Decision no. 17
of 21 January 2015

on the objection of unconstitutionality against the provisions of the Law on cybersecurity of Romania

Published in the Official Gazette no. 79 of 30 January 2015

Augustin Zegrean	— President
Valer Dorneanu	— Judge
Toni Greblă	— Judge
Petre Lăzăroiu	— Judge
Mircea Ştefan Minea	— Judge
Daniel Marius Morar	— Judge
Mona-Maria Pivniceru	— Judge
Puskás Valentin Zoltán	— Judge
Tudorel Toader	— Judge
Mihaela Senia Costinescu	— Assistant-Magistrate-in-chief

1. The case at issue is the settlement of the objection of unconstitutionality against the provisions of the Law on cybersecurity of Romania, objection raised by 9 Deputies belonging to the National Liberal Party Parliamentary Group in the Chamber of Deputies.

2. By Letter no. 2/6.103 of 23 December 2014, the Secretary General of the Chamber of Deputies has forwarded to the Constitutional Court the referral of unconstitutionality, which was registered at the Constitutional Court under no. 6.188 of 23 December 2014 and which constitutes the subject matter of Case-File no. 1.419A/2014. The Law on cybersecurity of Romania was enclosed, in copy, to the referral.

3. **As grounds for the objection of unconstitutionality**, its authors claim that the legal provisions are contrary to Article 1 (3) and (4) concerning the rule of law and the obligation to observe the Constitution and the laws. It is alleged that the impugned law introduces confusion and conditionality for holders of cyber infrastructures which are likely to create restrictions of the fundamental rights and liberties of citizens. The legal provisions do not comply with Article 6 of Law no. 24/2000 on the rules of legislative technique for drafting normative acts, and consequently, they infringe the principle of legality, which is essential for the proper functioning of the rule of law. Article 1 of the law establishes only obligations for the holders of cyber infrastructure without establishing also their rights. The list contained in Article 2 of persons/entities subject to the law is not precise, failing to stipulate on the situation of intermediaries of cyber infrastructures, of non-operational infrastructures, of shareholders of legal persons, or that of the founders of associations or foundations that own such infrastructures.

4. The authors of the referral argue that the law has fundamental conceptual problems, as it proposes a series of measures having a limiting effect on the right provided by Article 26 (1) of the Constitution on the personal, family and private life, and clearly infringes the European legislation under discussion referring to the security of information in the digital environment.

5. The authors of the objection of unconstitutionality claim that the impugned law generates restrictions on the rights and freedoms of citizens by enabling access to a cyber infrastructure and to the data contained therein, based on a simple reasoned request from the institutions set forth in the law, addressed to the infrastructure owners, without the prior approval of a judge, as stipulated in the Code of Criminal Procedure or in the case-law of the

Constitutional Court, in the Decisions no. 440/2014 and no. 461/2014, thus resulting in a violation of the constitutional provisions contained in Article 23 (1) on the inviolability of personal freedom and safety, as well as in Article 28 on the secrecy of correspondence.

6. On the other hand, it is pointed out that, under the provisions of Article 10 of the Law, the Romanian Intelligence Service is appointed as national authority in the field of cybersecurity, capacity in which it ensures the technical coordination, organisation and execution of activities related to Romania's cybersecurity. While the European Union, in the draft NIS (Network and Information System) Directive, proposes that authorities dealing with cybersecurity be "civilian bodies, subject to full democratic oversight, that should not fulfil any tasks in the field of intelligence", the Parliament of Romania grants unlimited and unattended access to all computer data held by persons of public and private law to institutions not fulfilling any of the above conditions. The fact that the Constitutional Court, in its recent case-law, has declared as unconstitutional two laws that, in essence, infringed the same rights as the law currently subject to review, is a serious reason for a real discussion on the implications of the Cybersecurity Law and, more generally, on the balance between individual rights and national security, which Romania has to ensure through its legal system. The authors of the referral argue that the possibility to have access, without a court order, to electronic data originating from any computer, irrespective of its owner, is an unjustified interference with the right to the protection of correspondence, i.e. with the right to privacy, as guaranteed by Articles 26 and 28 of the Constitution. Such interference is not only unnecessary in a democratic society, but it has precisely the opposite effect: it undermines the essence of a democratic society. Thus, on the pretext of protecting against cyber-attacks, any data may be accessed at the discretion of the executive power, without any control from the civil society.

7. It is argued in the referral of unconstitutionality that Article 148 (2) of the Constitution is also infringed, given the failure to transpose correctly the EU rules in this area. Thus, the provisions of Article 17 (1) (a) do not comply with the case-law of the Court of Justice of the European Union because they do not state exactly what data must be retained, whilst the framework in which these data are requested does not provide sufficient procedural guarantees. To fulfil this obligation, a continued monitoring of all people is required, which creates a disproportionate burden for the parties concerned and also involves violations of the rights of the persons monitored without a relative suspicion that they may be committing a crime. It is also pointed out that the law infringes in many respects also the proposal for a NIS (Network & Information Security) Directive, which aims at protecting the citizens' personal data and not at creating new tasks for the intelligence services. "While the NIS Directive aims at protecting the computer systems and computer data of citizens, the law, as adopted, is a blank cheque that may be used by the intelligence services to control any private person (LLC, Joint Stock Company, Registered Sole Trader, NGO,) holding a computer system (i.e. any computer or smart phone). The potential for misuse is thus enormous. It follows from numerous ambiguities present in the law, starting with a vague definition of computer system holders and continuing with the obligations of those covered by the law."

8. In conclusion, the authors of the objection of unconstitutionality take the view that "the entire architecture of this legislative act is likely to allow violations of the fundamental human rights with no effective remedy against such violations." Although in a democratic society the limits of the protection of fundamental rights can be reduced in the event of serious threats (terrorism, cross-border crime), evidence obtained from such procedures may not be used in ordinary cases (those not involving the protection of national security, as defined by law), where procedural safeguards must be strictly observed. However, "the impugned law does not introduce any prohibition on the use of data in any other way than as necessary for protecting against cyber attacks, which can undermine the guarantee of a fair trial".

9. In accordance with Article 16 (2) of the Law no. 47/1992 on the organisation and functioning of the Constitutional Court, the referral was communicated to the presidents of the two Chambers of Parliament, as well as to the Government, in order for them to express their viewpoints.

10. **The President of the Chamber of Deputies** has sent to the Constitutional Court, through Letter no. 2/51 of 7 January 2015, registered with the Constitutional Court under no. 99 of 7 January 2015, his viewpoint, whereby he claimed that the referral of unconstitutionality was unfounded.

11. In the arguments, he explained that Article 1 of the impugned law refers not only to the obligations for those concerned, but envisages legislative solutions covering the whole issue of social relations that represent the regulatory subject-matter of that law. Thus, the law departs from the assumption that cybersecurity measures should ensure a secure virtual environment, which would constitute a genuine support for maximising the benefits for the citizens, businesses and Romanian society as a whole. All cyber infrastructure holders and users, whether they are intermediaries or not, must take the necessary steps to ensure the security of their own infrastructures and to avoid affecting the security of other holders or users.

12. Furthermore, it is explained that, since the provisions of this law are applicable only to legal persons of public or private law, holders of cyber infrastructures, and not to individuals, the provisions of Article 26 (1) of the Constitution have no relevance whatsoever.

13. As regards the challenges against Article 17 of the Law, on access to data, the President of the Chamber of Deputies argues that the law concerns data that are relevant for taking pro-active and reactive measures at the level of cyber infrastructures, and not traffic data, so that there is no prejudice to the rights provided for in Articles 23 and 28 of the Basic Law. Moreover, the provisions of Articles 12 and 14 of the impugned law provide that public authorities and institutions responsible for applying this law ensure cyber infrastructures security according to the law and their legal competences. These entities must therefore comply with, and are strictly limited by respect of, the legal framework.

14. With regard to the designation of the Romanian Intelligence Service as national authority in the area of cybersecurity, it is pointed out, on the one hand, that the NIS Directive does not require that Member States of the European Union designate a civil authority and, on the other hand, that, according to Article 1 of Law no. 14/1992 on the organisation and functioning of the Romanian Intelligence Service, the activity of this institution is subject to parliamentary scrutiny carried out through the Standing Joint Committee of the Chamber of Deputies and the Senate.

15. **The Government** expressed its point of view by Letter no. 5/7.033/2014, registered with the Constitutional Court under no. 146 of 13 January 2015, which states that the purpose of the Law on cybersecurity is to ensure a consistent regulatory framework for social relationships in the online environment, which would ensure their cybersecurity, as part of Romania's national security.

16. On the challenges of unconstitutionality, the Government takes the view that "a careful reading of the law shows that these issues are not real, but are based on a biased interpretation of Article 17 of the Law, i.e. they do not take into account the general context of ensuring cybersecurity". It is shown that the competent authorities referred to in this article will have access to data of cyber infrastructure owners relevant for cybersecurity, not to messages or other content data stored, processed or sent by the computer system. The data concerned by this law are the logbooks of data storage, processing and transmission systems (logs), technical data or computer system configuration data and do not include messages or other content data. Where the preliminary analysis shows that there is a need for further investigation on content data, access to these, as well as any other activities aimed at restricting the rights and freedoms are carried out in compliance with the legal provisions in force, respectively based on an

authorisation issued by a judge. As cyber attacks take place very quickly, they may cause material damage to citizens, they may affect cyber infrastructures of national interest (CINIs) or even national security, and it is inefficient for competent authorities to await for an opinion drawn up by a public prosecutor and considered and approved by a judge in order to get access to technical data in a way which does not harm in any way the constitutional rights and freedoms. It is physically impossible for each of these incidents to be investigated, therefore the competent authorities focus only on those that are likely to produce significant adverse impacts, including in terms of national security. The Government argues that "such clarification will however be introduced in the law implementing rules, while in the legislative act the provision was mentioned only conceptually".

17. As concerns the plea that the law does not also cover "situations involving intermediaries that make available such infrastructures", the Government states that, in cases where such intermediaries are involved in the cyber infrastructure flow, they circumscribe to the capacity as holders of such infrastructures, as defined in Article 2 of the law.

18. Accordingly, for the reasons set out above, the Government considers that the referral of unconstitutionality of the Law on the cyber security of Romania is unfounded.

19. **The President of the Senate** did not communicate his viewpoint on the objection of unconstitutionality.

THE COURT,

having examined the objection of unconstitutionality, the report drawn up by the judge-rapporteur, the viewpoints of the President of the Chamber of Deputies and of the Government, the provisions of the Law on the cyber security of Romania, as well as the provisions of the Constitution, holds as follows:

20. The Constitutional Court has been legally referred to and is competent, according to the provisions of Article 146 a) of the Constitution, as well as of Articles 1, 10, 15, 16 and 18 of Law no. 47/1992 to adjudicate on the constitutionality of the impugned legal provisions.

21. The subject-matter of the constitutional review, as it results from the referral, is represented by the provisions of the Law on the cyber security of Romania.

22. The allegedly violated constitutional provisions are those of Article 1 (3) and (5) on the rule of law and the obligation to respect the laws and the supremacy of the Constitution, of Article 23 (1) on the inviolability of personal freedom and safety, of Article 26 on personal, family and private life, of Article 28 on the secrecy of correspondence, and of Article 148 on the integration with the European Union.

23. Having examined the objection of unconstitutionality, the Court notes that Law on the cyber security of Romania, which aims at completing the legislative framework in matters of national security, was initiated by the Government of Romania and then adopted by Parliament on 19 December 2015. In the "Explanatory Memorandum" attached to the law, the Government stated that, "by the adoption of this legislative act, Romania will continue to send strong signals of connection to the international realities, being fully aware of the need to get in line with similar steps taken by the European States"; in the absence of such a regulation "our country will not be able to harmonise the steps that it took in the field of cyber security with those of its partners within the European Union and NATO, steps needed for a coherent and sufficient approach of the challenges and opportunities that the cyberspace supposes".

24. With regard to the points raised, the Court notes that, at European level, pursuant to Article 114 of the Treaty on the Functioning of the European Union, it was initiated the ordinary legislative procedure for the adoption of a Directive concerning measures to ensure a high common level of network and information security across the Union - NIS (Network and Information Security) Directive. The initiative lies with the European Commission, which on 7 February 2013 sent the proposal for a Directive to the Council and to the European Parliament.

The proposal for a directive has completed the procedure of the first reading within the European Parliament, where it was adopted, as amended, on 13 March 2014. On 10 June 2014, the European Commission has given a partial approval of the Parliament's amendments. *Therefore, at the time when the case referred to the Constitutional Court for settlement is decided upon, there is no EU legislation in force related to cyber security.*

25. However, **the Court considers as relevant for the regulatory field several aspects adopted by the Union's institutions in the field in question.** Thus, according to the "Explanatory Memorandum" of the Directive, the need for adopting the European legislative act consists, on the one hand, *in securing the resilience and stability of network and information systems, essential for the completion of the Digital Single Market and the smooth functioning of the Internal Market* and, on the other hand, in ensuring a similar and training within the Member States likely to ensure an overall security of networks and information within the interconnected systems. The proposed directive is aimed at the following objectives: first, *it requests all Member States to ensure the development of a minimum level of national capacities through the setting up of authorities competent in the field of network and information systems,* to create intervention teams in case of computer emergency (Computer Emergency Response Teams - CERTs) and *to adopt national strategies on cybersecurity and national plans of cooperation* in the field concerned; secondly, *the competent national authorities should cooperate within a network* that would enable safe and effective coordination, including the exchange of information coordinated at EU level, as to counter cybersecurity threats and incidents, based on the European plan of cooperation in the field; thirdly, according to the model of the Framework Directive on electronic communications, the proposal seeks to ensure the development of a culture of risk management and sharing of information by the public and private sectors.

26. The Court also invokes recital 41 of the preamble to the directive which states that "*This Directive respects the fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union* notably, the right to *respect for private life and communications, the protection for personal data*, the freedom to conduct a business, the right to property, *the right to an effective remedy before a court and the right to be heard*. This Directive must be implemented according to these rights and principles."

27. The proposal for a Directive, as adopted by the European Parliament, contains several provisions which are mandatory for the Member States, provisions that should be transposed into the national legislation of each Member State. Thus, the preamble to the NIS Directive (recital 10) states that the competent authorities and the single points of contact should be ***civilian bodies***, subject to full democratic oversight, and ***should not fulfil any tasks in the field of intelligence***, law enforcement or defence or be organisationally linked in any form to bodies active in those fields. The provisions of Article 6 of the Directive, as amended by the EP, state that "(1) ***Each Member State shall designate one or more civilian national authorities*** competent in matters related to the security of network and information systems."

28. The proposal for a NIS Directive ***does not provide for the right of the designated authorities to access, upon reasoned request, data stored in computer networks and systems***, as required by Article 17 (1) (a) of the law subject to the review of constitutionality, but merely an obligation to notify cyber risks and incidents (Article 14) and to be subject to an audit in relation to the holders of critical infrastructures (Article 15). Thus, in cases where the notifications contain personal data, these shall be disclosed only to recipients within the competent authorities who need to process these data for the performance of their tasks in accordance with an appropriate legal basis, and the disclosed data shall be limited to what is necessary for the performance of the tasks of these recipients — Article 14 (2a), whilst the competent authorities have the power to request market operators to provide "evidence of effective implementation of security policies, such ***as the results of the security audit carried***

out by internal auditors, a qualified independent body or national authority, and make the evidence available to the competent authority or to the single point of contact" — Article 15 (2) of the Directive.

29. Furthermore, Article 3 of the proposal for a Directive defines the concept of ***market operator*** as "operator of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, financial markets, internet exchange points, food supply chains and health, and the disruption or destruction of which would have a significant impact within a Member State, a non-exhaustive list of which is set out in Annex II, insofar as the network and information systems concerned are related to its essential services." Annex II to the proposal for a Directive — List of market operators concerns, on the one hand, *e-commerce platforms*, Internet payment gateways, social networks, search engines, cloud computing services, application stores and, on the other hand, *fields relating to its essential services*, such as energy, transport, banking, financial market infrastructures and health. In addition, the proposal for a Directive and therefore the provisions on cybersecurity also cover *the field of public administrations* (point 26 of the preamble and Chapter IV of the proposal for a Directive).

30. According to the "Explanatory Memorandum" to the Directive, companies in the specific critical sectors and public administrations will be asked to assess the risks that they face and adopt appropriate and proportionate measures to ensure cybersecurity. These entities will be required to report to the competent authorities any *incidents* seriously compromising their networks and information systems and *significantly affecting the continuity of the critical services and supply of goods*. To avoid imposing a disproportionate burden on small operators, in particular on SMEs, the requirements are proportionate to the risk that the network or information system concerned faces and should not apply to microenterprises, but target only critical entities and impose measures that are proportionate to the risks. Thus, Article 14 (8) of the proposal for a NIS Directive establishes that ***microenterprises do not fall within the scope of this Directive unless they act as subsidiary for a market operator***.

31. Finally, according to Article 15 (6) of the proposal for a Directive, "***Member States shall ensure that any obligations imposed on market operators [...] may be subject to judicial review***."

32. At the time of the review of constitutionality, the Court concludes that national security laws include some regulations, primary or secondary legislative acts, which are already in force. Thus, ***Government Emergency Ordinance no. 98/2010 on the identification, designation and protection of critical infrastructures***, published in the Official Gazette of Romania, Part I, no. 757 of 12 November 2010, approved with amendments by Law no. 18/2011, published in the Official Gazette of Romania, Part I, no. 183 of 16 March 2011, establishes the legal framework on the identification, designation of national/European critical infrastructure and the assessment of the need to improve their protection, in order to increase the capacity to ensure the stability, security and safety of socio-economic systems and the protection of individuals. The ordinance transposes Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, published in the Official Journal of the European Union Series L No. 345 of 23 December 2008. The legislative act *defines national critical infrastructure*, referred to as *NCI*, as an asset, a system or part thereof, located on the national territory which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact at national level as a result of the failure to maintain those functions. This legislative act establishes *the cross-cutting criteria for the identification of NCI:* casualties criterion, assessed in terms of the potential number of fatalities or injuries; economic effects criterion, assessed in terms of the significance of economic loss and/or degradation of products or services, including possible

environmental effects; public effects criterion, assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services. In accordance with the procedure laid down by this emergency ordinance, the responsible public authorities shall identify potential NCIs corresponding to the sectoral and cross-cutting criteria. *The legislative act contains 3 Annexes*: Annex no. 1 — List of sectors, subsectors of the national critical infrastructure/ European critical infrastructure (NCI/ECI) and of responsible public authorities; Annex no. 2 — Procedure of identification by responsible public authorities of critical infrastructures which may be designated as national critical infrastructure/European critical infrastructure (NCI/ECI) and Annex no. 3 — Procedure on the security plan for the operator.

33. For implementing the emergency ordinance, the Government issued ***Decision no. 718/2011***, published in the Official Gazette of Romania, Part I, no. 555 of 4 August 2011, which approves the *National strategy on critical infrastructure protection.*

34. ***Government Decision no. 494/2011***, published in the Official Gazette of Romania, Part I, no. 388 of 2 June 2011, *governs the setting up* as a public institution with legal personality, under the coordination of the Ministry of Communications and Information Society, of the *National Centre for Response to Cybersecurity Incidents — CERT-RO, an independent structure for expertise and research-development in the field of cybersecurity*. The Centre is headed by a Director-General and a Deputy Director-General, supported by the Steering Committee, which consists of representatives of the Ministry of Communications and Information Society, the Ministry of National Defence, the Ministry of Administration and Interior, the Romanian Intelligence Service, the Foreign Intelligence Service, the Special Telecommunications Service, the Protection and Guard Service, the National Registry Office for Classified Information and the National Authority for Management and Regulation in Communications. The Government Decision defines *terms and expressions such as cyber infrastructure, cyberspace, cybersecurity, cyber attack, cyber incident etc.* and establishes the powers of CERT-RO.

35. Another legislative act issued in the field of national security is ***Government Decision no. 271/2013*** approving *Romania's Cybersecurity Strategy and the National Action Plan on the implementation of the National Cybersecurity System*, published in the Official Gazette of Romania, Part I, no. 296 of 23 May 2013.

36. Cybersecurity strategy sets out the objectives, principles and major strands of action for the identification, prevention and counteracting of threats, vulnerabilities and risks to Romania's cybersecurity and for promoting national goals, values and interests at the level of the cyberspace. In this respect, it sets out the meanings of the terms and phrases used in this area, it provides *for the establishment of the National System for Cybersecurity* (NSCS), which is the overarching framework for cooperation which brings together public authorities and institutions with responsibilities and capabilities in the field, in order to coordinate action at national level for ensuring the security of the cyber space, including through cooperation with the academic and business environment, professional associations and non-governmental organisations. Furthermore, it provides that the *Cybersecurity Task Force (CSTF)* is the body through which the coordination of the NSCS is achieved. The representatives of the Ministry of Defence, the Ministry of Interior, the Ministry of Foreign Affairs, the Ministry for the Information Society, the Romanian Intelligence Service, the Special Telecommunications Service, the Foreign Intelligence Service, the Protection and Guard Service, the National Registry Office for Classified Information, and the secretary of the Supreme Council for National Defence, are part of the CSTF, as permanent members. The CSTF is managed by a President (the presidential advisor on matters of national security) and a Vice-president (the advisor of the Prime Minister on matters of national security). The technical coordinator of the CSTF is the Romanian Intelligence Service, under the terms of the law.

37. *The national action plan on the implementation of the National system of cybersecurity* is contained in Annex 2 to this Decision and is a classified document.

38. On 27 May 2014, the Government of Romania initiated the bill on the cybersecurity of Romania, aimed at supplementing the legislative framework concerning national security, taking the view that the issue of cybersecurity, as part of the national security, is a priority that requires the adoption of measures needed to develop cyber defence mechanisms. The rationale behind the issuance of the legislative act, as it results from the "Explanatory Memorandum" attached to it, is "the recent evolution of cyber attacks in our country" leading to the opinion that "Romania is definitely a target for hostile actors in the cyberspace, and the current level of cybersecurity is insufficient for dealing with attacks of high level or destructive intentions." The law aims at establishing a general regulatory framework for the activities in the field of cybersecurity, defining the obligations of legal persons of public or private law in order to protect cyber infrastructures, and at ensuring the general cooperation framework for cybersecurity, through the establishment of the National System of Cybersecurity.

39. The bill was adopted on 17 September 2014 by the Chamber of Deputies, in its capacity as first Chamber notified, under Article 75 (2), third sentence of the Constitution — given that the 45-day period was exceeded, and on 19 December 2014, the Senate of Romania, as the decision-making Chamber, adopted the Law on the cybersecurity of Romania. The Law was sent to the President of Romania for promulgation, and, within the deadline provided by law, 69 MPs made the request for referral to the Constitutional Court, which is the subject-matter of this case-file.

40. Having analysed the document prepared by the initiator of the law, entitled "Explanatory Memorandum", section 6 — Consultation carried out for the purpose of preparing the draft legislative act, under the heading entitled Information on endorsement by competent authorities, the Court finds that the Government mentions only the opinion of the Legislative Council.

41. According to the provisions of Article 1 of the impugned law, it sets the general regulatory framework for activities in the field of cybersecurity and the obligations of legal persons of public or private law in order to protect the cyber infrastructures, and the provisions of Article 3 (1) of the law set out that "cybersecurity is part of Romania's national security". With regard to the regulatory field of the legislative act subject to constitutional review, the Court notes that, pursuant to Article 119 of the Basic Law, "the Supreme Council for National Defence shall ensure the organisation and unitary coordination of activities concerning the country's defence and national security, the participation in maintaining international security and in collective defence arrangements within the systems of military alliance, as well as in peace-keeping or restoring missions". For the enforcement of these provisions, Article 4 (d) (1) of Law no. 415/2002 on the organisation and functioning of the Supreme Council for National Defence, establishes, amongst the powers of the ***SCND***, that it "***endorses draft legislative acts initiated or issued by the Government on national security***". Furthermore, according to Article 9 (1) of Law no. 24/2000 on the rules of legislative technique for drafting normative acts, "In the cases laid down by law, when drafting legislative acts, the initiator must seek the opinion of the authorities concerned with implementation thereof, depending on the scope of the regulation". In addition, Article 31 (3) of that law states that "The final form of the instruments setting forth the contents and reasons of draft legislative acts shall include references to the opinion of the Legislative Council and, where appropriate, of the Supreme Council for National Defence, of the Court of Auditors or of the Economic and Social Council." Therefore, under the impugned legal provisions, the Government was required to request the opinion of the Supreme Council for National Defence when drafting the bill on the cybersecurity of Romania.

42. For the reasons set out, as during the legislative procedure, the initiator has not complied with the legal obligation under which the Supreme Council for National Defence

endorses draft legislative acts initiated or issued by the Government on national security**, the Court notes that the legislative act was adopted in breach of the relevant constitutional provisions of Article 1 (5), which enshrine the principle of legality, and of Article 119 concerning the powers of the Supreme Council for National Defence.**

43. By examining the normative content of the law, the Court notes that it provides for the establishment of the *National System of Cybersecurity*, referred to as *NSCS*, which brings together public authorities and institutions with responsibilities and powers in this field (Article 6). The unitary coordination of activities is carried out by the *Cybersecurity Task Force*, called CSTF (Article 8). The Romanian Intelligence Service is designated as national authority in the field of cybersecurity, in which capacity it ensures the technical coordination of the CSTF, as well as the organisation and execution of activities related to the cybersecurity of Romania. To this end, within the Romanian Intelligence Service operates the *National Cybersecurity Centre*, called *NCSC* [Article 10 (1)]. Different authorities are designated in the area of cybersecurity for their fields of activity, ensuring the security of their own cyber infrastructures or of those under their responsibility: The Ministry of National Defence, the Ministry of Interior, the National Registry Office for Classified Information, the Foreign Intelligence Service, the Special Telecommunications Service and the Protection and Guard Service. *The National Centre for Response to Security Incidents*, hereinafter referred to as *CERT-RO*, is a national contact point with CERT structures operating within public authorities or institutions, or other national or international legal persons of public or private law, with respect for the powers of the other relevant authorities and public institutions in this field, according to the law [Article 10 (5)]. The authority involved in the security of cyber infrastructures held or administered by providers of public electronic communications networks or of publicly available electronic communications services is the *National Authority for Management and Regulation in Communications*, called *ANCOM* [Article 13 (2)], an institution established by Government Emergency Ordinance no. 22/2009.

44. A novelty introduced by the impugned law, under Article 10 (1), is the ***designation of the Romanian Intelligence Service as national authority in the field of cybersecurity***, in which capacity it ensures the organisation and implementation of activities relating to the cybersecurity of Romania. To this end, *within the structure of Romanian Intelligence Service operates the National Cybersecurity Centre (NCSC), which has been set up, organised and which already operates within the Romanian Intelligence Service, with specialised military staff, according to certain decisions of the Supreme Council for National Defence.* Public authorities and institutions within the CSTF delegate a representative for the NCSC. According to Article 11 of the law, the main functions of the NCSC cover actions aimed at the identification, prevention, protection, reaction and management of the consequences of cyber threats and attacks; securing data and information exchange between public authorities and institutions that are part of the NCSC; analysis and integration of data and information from public authorities and institutions that are part of the NCSC for establishing, carrying out or proposing all appropriate measures for ensuring cybersecurity; ensuring collection and identification of developments in cyberspace; reception of notifications made by legal persons of public law who hold or manage cyber infrastructures of national interest (CINI); in the event of a cyber attack, ensuring collection and assessment of data and information concerning the incident, making a proposal or taking reactive action of great urgency for ensuring data integrity and for remedying the factual situation, informing the competent bodies for investigation and research or, where appropriate, notifying the criminal investigation bodies.

45. Furthermore, Article 15 (8) of the law sets out *the obligation of all legal persons of public or private law, holders of CINI, to promptly forward the data concerning cybersecurity at their level to the NCSC*, in accordance with their competences under the law.

46. In relation to the designation of the Romanian Intelligene Service, recte the NCSC, as national authority in the area of cybersecurity, the authors of the pleas of unconstitutionality argue that the legislator grants unlimited and unattended access to all computer data held by persons of public and private law to an institution that does not fulfil the condition relating to a civilian body, subject to democratic oversight.

47. In its analysis of constitutionality, the Court departs from the assumption that cybersecurity strategy and the cybersecurity law play an important role in safeguarding the national security of Romania, on the one hand, and the protection of a person against risks on privacy and personal data protection in the online environment, on the other hand. On these aspects analysed jointly, by the Judgement of 6 September 1978 in the Case of *Klass and Others v. Germany*, the European Court of Human Rights held that "Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction" (paragraph 48). However, the Court, aware of the danger inherent in secret surveillance measures, "being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate" (paragraph 49).

48. In this light, the Constitutional Court must verify whether or not the legislation in the field concerned is consistent with the right to personal, family and private life, with the inviolability of the secrecy of correspondence, with the right to the protection of personal data, fundamental values that should be guiding principles of cybersecurity policy at national level, and ensure that the legislation adopted is not conducive to measures that would constitute unconstitutional interference with those rights. That being so, the Court considers that, in order to encourage a climate of order, governed by the principles of the rule of law, democracy, the setting up or identification of a body responsible for coordinating security issues of cyber systems and networks, as well as those related to information, acting as a contact point for relations with similar bodies abroad [as required by Article 10 (4) of the law], including cross-border cooperation at European Union level, must concern a *civilian body that functions entirely on the basis of democratic oversight* and not an authority operating in the field of intelligence, law enforcement or defence or as a structure of any body working in these fields.

49. As regards the provisions of Article 1 (3), first sentence of the Constitution, which enshrine the principle of the rule of law, the Court held in its case-law (see Decision no. 70 of 18 April 2000, published in the Official Gazette of Romania Part I no. 334 of 19 July 2000) that its requirements concerned the major purposes of State activity, anticipated in what is usually called the rule of law, an expression involving the subordination of the State to the Law, enabling those means that would allow the right to censor political options and, in this context, to temper discretionary abusive possible trends of State structures. The rule of law ensures the supremacy of the Constitution, correlation of laws and of all normative acts with the Constitution, the existence of the system of separation of public powers, which must act within the limits of the law, i.e. within the limits of a law expressing the general will. *The rule of law establishes a number of safeguards, including judicial safeguards, to ensure respect for the rights and freedoms of citizens through the self-limitation of the State, respectively that public authorities must act within the law.*

50. In the Court's analysis, the option for the designation as national authority in the field of cybersecurity of a civilian and not a military body acting in the field of intelligence is justified by the need to prevent the risk of deviating the purpose of cybersecurity legislation in the sense of using the powers conferred by this law, by the intelligence services, in order to obtain information and data leading to the infringement of the constitutional rights to personal, family and private life and to the secrecy of correspondence. Or, this is precisely what the law subject

to constitutional review does not circumvent by designating the Romanian Intelligence Service and its militarised structure, the NCSC, in this capacity.

51. Thus, by examining the tasks set out by the legislative acts subject to constitutional review, we can easily identify the intention of the legislator to grant the NCSC the power to collect all data concerning the security of the infrastructure, whatever their nature, both in the public and private sectors. However, if the National Cybersecurity Centre is a military structure as part of an intelligence service, hierarchically subordinated to the management bodies of this institution, and therefore under direct military-administrative control, it is obvious that *such entity does not meet the requirements with regard to the guarantees necessary for ensuring the respect for the fundamental rights relating to personal, family and private life and the secrecy of correspondence*.

52. Furthermore, as the designated national authority serves as national single point of contact in the field of the security of network and information systems, ensuring links with similar bodies in the European Union, the fact that Romania designates an authority which would not meet the demands of the European legislative act, in the process of being adopted, calls into question both a potential alignment of the national regulation with the European law and the effective cooperation between institutions which, although they have the same purpose, are not based on a similar organisational structure and do not operate under democratic oversight.

53. For all of those reasons, the Court finds that **the provisions of Article 10 (1) of the law subject to constitutional review infringe the constitutional provisions of Article 1 (3) and (5) on the rule of law and the principle of legality, as well as those of Article 26 and Article 28 concerning personal, family and private life, respectively the secrecy of correspondence, from the perspective of a lack of safeguards needed to guarantee these rights**.

54. The Court notes that the provisions of Article 2 lay down the scope of the law, in terms of its addressees, stating that legal persons of public or private law subject to the legal provisions, called generically ***holders of cyber infrastructure***s, are: the owners, operators, managers or users of cyber infrastructures, defined in Article 5 g) as infrastructures in the field of information technology and communications, consisting of computer systems, related applications, networks and electronic communications services.

55. The definition of the term "holders of cyber infrastructures" is particularly important because the inclusion in this category involves, for the persons concerned, the obligation to comply with the law, on the one hand, and the justification, for the authorities designated by law with powers in the area of cybersecurity, to order specific measures in their regard.

56. The obligations incumbent on the addressees of the law refer to ensuring cyber infrastructure resilience, respectively the capacity of cyber infrastructure components to resist a cyber incident or attack and to return to normality. This status is maintained upon application of a mix of pro-active and reactive measures to ensure confidentiality, integrity, availability, authenticity and non-repudiation of information in electronic format, of resources and services, public or private, in cyberspace. ***The inclusion of cyber infrastructure users within the scope of the law***, therefore of all legal persons using electronic communications networks and services, raises issues on how they can meet their obligations and responsibilities under the law, when they are not the owners, managers or operators of the cyber infrastructures that they are using; the law, under Article 16, mentions *cyber infrastructures of their own or under their responsibility*. Furthermore, to the extent to which the envisaged obligations and responsibilities lie both with owners, administrators or operators of cyber infrastructure, and users of these infrastructures, and the law does not determine the meaning of the term user, it follows that the obligations and responsibilities shall be exercised concurrently at the level of each system or computer network. For example, according to Article 16 (1) (a) and (b) of the

law, both the owner and the user shall be required to apply security policies, to identify and implement appropriate technical and organisational measures to effectively manage the risks posed to the security. However, security policies, technical measures and, in particular, organisational measures, may sometimes not be considered appropriate by the two entities, they may not coincide or be compatible, so that the objective pursued by law might not be achieved. However, the addressees of the law must have a clear and accurate representation of the legal rules applicable, so as to adapt their behaviour and foresee the consequences of their non-compliance; the lack of foreseeable rules in this respect is a prerequisite of a non-unified and discretionary application in Romania's activity of cyber securisation.

57. In conclusion, since the terms used by the law do not clearly define the scope of the rules contained in the act under review of constitutionality, the Court concludes that the latter does not have a precise and foreseeable nature, and, consequently, **the provisions of Article 2 are in breach of Article 1 (5) of the Basic Law**.

58. The Court holds that all holders of cyber infrastructure shall be covered by Article 16 (setting out their obligations) and Article 17 (establishing the responsibilities that they must fulfil). Among the responsibilities of such persons is also the one ***to grant the necessary support, upon reasoned request*** by the Romanian Intelligence Service, the Ministry of National Defence, the Ministry of Interior, the National Registry Office for Classified Information, the Foreign Intelligence Service, the Special Telecommunications Service, the Protection and Guard Service, CERT-RO and ANCOM, ***in fulfilling their responsibilities, and "allow access to representatives appointed for this purpose to the data held, relevant in the context of the request".*** The legal text requires a double analysis: first, in terms of the type of data to be accessed, second, in terms of the way in which access is granted.

59. On the first point, although the legislation on personal data protection is not expressly mentioned in the law, access to data held by persons subject to the law does not exclude accessing, processing and use of ***personal data***. Furthermore, given that cyber infrastructures consist of computer systems, networks and electronic communications services that facilitate the storage and transfer of data, it is obvious that the type of data contained in these systems and networks include ***data relating to the private life*** of the users. The provision under which access shall be made with regard to "*the data held, relevant in the context of the request*" allows the interpretation that the authorities designated by law must be allowed access to any data stored on these cyber infrastructures, if the authorities deem those data to be relevant. One can thus note the unforeseeable nature of the rule, both in terms of the type of data accessed and in terms of assessment of the relevance of the data requested, likely to allow a discretionary application by the authorities listed in the provision. Thus, the data to which they may request access may concern, for example, logbooks of data storage, processing and transmission systems, technical data, computer systems design data, messages or other content data. The absence of a precise legal regulation to accurately determine the data necessary for identifying the developments that took place in the cyberspace (cyber threats, attacks or incidents), opens up the possibility to abuses by the competent authorities. The regulatory framework in such a sensitive area must be made in a clear, foreseeable and free of confusion manner, so as to remove, insofar as possible, the possibility of abuse or arbitrariness by those called upon to apply the legal provisions.

60. With regard to these issues, the Court has already ruled in an indubitable manner, through Decision no. 440 of 8 July 2014, published in the Official Gazette of Romania Part I no. 653 of 4 September 2014, stating that, "the data subject to regulation, although of predominantly technical nature, are retained in order to provide information about the person and his or her private life. Even if, under Article 1 (3) of the law, this does not apply also to the content of the communication or to the information consulted when using an electronic communications network, the other data retained, aimed at identifying the caller and the person

called, i.e. the user and the recipient of an information communicated electronically, the source, the destination, the date, the time and the duration of a communication, the type of communication, the communication equipment or the devices used by the user, the location of the mobile communication equipment, as well as other 'data needed' — not defined in the law —, are likely to prevent the free manifestation of the right to communication or expression. Specifically, the data concerned allow very precise conclusions concerning the private lives of the persons whose data have been retained, conclusions that could concern the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them . Such a restriction on the exercise of the right to personal, family and private life, secrecy of correspondence and freedom of expression, must occur in a clear, foreseeable and unequivocal manner so as to remove, if possible, the occurrence of arbitrariness or abuse by authorities in this area". (paragraph 56)

61. In addition, the Court of Justice of the European Union held, in its Judgement of 8 April 2014 in the joined cases C-293/12 — *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and others* — and C-594/12 *Kärntner Landesregierung and others*, that the data covered by 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 the invalidated Directive 2002/58/EC allowed very precise conclusions concerning the private lives of the persons whose data have been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them (paragraph 27) and that, in such circumstances, even though, according to Article 1(2) and Article 5(2) of Directive 2006/24, it is prohibited to retain the content of the communications or information consulted when using an electronic communications network, the retention of the data in question might have an effect on the use, by subscribers or registered users of the means of communication covered by that directive and, consequently, on their freedom of expression, guaranteed by Article 11 of the Charter (paragraph 28).

62. Moreover, *access* to data concerning cyber infrastructure data [infrastructure defined by Article 5 (g) of the law as a computer system, related applications, electronic communications networks and services] within the meaning of the law subject to constitutional review overlaps with the notion of "access to a computer system", governed by Article 138 (1) (b) and (3) of the Code of Criminal Procedure, which consists of "entering a computer system or computer data storage medium, either directly or remotely through specialised software or through a network, in order to identify evidence". Furthermore, in the same context, *data held* means "computer data" covered by Article 138 (5) of the Code of Criminal Procedure, which are "any representation of facts, information or concepts in a form suitable for processing in an information system, including software suitable to determine the performance of a function by a computer system". However, access to a computer system in order to obtain such data constitutes one of the particular methods of surveillance or investigation under Article 138 (13) of the Code of Criminal Procedure, which can be ordered only under the conditions of Article 140 (by the judge) or Article 141 (by the prosecutor for a maximum period of 48 hours). In addition, relevant data can also be those generated or processed by providers of public electronic communications networks or by providers of publicly available electronic communications services and retained by them, but, in this case as well, such data can be obtained only upon authorisation by the judge, pursuant to Article 152 of the Code of Criminal Procedure.

63. With regard to the second aspect, the impugned law just lists the authorities that may request access to the data held, upon reasoned request, and it does not establish the modality of an effective access to the data held, so that the persons whose data have been retained have sufficient guarantees to protect them against misuse and unlawful access or use. Thus, the *law* does not provide for objective criteria to limit to a minimum the number of persons who have access and who can subsequently use the data retained and *does not establish that access by national authorities to the data stored is conditional upon the prior review carried out by a court*, thus limiting this access and their use to what is strictly necessary for achieving the objective pursued. The legal safeguards on the actual use of the data retained are not sufficient and appropriate to remove the fear that personal rights, of personal nature, are infringed upon, so that the expression thereof can take place in an acceptable manner (see also Decision no. 440 of 3 May 2012, published in the Official Gazette of Romania Part I no. 527 of 30 July 2012, paragraph 57).

64. ***Requests for access to the data retained for use thereof as provided by law, filed by State bodies designated as cybersecurity authorities for their fields of activity, are not subject to authorisation or approval by the court***, thereby discarding the guarantee of an effective protection of the data retained against the risk of abuse and against any unlawful access and use of such data. This situation is likely to constitute an interference with the fundamental rights to personal, family and private life and to the secrecy of correspondence, and is thus contrary to the constitutional provisions guaranteeing and protecting these rights. The lack of such authorisations has been criticised, *inter alia*, by the Court of Justice of the European Union in its Judgement of 8 April 2014, this lack being tantamount to insufficient procedural guarantees needed to protect the right to privacy and the other rights enshrined in Article 7 of the Charter of Fundamental Rights and Freedoms, and the fundamental right to the protection of personal data, enshrined in Article 8 of the Charter (paragraph 62).

65. In conclusion, in so far as the measures adopted by the law subject to constitutional review are not clear and foreseeable, State interference in the exercise of the constitutional rights to personal, family and private life and to the secrecy of correspondence, although provided for by law, is not clearly, rigorously and exhaustively worded, so as to give public confidence, its strictly necessary nature in a democratic society is not fully justified, and the proportionality of the measure is not ensured by adequate safeguards, we consider that the provisions of **Article 17 (1) (a) of the Law on the cybersecurity of Romania infringe Article 1 (5), Article 26, Article 28 and Article 53 of the Constitution**. Therefore, the restriction on the exercise of these personal rights while taking into account certain collective rights and public interests, relating to cybersecurity, breaks the fair balance that should exist between individual interests and rights, on the one hand, and those of the society, on the other hand, as the impugned law does not establish sufficient guarantees to ensure effective protection of data against the risk of abuse and against any unlawful access and use of personal data (*ad similis*, Decision no. 461 of 16 September 2014, published in the Official Gazette of Romania Part I no. 775 of 24 October 2014, paragraph 44).

66. Further, in its analysis, the Court notes that it follows from the joint reading of the provisions of Article 2, Article 19 and Article 20 of the law that, within the category of cyber infrastructure owners, *a sub-category is created — holders of cyber infrastructures of national interest (CINI)*, which, according to Article 2 (h) of the law, are cyber infrastructures supporting public or public-interest services or information society services, whose impairment may prejudice national security or cause serious damage to the Romanian State or to its citizens. They are listed in the ***CINI Catalogue***, drawn up by the Ministry for the Information Society, upon consultation of the CSTF, upon proposal by the NCSC or, where appropriate, the CERT-RO and ANCOM. According to Article 19 (1), the catalogue ***shall be approved by Government Decision***. ***CINI identification*** *shall be carried out in accordance with the selection criteria*

contained in the methodology developed by the Romanian Intelligence Service and the Ministry for the Information Society and is ***approved by Government Decision.***

67. On these matters, the Court considers that the ***method for determining the criteria for conducting the selection of cyber infrastructures of national interest and, hence, of CINI holders does not comply with the requirements of transparency, certainty and foreseeability.*** Thus, the reference to an infra-legal legislation, i.e. Government Decisions, legislative acts characterised by a high degree of instability, for governing the criteria according to which obligations in matters of national security become applicable, violates the constitutional principle of legality enshrined in Article 1 (5) of the Constitution. The choice for such a regulatory approach appears to be all the more unjustified as, in a similar matter, i.e. that of the identification of national critical infrastructures, Government Emergency Ordinance no. 98/2010 lays down, in its very content, the cross-cutting criteria for the identification of the NCI. Furthermore, the Annex to the legislative act approves the list of national critical infrastructure/European critical infrastructure (NCI/ECI) sectors, sub-sectors and the responsible public authorities (energy, information technology and communications, water supply, food, health, national security, administration, transport, chemical and nuclear industry, space and research). However, the Law concerning cybersecurity, under Article 19, refers to lower level legislation, *and the identification of the CINI is based on a methodology developed by the Romanian Intelligence Service and the Ministry for the Information Society, under a non-transparent procedure, which is not provided for by law, and, therefore, which is likely to be described as arbitrary.*

68. Therefore, the Court concludes that both the ***criteria for the selection of national interest cyber infrastructures and the modality in which they are established must be provided for by law*** *and* ***the primary regulatory legislative act should contain a list as exhaustive as possible of areas in which the legal provisions are deemed applicable.***

69. On the other hand, the Court considers that ***the obligations arising from the Law on the cybersecurity of Romania must be applicable solely to legal persons of public or private law holding or having in their responsibility a CINI (also including, under the law, public administrations)***, as only situations of danger for an infrastructure of national interest may have implications for the security of Romania, given the size, dispersion and accessibility of such infrastructure, the economic effects, assessed depending on the significance of the economic losses and/or degradation of products or services, the effects on the population, assessed according to its impact on public confidence and disruption of daily life; including the loss of essential services. However, the legal provisions in the wording subject to constitutional review are very general, the obligations being aimed at all holders of cyber infrastructures, consisting of computer systems, related applications, networks and electronic communications services regardless of their importance, which may concern the national interest or only the interest of a group or of an individual. To avoid imposing a disproportionate burden on small operators, the requirements should be proportionate to the risks posed to the network or information system concerned and should not apply to holders of cyber infrastructures with insignificant importance from the point of view of the public interest. Therefore, the risks will have to be identified at the level of the entities operating in essential/crucial fields for the proper conduct of national public services, which will have to decide on the measures to be adopted in order to mitigate such risks.

70. For the above reasons, we consider that the **provisions of Article 19 (1) and (3) of the Law on the cybersecurity of Romania infringe the provisions of Article 1 (5) of the Constitution, since they do not meet the requirements of foreseeability, stability and certainty.**

71. Next, the Court notes that the provisions of Articles 20 and 21 (2) of the impugned law establish the ***obligations incumbent on legal persons of public or private law, owners or***

responsible for a CINI, *inter alia*, the obligation to carry out annual cybersecurity audits or to allow such audits upon reasoned request by the competent authorities in accordance with this law, to set up structures or appoint persons responsible for the prevention, detection and response to cyber incidents, to immediately notify, where appropriate, the NCSC, CERT-RO, ANCOM or the authorities designated, in accordance with the law, in the field of cybersecurity on cyber incidents and risks, which, by their effect, can be detrimental in any way to users or beneficiaries of their services. Furthermore, where cyber incidents or risks have been notified, CINI holders are required to enable competent authorities to intervene in order to identify and analyse the causes of cyber incidents, respectively to reduce or mitigate the effects of cyber incidents, to retain and ensure the integrity of the data related to the cyber incidents for a period of 6 months from the date of notification.

72. The law lays down that *these provisions shall not apply to the authorities referred to in Article 10 (1) and (2) of the* law, namely the Romanian Intelligence Service, the Ministry of National Defence, the Ministry of Interior, the National Registry Office for Classified Information, the Foreign Intelligence Service, the Special Telecommunications Service and the Protection and Guard Service. *The Court considers this exemption as unjustified, as the authorities listed, as well, carry out activities in the field of national security, or are holders of/responsible for CINIs* and are likely to be subject to cyber attacks.

73. In accordance with Article 20 (1) (c) of the law, legal persons of public or private law, holding or being responsible for a CINI, ***must allow cybersecurity audits*** upon reasoned request by the competent authorities. Audits are conducted by the Romanian Intelligence Service or by cybersecurity service providers. In other words, as the *Romanian Intelligence Service* is the national authority in the field of cybersecurity, therefore the authority competent, according to the law, to request legal persons of public or private law who own or are responsible for CINIs, to conduct cybersecurity audits, there is a real possibility that *this institution should be concomitantly in the position of the authority requesting the audit, of the authority performing the audit, of the authority to which the result of the audit is communicated and, finally, in the position of the authority that ascertains a possible offence, according to Article 28 (e) of the law, and applies the penalty, according to Article 30 (c) of the law.* Or, *such a situation is unacceptable* in a society governed by the rule of law. The legal provisions are likely to generate a discretionary, even abusive application of the law, being prohibited to have all the tasks in the field covered concentrated within a single institution. *The Court considers that the audit must be carried out by internal auditors or by a qualified independent body* that would verify the compliance of cybersecurity policy implementation at the level of cyber infrastructures and send the result of the assessment to the competent authority or to the single point of contact.

74. Starting from the definition of "cybersecurity audit", laid down in Article 5 (d), which establishes that this is a regular, detailed, measurable and technical assessment of how cybersecurity policies are applied at the level of cyber infrastructures, and also includes the issuing of recommendations to minimise the risks identified, the Court concludes that, within the meaning of this law, such auditing supposes only an assessment of the cybersecurity policies and not access to the data stored in cyber infrastructures.

75. As regards the rule set out in Article 20 (1) (h), namely ***the obligation to immediately notify, where appropriate, the NCSC, CERT-RO, ANCOM or the authorities designated***, in accordance with the law, in the field of cybersecurity with regard to cyber risks and incidents, the Court takes the view that *it should determine the precise circumstances in which notification is necessary, as well as the content of the notification, including the types of personal data which should be notified, and, if necessary, the extent to which the notification and its supporting documents will include details of the personal data affected by a specific security incident (such as IP addresses).* It is important to bear in mind that the competent authorities in the field of networks and information security should be allowed to collect and process personal

data in the context of a security incident only if this is strictly necessary for achieving the objectives of public interest pursued by the law, with due regard for the principle of proportionality. The law must also provide appropriate safeguards to ensure effective protection of the data processed by authorities competent on cybersecurity and must not exclude the obligation to notify breaches of personal data protection under the law applicable, pursuant to Articles 21 and 22 of Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. But, considering the provisions of Article 20 (2), the Court notes that the *legislator delegates its power to legislate to the Ministry for the Information Society, to ANCOM or to the authorities designated, in accordance with the law*, in the field of cybersecurity, which will establish "the minimum requirements for cybersecurity, the modality of notification, as well as the data and information mandatorily accompanying the notification, which are then approved by *orders or decisions* issued within 90 days from the entry into force of the law, *by the governing bodies of the respective public authorities or institutions*, published in the Official Gazette of Romania Part I". ***The reference to administrative acts of a lower regulatory level, in an area critical for national security, with impact on individual fundamental rights and freedoms, infringes the constitutional provisions contained in Article 1 (5) relating to the principle of legality.*** A legal provision must be accurate, unambiguous, it must lay down clear, foreseeable rules whose application should not allow arbitrariness or abuse. Moreover, the rule should regulate in a unitary, uniform manner and should establish minimum requirements applicable to all its addressees. However, as long as the orders or decisions are issued by the managing bodies of the public authorities or institutions designated by law, it is clear that *the law unduly mitigates the regulation in this area*, leaving it up to each entity to determine, on a case-by-case basis, the essential measures, such as minimum requirements in terms of cybersecurity, the methods of notification, as well as the data and information accompanying the notification. Moreover, by listing the authorities that establish these aspects, the legislator has omitted even the Supreme Council for National Defence, which, according to Article 9 (1) (f) of the law, approves the proposals made by the CSTF on the minimum requirements in terms of cybersecurity and cybersecurity policies for the public authorities and institutions referred to in Article 10 (1) and (2) of the law.

76. In conclusion, the Court finds that **the provisions of Article 20 (1) (c) and (h), in conjunction with Article 20 (2) are unconstitutional, as they are contrary to Article 1 (3) and (5), Article 26 and Article 28 of the Constitution.**

77. From the analysis of law, the Court holds that ***it does not regulate the right of the addressees of the law, on whom obligations and responsibilities have been imposed, to challenge in court the administrative acts*** concluded with respect to the fulfilment of such obligations, and which are likely to adversely affect a right or a legitimate interest.

78. According to Article 21 of the Constitution, everyone shall have access to the courts in order to defend their rights, freedoms and legitimate interests. By Decision no. 1 of 8 February 1994, published in the Official Gazette of Romania Part I no. 69 of 16 March 1994, the Constitutional Court held that free access to justice entailed access to any procedural means whereby the act of justice is carried out. The Court considered that the legislator had the exclusive competence to determine the rules for conducting the trial before the courts, as it clearly results from Article 126 (2) of the Constitution. Furthermore, in its case-law (Decision no. 71 of 15 January 2009, published in the Official Gazette of Romania, Part I, no. 49 of 27 January 2009), the Court held that free access to justice was fully respected whenever the party concerned, in order to assert a right or legitimate interest, has been able to address at least once to a national court.

79. On the other hand, under Article 6 § 1 of the Convention for the Protection of Human Rights and Fundamental Freedoms, everyone has the right to a fair trial by an independent and

impartial tribunal, which will decide on the infringement of his civil rights and obligations. The European Court of Human Rights ruled in its case-law, in general terms, that Article 6 § 1 of the Convention guaranteed everyone's right to bring before the courts any claims relating to civil rights and obligations (see Judgement of 21 February 1975 in the Case of *Golder v. the United Kingdom*, paragraph 36, and Judgement of 20 December 2011 in the Case of *Dokic v. Serbia*, paragraph 35). Likewise, in the Judgement of 26 January 2006 in the Case of *Lungoci v. Romania*, paragraph 36, published in the Official Gazette of Romania, Part I, no. 588 of 7 July 2006, it was stated that free access to justice involved, through its very nature, a State regulation and could be subject to limitations, as long as it did not infringe the essence of the right.

80. Romania is a State governed by the rule of law, in which, according to Article 1 (5) of the Constitution "observance of the Constitution, of its supremacy, and the laws shall be obligatory". Where Article 20 (1) of the Constitution provides that the constitutional provisions on citizens' rights and freedoms shall be interpreted and applied in compliance with the Universal Declaration of Human Rights, the covenants and other treaties to which Romania is party, and Article 21 of the Constitution enshrines the free access to justice, whose exercise, under paragraph (2), may not be restricted by any law, that Parliament has a duty to legislate appropriate rules to ensure actual compliance with that right, in the absence of which the existence of the rule of law, laid down by Article 1 (3) of the Constitution, is inconceivable. Without complying with this duty, the constitutional rules referred to would be purely declaratory, which is inadmissible for a State that shares the democratic values that are part of the European public policy, as shaped by the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union (see, to that effect, the Constitutional Court Decision no. 233 of 15 February 2011, published in the Official Gazette of Romania, Part I, no. 340 of 17 May 2011).

81. In the light of those considerations of principle, the Court finds that **the lack of any provision in the law that would ensure the possibility, for a person whose rights, freedoms or legitimate interests have been affected by acts or facts that are based on the provisions of the Law on the cybersecurity of Romania, to address themselves to an independent and impartial court is contrary to Article 1 (3) and (5), Article 21 and Article 6 of the Convention for the Protection of Human Rights and Fundamental Freedoms.**

82. In accordance with Article 27 (1), the monitoring and control of the implementation of the impugned law are ensured, in accordance with the competences established by law, by the Chamber of Deputies, the Senate, the Presidential Administration, the Government, the SCND and the public institutions and authorities referred to in Article 10 (1) and (2), for their own cyber infrastructures or for those under their responsibility, by the Romanian Intelligence Service for its own cyber infrastructures owned or for those under its responsibility, as well as for holders of CINIs, legal persons of public law, by the Ministry for the Information Society, respectively by ANCOM, as appropriate, for holders of CINIs, legal persons of private law.

83. ***The choice of the legislator to confer jurisdiction for monitoring and controlling the implementation of the legal provisions to the Chamber of Deputies, the Senate, the Presidential Administration, the General Secretariat of the Government and the SCND***, whereas Article 10 (1) and (2) lays down the competent authorities in the field of cybersecurity concerning their own cyber infrastructures or of those under their responsibility, without including in this category the authorities listed above, which are mentioned throughout the entire legislative act as legal persons of public law, and which must comply with the obligations set by law, ***indicates inconsistency and generates confusion as to the legal regime applicable to these institutions***. From the combined interpretation of Article 20 (1) and Article 21 (1) (a), it follows that, on the one hand, the Parliament, the Presidential Administration, the General Secretariat of the Government and the SCND have, for example, the obligation to allow

cybersecurity audits carried out by the Romanian Intelligence Service or to notify the SCND about cyber incidents and risks and, on the other hand, *they will monitor and verify compliance with these obligations and, in case of non-compliance with the legal provisions set forth under Article 28 in conjunction with Article 30 (c) of the law, the authorities will apply sanctions to themselves, upon finding of infringements.* Therefore, the Court notes that the legislator is circumventing the legal principles stating that the control must be carried out by an independent authority, separate from the controlled authority, and, by the rules adopted, it renders illusory the compliance with the obligations related to cybersecurity. Furthermore, the provisions under which the Parliament, the Presidential Administration, the General Secretariat of the Government and the SCND become agents reporting the infringements committed and applying civil sanctions, show disregard of the principles of law governing a democratic State, namely **the principle of separation of State powers, provided for by Article 1 (4) of the Constitution, and the principle of legality enshrined in Article 1 (5).** Thus, by virtue of the impugned law, the legislative authority, the Presidential Administration, the Government or the SCND, authorities of constitutional status, whose powers are specifically provided for in the Basic Law, *are subrogated to the tasks that, according to Government Ordinance no. 2/2001 on the legal regime of infringements (which is, moreover, referred to in the impugned law), lie with the central or local government bodies.*

84. On the other hand, the Court notes that ***the law subject to review does not establish powers of control and monitoring in relation to all holders of cyber infrastructures***, A*rticle 27 (1) setting out these powers only in respect of legal persons of public or private law holding CINIs*. However, while the law provides, in Articles 15, 16 and 17, duties and responsibilities for all legal persons of public or private law holding cyber infrastructures, and Article 28 (a), (b), (c) qualifies as infringement non-compliance with those obligations, *the legislative omission regarding the authority competent to supervise owners of infrastructure who are not qualified as CINIs* **vitiates the constitutionality of the legal text contained in Article 27 (1), in relation to Article 1 (5) of the Constitution.** The rules laid down in administrative matters, both in relation to the conduct complained of and to the procedure for finding and sanctioning it must be clear, precise and foreseeable in order to ensure that the addressee can adapt its conduct so as to comply with the legal provision.

85. The Court also notes that the provisions of ***Article 30*** of the law contain provisions on the finding of infringements and the application of penalties. The Court made a first observation with regard to ***the confusion generated by the legal text due to a non-correlation with Article 28*** which enshrines the infringements resulting from the failure to comply with the legal provisions. Thus, the Court identifies: *the failure to identify the authority competent to find and apply a penalty for the infringements* listed in Article 28 (i) and (j) and committed by legal persons of private law; *the failure to identify the authority competent to find and apply a penalty for the infringements* listed in Article 28 (a), (i) and (j) and committed by legal persons of public law; *civil sanctions set forth in Article 30 (c) for breach of obligations* by the public authorities and institutions referred to in Article 27 (1) (a) of the law, with regard to their own cyber infrastructures, obligations *from which they were exempted* under Article 20 (1), second sentence [infringements laid down by Article 28 (e) to (h) of the law].

86. In its case-law, the Constitutional Court has repeatedly stated that any piece of legislation must fulfil certain qualitative criteria, such as foreseeability, implying that *it must be sufficiently precise and clear in order to be applied* (see, for example, Decision no. 189 of 2 March 2006, published in the Official Gazette of Romania Part I no. 307 of 5 April 2006, Decision no. 903 of 6 July 2010, published in the Official Gazette of Romania Part I no. 584 of 17 August 2010, or Decision no. 26 of 18 January 2012, published in the Official Gazette of Romania, Part I, no. 116 of 15 February 2012). In the same vein, the European Court of Human Rights ruled that the law must be accessible to individuals and foreseeable as to its effects. In

order for the law to satisfy the requirement of foreseeability, it must define with sufficient clarity the scope and manner of exercising the discretion of the authorities in this area, in the light of the legitimate aim pursued, so as to give the individual adequate protection against arbitrariness. Furthermore, only *a rule formulated with sufficient precision, so as to enable any individual to regulate his/her conduct* can be considered a "law"; if need be, with expert advice, the individual must be able to foresee, to a reasonable extent, having regard to all the circumstances of the case, the consequences that may follow from a given act (see Judgement of 4 May 2000 in the Case of *Rotaru v. Romania*, paragraph 52, and Judgement of 25 January 2007 in the Case of *Sissanis v. Romania*, paragraph 66).

87. That being so, the Court considers that the lack of precision in the legislation subject to constitutional review, consisting of *the failure to establish with sufficient clarity the monitoring and control procedures and those on the finding and the sanctioning of infringements*, also affects, as a consequence, the guarantees set forth in the Convention and in the Constitution on the right to a fair trial, including those related to the right of defence. Moreover, the European Court of Human Rights held, in essence, that non-compliance with the fundamental guarantees, which protect the alleged perpetrators of offences against possible abuse by the authorities designated to prosecute and punish them, was an issue to be examined under Article 6 of the Convention for the Protection of Human Rights and Fundamental Freedoms (see, for example, Judgement of 4 October 2007 in the Case of *Anghel v. Romania*, paragraph 68).

88. In order for the right to a fair trial not to remain theoretical and illusory, rules of law must be clear, precise and comprehensible, so as to be able to clearly warn their recipient of the seriousness of the consequences of non-compliance with the legal wordings set out therein. In the light of the above, the Court holds that, obviously, the provisions of Articles 27 (1) and 30 of the law, characterised by a poor legislative technique, **do not meet the requirements of clarity, precision and foreseeability and are therefore incompatible with the fundamental principle concerning the observance of the Constitution, its supremacy and the law, provided for by Article 1 (5) of the Constitution and with the right to a fair trial, provided for by Article 21 (3) of the Constitution and by Article 6 of the Convention for the Protection of Human Rights and Fundamental Freedoms.**

89. In accordance with Article 27 (2) of the law, during the monitoring and control activities, the persons designated by the managing bodies of the authorities set forth in Article 27 (1) ***are entitled to request declarations or any document needed in order to carry out the control, to conduct inspections, even unannounced inspections, on any facilities, premises or infrastructure intended for CINIs***, and receive, upon request or on the spot, information or supporting documents. The rule laid down in Article 27 (2) (b), which allows the public authorities listed in Article 10 (1) and (2) of the law to conduct inspections at any facilities, premises or infrastructure intended for CINIs, under their responsibility, requires access to a specific location, with respect to certain objects, computer systems for data storage, processing and transmission, including of personal data, access that calls into question the protection of the constitutional rights to personal, family and private life and to the secrecy of correspondence. In so far as the concepts with which the law operates (facilities, premises and infrastructures) are not determined in a foreseeable manner and the scope of the data subject to control is uncertain, the Court considers that the impugned law does not regulate guarantees to allow an effective protection against the risk of abuse and against any unlawful access and use of personal data. While the concept of cyber infrastructure is defined by law, the concept of *facility* used in the text of Article 27 (2) (b) may be a computer system or network or an electronic communications service, given the scope of the law and the definitions contained therein, so that access to these information systems would not be permitted without an authorization by the judge. Also, the notion of *premises* can mean also the location of these

information systems, in which case the Court finds that the provisions on home search, provided for by Articles 157 to 167 of the Code of Criminal Procedure, are applicable, in the sense that this measure can only be ordered by a judge.

90. In view of the above, the reference to "*compliance with the legal provisions in force*" is confusing, because neither the provisions of the Code of Criminal Procedure mentioned above nor the provisions of other legislative acts are indicated as applicable provisions.

91. Therefore, the reasons set forth in the Constitutional Court Decisions no. 440/2014 and no. 461/2014 apply *mutatis mutandis*, so that the arguments mentioned before, on the unconstitutionality of the provisions of Article 17 (1) (a) of the Law on the cybersecurity of Romania, are fully sustainable also as regards **the provisions of Article 27 (2) of the law.** That being so, the Court concludes that **they infringe the provisions of Article 1 (5), of Article 26, of Article 28 and of Article 53 of the Constitution.**

92. Beyond the specific aspects whose unconstitutionality was reasoned above, the Court notes that the entire legislative act is marked by flaws in terms of compliance with the rules of legislative technique, clarity, coherence, foreseeability, **likely to entail a breach of the principle of legality enshrined in Article 1 (5) of the Constitution.** The Law makes references, in several cases, to *the regulation of aspects which are essential in the field governed by secondary legislation*, such as Government decisions, methodological standards, orders or decisions or "mutually agreed procedures". See, in this regard, the provisions of Article 15 (2), Article 17 (1) (b), Article 19 (1) and (3), Article 20 (2), Article 23 (2), (5) and (6) and Article 30 (d) of the law.

93. Furthermore, except where the reference concerns specifically the cybersecurity law, in which case the term used was "this law", *the law repeatedly uses the terms "in accordance with the law", "according to the competencies laid down by law" or "under the terms of the law", without specifying the provisions of the laws to which the reference is made.* That is the case in Article 7 (1) (d), Article 10 (2) and (5), Article 11 (1) (j), Article 15 (8), Article 19 (6), Article 20 (1) (h), Article 21 (1), Article 21 (2) (d), Article 27 (1), Article 27 (2) (b) of the law. With regard to these issues, the Court notes that, according to Article 39 (1) — *Reference to another legislative act*, in Law no. 24/2000 on the rules of legislative technique for drafting normative acts, ***"reference in a legislative act to another legislative act is made by specifying the legal category thereof, the number, the title and the date of publication of that act*** *or only the legal category and the number, if by doing so any confusion is excluded."*

94. Moreover, the Court notes that the provisions of Article 6 (1), Article 8 (1) and Article 10 (1), second sentence of the law enshrine ***bodies/institutions/authorities established under previous legislative acts, i.e. Government decisions (NSCS and CSTF) or decisions by the Supreme Council for National Defence (SCND)***, which have preceded the primary regulatory act establishing the general framework regulating cybersecurity. Thus, their adoption creates confusion so as to the setting of the date on which these entities come into existence and exercise their powers — date of adoption of the Government/SCND decision or the date on which the Law on the cybersecurity of Romania will take effect.

95. With regard to the issues concerning the criteria of clarity, precision, foreseeability and predictability that a law must meet, the Court notes that the legislator, the Parliament or the Government, as the case may be, is required to lay down rules that comply with the characteristics given above. According to the first sentence of Article 8 (4) of Law no. 24/2000, *"the legislative text must be worded clearly, fluently and understandably, without syntactic difficulties and obscure or ambiguous fragments"*, and according to Article 36 (1) of the same law *"the legislative acts must be written in a specific, concise, sober, clear and precise legal regulatory language and style, which would exclude any misunderstanding, with strict compliance with the grammatical and spelling rules*".

96. The Court finds that, through the regulation of the legislative drafting rules, the legislator has imposed a number of criteria required for the adoption of any legislative act, whose observance is necessary for ensuring the systematisation, uniformity and coordination of legislation, as well as the appropriate legal form and content for every legal instrument. Thus, compliance with these rules contributes to ensuring a legislation that complies with the principle of legal certainty, possessing the required clarity and foreseeability.

97. For all of the foregoing considerations, **the Court finds that the Law on the cybersecurity of Romania is vitiated in its entirety, so that the objection of unconstitutionality is to be accepted and the legislative act is to be declared unconstitutional in its entirety.**

98. In accordance with its case-law, the Court notes that once the law is declared unconstitutional in its entirety, such a decision has a final effect on the legislative act, i.e. the legislative process in respect of that provision ceases as of right.

99. On the other hand, whereas the provisions of Article 61 (1) of the Constitution stipulate that "Parliament is the supreme representative body of the Romanian people and the sole legislative authority of the country", its law-making competence in relation to a certain area cannot be limited if the law thus adopted complies with the requirements of the Basic Law. Therefore, the legislator's decision to legislate in matters in which the Constitutional Court has accepted a referral of unconstitutionality concerning a law in its entirety implies going through all the phases of the legislative process provided for in the Constitution and in the Standing Orders of the two Chambers of Parliament (see, to this effect, the Constitutional Court Decision no. 308 of 28 March 2012, published in the Official Gazette of Romania, Part I, no. 309 of 9 May 2012).

100. For the reasons set forth herein, on the grounds of Article 146 (a) and of Article 147 (4) of the Constitution, as well as of Article 11 (1) A.a), of Article 15 (1) and of Article 18 (2) of Law no. 47/1992, by majority vote,

THE CONSTITUTIONAL COURT

In the name of the law

DECIDES:

Allows the objection of unconstitutionality and finds that the Law on the cybersecurity of Romania is unconstitutional, in its entirety.

Final and generally binding.

The decision shall be communicated to the President of Romania, to the presidents of the two Chambers of Parliament and to the Prime Minister, and it shall be published in the Official Gazette of Romania, Part I.

Delivered in public hearing on 21 January 2015.