established the C.N.I.C. as the sole entity executing both the authorization acts issued under Article 13 of Law No 51/1991 on Romania's national security and the technical surveillance warrants issued according to the Code of Criminal Procedure. The Court sanctioned this regulation, holding that regarding the execution of technical surveillance warrants issued under the Code of Criminal Procedure, it is not sufficient to indicate the name of a structure, entity, institution, or body that does not benefit from regulation at the level of law; "*although, according to Article 285 (2) of the Code of Criminal Procedure, the procedure during the criminal investigation is non-public, this does not mean the procedure is secret, but only that in this phase of the criminal process, the publicity specific to the trial phase does not exist*"[29].

[27] According to Art. 4 of Government Emergency Ordinance no. 6 of 11 March 2016 on certain measures for the execution of technical surveillance warrants ordered in criminal proceedings, published in the Official Gazette, Part I, no. 190 of 14 March 2016.

[28] Decision no. 55/2022, para. 155.

[29] Ibidem., para. 204.

The CCR case law, consistent with the dynamics of legislative amendments that essentially enshrined the same normative solution, responded to criticisms, also present in legal literature[30], according to which the mere reconfiguration of the SRI as a technical body does not change its nature as an intelligence service–militarized and subordinated to the executive–which is structurally incompatible with the safeguards of judicial independence. Regarding the field analyzed herein, that of digital evidence, the cited case law is particularly relevant from the perspective of the principle that control over the technical infrastructure determines the validity of the evidence. The dependence on the SRI's technical infrastructure turned judicial bodies into mere passive beneficiaries of data whose integrity was impossible to verify, in violation of the safeguards of the right to a fair trial. In the context of technological developments and the remodeling of evidence in criminal proceedings, it is essential that the modernization of the means of evidence–namely the introduction of digital evidence in building the prosecution's case–be achieved without compromising the independence of criminal investigation bodies and fundamental rights.

4. Convergence of European and National Jurisprudence on Data Protection and Technical Surveillance. Sanctioning the Cooperation Protocols between the Public Ministry and the SRI

As in the *Big Brother* precedent, the CCR case law regarding the execution of technical surveillance warrants correlates with the relevant CJEU case law. In the joined cases *Tele2 Sverige AB and Watson*[31], the CJEU emphasized that national legislation must provide objective criteria establishing a connection between the collected data and the pursued goal[32]. Reiterating the reasoning used in the *Digital Rights Ireland* case[33], the Court held that the continuous and undiscriminated use of communication storage and interception mechanisms is liable "*to generate in the minds of the persons concerned the feeling that their private life is the subject of constant surveillance*"[34]. Furthermore, generalized surveillance is incompatible with the foundations of a democratic society, affecting the very essence of freedom of expression. This same interpretation was reconfirmed by the CJEU several years later in the *VD and SR* judgment (Joined Cases C-339/20 and C-397/20)[35], where the Court established that not even the combating of economic offenses, such as market abuse, can justify the generalized storage of personal data[36]. The Court ruled that

[30] Cristescu, D. I., *Vademecum on the investigation of illicit manifestations against national security (III)*, published on Juridice.ro on December 8, 2023.

[31] CJEU, Grand Chamber, Judgment of 21 December 2016 delivered in joined cases C-203/15 *Tele2 Sverige AB v. Post- och telestyrelsen* and C-698/15 *Secretary of State for the Home Department v. Tom Watson and Others*, ECLI:EU:C:2016:970.

[32] Ibidem, para. 110.

[33] CJEU, Grand Chamber, Judgment of 8 April 2014 in joined cases C-293/12 *Digital Rights Ireland Ltd* and C-594/12 *Kärntner Landesregierung and Others*, ECLI:EU:C:2014:238, para. 37.

[34] CJEU, Judgment in *Tele2 Sverige and Watson* (C-203/15 and C-698/15), para. 100.

[35] CJEU, Judgment of 20 September 2022, *VD and SR*, Joined Cases C-339/20 and C-397/20, EU:C:2022:703.

[36] French legislation provided for "on a preventive basis, the generalized and undifferentiated retention of traffic data by electronic communications service providers for one

national courts may not maintain, on a provisional basis, the effects of a non-compliant law for the purpose of saving digital evidence in ongoing criminal cases. Information and evidence obtained as a result of generalized surveillance must be excluded[37]–a point on which we also note the CCR case law, which ruled to the same effect, this time within the framework of a legal dispute of a constitutional nature.

Thus, through Decision No 26/2019[38] on the request for the settlement of the legal dispute of a constitutional nature between the Romanian Parliament, on the one hand, and the Public Ministry–the Prosecutor's Office attached to the High Court of Cassation and Justice, the High Court of Cassation and Justice, and the other courts of law, on the other hand, the CCR essentially established the obligation of the High Court of Cassation and Justice and the other courts, as well as the Public Ministry–the Prosecutor's Office attached to the High Court of Cassation and Justice and its subordinate units–to verify, in pending cases, the extent to which a breach of the provisions regarding the competence *ratione materiae* and *ratione personae* of the prosecution body occurred through the conclusion of Protocols between the Public Ministry and the SRI, and to order the appropriate legal measures.

The aforementioned sequence of decisions marks a landmark moment in the evolution of the regulatory framework amidst the challenges posed by the technical complexity of digital evidence, such as the lack of adequate technical infrastructure highlighted even in the public communication of the Public Ministry at that time[39]. Although the primary focus of national and European debates was the involvement of intelligence services in the judiciary, our intention is to emphasize the complexity of the technical management of digital evidence and the rigorous requirements for the protection of fundamental rights in an increasingly technology-driven environment. Indeed, these aspects are also noted in EU rule of law evaluation documents, which consistently mention the need for a predictable legislative framework that guarantees effective judicial review[40].

III. Cybersecurity and Structural Preventive Surveillance

Technological development and risks to national security have led to the adoption of laws aimed at addressing new regulatory needs. In this regard as well, Romania's legislation has followed a sinuous path, in which the CCR's intervention has constituted a significant shaping factor.

---

year from the date of recording, with a view to combating market abuse offenses, including the unlawful use of inside information." – Court of Justice of the European Union (Research and Documentation Directorate), *Thematic Factsheet – Personal Data Protection*, July 2024, available at , pp. 53-57.

[37] Ibidem, p. 57.

[38] Official Gazette no. 193 of 12 March 2019.

[39] See National Anticorruption Directorate Press Release no. 252/VIII/3 of 9 March 2016, requesting the Ministry of Justice to increase the number of positions and the institution's budget to ensure the technical infrastructure necessary for the execution of surveillance warrants, available online at: https://www.dna.ro/faces/comunicat.xhtml?id=7206.

[40] See the Report from the Commission to the European Parliament and the Council on Progress in Romania under the Cooperation and Verification Mechanism (CVM) of 2017 and 2018, as well as the 2022 Rule of Law Report – Country Chapter on the rule of law situation in Romania, Luxembourg, 13.7.2022, SWD(2022) 523 final.

Thus, in 2015, the Cybersecurity Law was found unconstitutional in its entirety, primarily due to its unclear and imprecise manner of regulation[41], namely because it regulated its scope of application in a very general way, without distinguishing between the categories of persons who own, organize, administer, or use computer networks and systems. Beyond the technical aspects and the issues specific to the regulation of cyber infrastructure and the authorities with competence in the field, the Court also sanctioned the absence of any provision within the law ensuring the possibility for a person–whose rights, freedoms, or legitimate interests were affected by acts or deeds based on the provisions of the Cybersecurity Law of Romania–to appeal to an independent and impartial court of law. The Court held that this omission fails to comply with the provisions of Article 1 (3) and (5), Article 21 of the Constitution, as well as Article 6 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

Subsequently, however, the legislator incorporated the requirements established by the Court, so that a new Cybersecurity Law passed the constitutionality test and is currently in force. Through Decision No 70/2023[42], the CCR held that the adopted law is clear; regarding the specific component of data retention and use, it assessed that the mechanisms for notifying cybersecurity incidents and those for communicating cybersecurity risks, threats, and vulnerabilities ensure, in each individual case, determined timeframes/intervals–spanning from the moment of incident notification to the communication of additional data and information regarding the said incident. These timeframes are established to allow any concerned legal subject the physical, technical, and operational capacity to transmit the information in question to the competent authorities. The Court provided further clarification regarding the reporting obligation established by law, specifying that not every cybersecurity incident is capable of triggering the reporting mechanisms provided for by the law. For instance, not every propaganda or disinformation campaign is envisioned by the legislator, but only those of extreme gravity that represent a threat to national security[43].

Regarding the criticism that including all computer networks and systems within the national security protection system–specifically within the cybersecurity sector of national security–violates the right to intimate, family, and private life, as well as the freedom of expression, the Court found that the analyzed legislative solution does not target computer networks and systems in their materiality. Instead, the object of national security interest consists of the negative effects produced by cyberattacks and threats, as well as hybrid threats in cyberspace that affect the state's resilience capacity, namely propaganda and disinformation campaigns in cyberspace that affect the constitutional order.

In the reasoning of its decision, the Court mandated the necessity of a balance between cybersecurity protection needs and individual rights, placing particular emphasis on the protection of the right to privacy. The Court's interpretation sought to establish a distinction between technical data, necessary for the analysis of the

[41] Decision no. 17/2015, Official Gazette no. 79 of 30 January 2015.
[42] Official Gazette no. 131 of 15 February 2023.
[43] Decision no. 70/2023, Official Gazette no. 211 of 14 March 2023, para. 143.

cybersecurity incident, and content data. The Court held that the challenged law clearly specified that the information requested from cybersecurity technical service providers does not target personal data or content data[44]. The Court emphasized that the law did not authorize access to the content of users' private communications. The reporting obligation provided for by the legal text was strictly limited to the technical elements necessary for identifying and counteracting cyber threats.

This case-law, and the manner in which it has guided the adoption of a law essential in the context of current technological developments and the complex risks to which societies are subjected, reveals a fundamental requirement of the rule of law: cybersecurity, even when subsumed under national security, cannot constitute a regulatory space exempted from the constitutional rigors of clarity, proportionality, and effective judicial review. The analyzed legislative evolution demonstrates that the Court's intervention played an essential shaping role in defining the constitutional limits of state interference in the digital sphere. While the first regulation was sanctioned for its general, imprecise nature and lack of effective safeguards, the new cybersecurity law was validated precisely to the extent that it integrated clear criteria for determining its scope of application, established predictable procedural mechanisms, and expressly excluded access to the content data of private communications. From the perspective of digital evidence, this case law is of particular importance. Cyberspace currently represents one of the primary sources of data liable to become means of evidence in criminal proceedings or other proceedings relevant to national security. Thus, the classification and delimitation of this data–between technical data and content data–acquires a constitutional value. The Court has imposed the principle that the analysis of security incidents may justify the processing of strictly necessary technical data, but it cannot fail into a generalized mechanism for surveillance or for the collection of communication content in the absence of the specific safeguards of criminal procedural law and judicial authorization.

CONCLUSIONS

The analysis conducted in the present study was intended to outline the constitutional limits of digital evidence by referring to three interdependent levels: the retention of and access to data resulting from electronic communications, the use of technical surveillance measures in criminal proceedings, and the expansion of data collection mechanisms in the fields of cybersecurity and national security. This structure reflects the profound transformation of evidentiary matters in the digital age and the necessity of reconfiguring the safeguards of the rule of law in the face of technological expansion.

As regards data retention and access, the case law of the Constitutional Court of Romania– established by Decision No 1.258/2009 and subsequently consolidated– marked a defining moment in the process of constitutionalizing the digital space. The Court rejected the logic of generalized and undifferentiated surveillance, reaffirming

[44] Article 21 (5) of Law No 58/2023 on the cybersecurity and cyber defense of Romania: "*The data and information provided for in para. (1) do not target, through the purpose of the request, personal data and content data*."

that the efficiency of combating crime or terrorism cannot justify the establishment of continuous and global data storage obligations. The imposed standards–the quality of the law, the clear definition of competences, time limitations, effective judicial review, and the proportionality of the interference–have shaped a protection framework that transcends the strict field of electronic communications and projects itself onto the entire architecture of digital evidence.

In the field of technical surveillance within criminal proceedings, the Court transferred and consolidated these standards, insisting on the necessity of legislative precision in defining the bodies empowered to execute warrants, on the clear demarcation between intelligence activities and criminal investigation activities, and on the existence of effective remedies in case of breach of legal competence. The case law regarding the involvement of intelligence services and the management of technical infrastructure highlights an essential thesis for the digital evidence regime: the legality and fairness of evidence do not depend exclusively on the formal authorization of the measure, but also on the institutional and technical framework in which it is executed. In this context, control over the infrastructure becomes an intrinsic component of the guarantees of a fair trial.

Regarding cybersecurity and national security, the analysis reveals a refinement of the constitutional approach. While in the matter of generalized retention the Court sanctioned the lack of adequate safeguards, in recent decisions it has upheld the constitutionality of regulations that differentiate between technical data and content data and that limit reporting obligations to serious and concrete threats. This evolution confirms that not every interference is, by its nature, incompatible with constitutional requirements, but only that which exceeds the limits of necessity and proportionality or which operates within an imprecise regulatory framework devoid of effective control.

Thus, the constitutional limits of digital evidence in the field of cybersecurity are structured around three essential coordinates:

a) The legality and predictability of the norm, in the sense of clearly defining the categories of targeted entities, the types of relevant incidents, and the nature of the data that may be requested;

b) The proportionality of the interference, by restricting reporting obligations to serious incidents capable of affecting national security, and by excluding access to content data;

c) Effective jurisdictional safeguards, allowing the person concerned to challenge any potential abusive measures and ensuring the control of an independent court over the interference with fundamental rights.

Viewed as a whole, the Romanian experience highlights a progressive process of constitutionalizing digital evidence, achieved through a continuous dialogue with the case law of the CJEU and the ECtHR. The convergence of European and national standards confirms the existence of a common matrix of digital constitutionalism, founded on the rejection of generalized surveillance, the supremacy of judicial review, and the protection of the essence of fundamental rights.

In accordance with the premises set forth in the introduction, the central conclusion of the study is that the legitimacy of digital evidence does not arise from the technological performance of the collection means, but from their integration into

a clear, predictable regulatory framework subject to genuine jurisdictional control. In a rule of law, technology cannot become a substitute for constitutional safeguards, nor an instrument for the discretionary exercise of power. Judicial truth remains inseparable from the legality of the means by which it is obtained.

Beyond constitutional adjudication and doctrinal debates, the practical implementation of online surveillance measures in Romania reveals additional structural challenges. Recent analyses from legal practice emphasize that the interception of electronic communications, access to traffic and subscriber data, and cooperation obligations imposed on service providers operate at the intersection between criminal procedural law, data protection law, and national security legislation. From a practical standpoint, online surveillance does not concern only traditional telecommunication operators, but increasingly digital platforms, internet service providers, and entities managing electronic communications infrastructure. This technological expansion intensifies the need for clear delimitation of competences, especially in relation to the authorization procedure, the execution of surveillance warrants, and the preservation and integrity of digital evidence. In the perspective of accelerated technological developments–artificial intelligence, algorithmic data analysis, the interconnection of information databases–the challenges regarding digital evidence will continue to test the capacity of constitutional law to protect the balance between liberty and security. Precisely for this reason, the consolidation of a coherent digital constitutionalism, anchored in the principles of proportionality, subsidiarity, and effective control, represents not only a theoretical requirement but a structural condition for maintaining the rule of law in a more digitalized environment.

Abstract

This study examines the constitutional boundaries of the use of data resulting from electronic communications or technical surveillance measures across three distinct yet interconnected levels. Firstly, it examines the decisions of the Constitutional Court of Romania regarding data retention and access, which have outlined general protection standards applicable regardless of the nature of the proceedings–whether civil or criminal. Secondly, the analysis focuses on technical surveillance measures within criminal proceedings as some of the most intrusive evidentiary tools, highlighting the requirements of legality, foreseeability, proportionality, and effective judicial oversight. Thirdly, the research addresses the expansion of data collection mechanisms in the fields of cybersecurity and national security, where surveillance acquires a structural dimension, transcending a strictly procedural purpose.

Building on the chronological evolution of constitutional case law, the study highlights how the Court has sanctioned generalized or insufficiently regulated surveillance and mandated the clear statutory definition of competent authorities and the safeguards applicable to interferences with private life and the secrecy of communications. The analysis demonstrates that, in a state governed by the rule of law, neither the efficiency of criminal investigations nor the imperatives of national security can justify surveillance mechanisms lacking adequate and sufficient safeguards.

Recent Romanian case law reveals a process of progressive constitutionalization of the digital space, where the legitimacy of digital evidence resides from its integration into a clear, restrictive normative framework subject to real jurisdictional control, ensuring that technology does not become an instrument for the discretionary exercise of power. Far from conducting an exhaustive examination of such a complex field, this research calls for a comparative law approach within the framework of contemporary digital constitutionalism.

Key words: digital evidence; rule of law; technical surveillance; proportionality; right to privacy; secrecy of communications; constitutional court.

References

I. Decisions of the Constitutional Court of Romania

1. Decision No 1.258 of October 8, 2009, regarding the exception of unconstitutionality of the provisions of Law No 298/2008 on the retention of data generated or processed by electronic communications service providers, published in the Official Gazette no. 798 of 23 November 2009.

2. Decision No 440 of 8 July 2014, regarding the exception of unconstitutionality of the provisions of Law No 82/2012 on data retention, published in the Official Gazette no. 653 of 4 September 2014.

3. Decision No 51 of 16 February 2016, regarding the exception of unconstitutionality of the provisions of Article 142 (1) of the Code of Criminal Procedure, published in the Official Gazette no. 190 of 14 March 2016.

4. Decision No 26 of 16 January 16, 2019, on the request for the settlement of the legal conflict of a constitutional nature between the Romanian Parliament, on the one hand, and the Public Ministry – the Prosecutor's Office attached to the High Court of Cassation and Justice, the High Court of Cassation and Justice, and the other courts of law, on the other hand, published in the Official Gazette no. 193 of 12 March 2019.

5. Decision No 55 of 16 February 2022, regarding the objection of unconstitutionality of the Law for the approval of Government Emergency Ordinance no. 6/2016 on certain measures for the execution of technical surveillance warrants ordered in criminal proceedings, published in the Official Gazette no. 590 of 17 June 2022.

6. Decision No 295 of 18 May 2022, regarding the objection of unconstitutionality of the Law for the amendment and completion of certain normative acts in the field of electronic communications and for the establishment of measures to facilitate the roll-out of electronic communications networks, published in the Official Gazette no. 533 of 31 May 2022.

7. Decision No 70 of 28nFebruary 2023, regarding the objection of unconstitutionality of the provisions of the Law on the cybersecurity and cyber defense of Romania, published in the Official Gazette no. 211 of 14 March 2023.

II. CJEU and ECtHR

8. CJEU, Judgment of 8 April 2014, Digital Rights Ireland Ltd, Joined Cases C-293/12 and C-594/12, EU:C:2014:238.

9. CJEU, Judgment of 21 December 2016, Tele2 Sverige AB and Watson, Joined Cases C-203/15 and C-698/15, EU:C:2016:970.

10. CJEU, Judgment of 20 September 2022, VD and SR, Joined Cases C-339/20 and C-397/20, EU:C:2022:703.

11. ECtHR, Judgment of 6 September 1978, Klass and Others v. Germany, Application no. 5029/71.

12. ECtHR, Judgment of 26 April 2007, Dumitru Popescu v. Romania (no. 2), Application no. 71525/01.

III. Normative Acts and International Documents

13. The Constitution of Romania, republished in the Official Gazette (*M. Of.*) no. 767 of 31 October 2003.

14. The Convention for the Protection of Human Rights and Fundamental Freedoms, ratified by Romania through Law no. 30/1994, published in the Official Gazette (*M. Of.*) no. 135 of 31 May 1994.

15. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, published in the *OJ* L 105 of 13 April 2006.

16. Government Emergency Ordinance (GEO) no. 6 of March 11, 2016, on certain measures for the execution of technical surveillance warrants ordered in criminal proceedings, published in the Official Gazette (*M. Of.*) no. 190 of 14 March 2016.

17. European Court of Human Rights, *Thematic Factsheet – Personal Data Protection*, July 2024.

18. Venice Commission, *Report on the Democratic Oversight of the Security Services* (CDL-AD(2007)016), Strasbourg, 11 June 2007.

19. European Commission, *Report to the European Parliament and the Council on Progress in Romania under the Cooperation and Verification Mechanism (CVM)*, COM(2017) 44 final, Brussels, 25.01.2017.

20. European Commission, *Report to the European Parliament and the Council on Progress in Romania under the Cooperation and Verification Mechanism (CVM)*, COM(2018) 778 final, Strasbourg, 13.11.2018.

21. European Commission, *Commission Staff Working Document – 2022 Rule of Law Report, Country Chapter on the rule of law situation in Romania*, SWD(2022) 523 final, Luxembourg, 13.07.2022.

22. Charter of Fundamental Rights of the European Union, published in the *Official Journal of the European Union*, C series, no. 83 of 30.03.2010 (2010/C 83/02).

23. European Parliament, Council and Commission, *European Declaration on Digital Rights and Principles for the Digital Decade*, published in the *Official Journal of the European Union*, C series, no. 23 of 23 January 2023 (2023/C 23/01).

24. Law No 58 of 14 March 2023 on the cybersecurity and cyber defense of Romania, published in the Official Gazette (*M. Of.*) no. 214 of 15 March 2023.

IV. Papers

25. Popa, A.-N., *CCR Case-law regarding the concept of "national security"*, published on Juridice.ro on 10.02.2020, available online at: https://www.juridice.ro/712215/jurisprudenta-ccr-cu-privire-la-notiunea-de-securitate-nationala.html#_ftn10.

26. Cristescu, D. I., *Vademecum on the investigation of illicit manifestations against and contrary to national security (III)*, published on Juridice.ro on December 8, 2023, available online at: https://www.juridice.ro/716980/vademecum-privind-investigarea-manifestarilor-ilicite-la-adresa-si-contra-securitatii-nationale-iii.html.

27. National Anticorruption Directorate, *Press Release no. 252/VIII/3 of March 9, 2016*, available online at: https://www.dna.ro/faces/comunicat.xhtml?id=7206.

28. C. F. Stoica, M. Safta, *Theoretical and practical issues relating to the right to the protection of personal data*, 5(2), Juridical Tribune – Review of Comparative and International Law 88–10, 2015.

29. Lynskey, O., *The Foundations of EU Data Protection Law*, Oxford University Press, Oxford, 2015.

30. Gianina-Anemona Radu, 'Theoretical and Practical Aspects Regarding Technical Surveillance in the Criminal Trial' (2023) *Valahia University Law Study* SI 216–223 https://www.ceeol.com/search/article-detail?id=1353109

31. Rodotà, S., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Ediția a II-a, Ed. Laterza, Roma-Bari, 2004.

32. T. Toader, M. Safta, 'Constitutional Identity and Relations Between EU Law and Romanian Law' in András Zs Varga and Lilla Berkes (eds), *Common Values and Constitutional Identities – Can Separate Gears Be Synchronised?* (Central European Academic Publishing 2023) 271–352

33. Mihail Udroiu, 'A posteriori control of the legality of technical surveillance in Romanian criminal proceedings' (Studia Universitatis Babeș-Bolyai Iurisprudentia, Vol 68 No 2, 23 Dec 2023) https://doi.org/10.24193/SUBBiur.68(2023).2.6

Information about the authors:
Safta Marieta,
Professor at the Faculty of Law, "Titu Maiorescu" University of Bucharest,
Associate Professor at the Faculty of Law,
Bucharest University of Economic Studies,
187 Calea Văcărești, 040051, Bucharest, Romania

Stanciu Claudia Ana Maria,
PhD Student at the Doctoral School of Law,
Bucharest University of Economic Studies,
Lawyer, Bucharest Bar,
7 Piața Romană, 010374, Bucharest, Romania