Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

Articles

Studia Iuridica Lublinensia vol. 34, 1, 2025
DOI: 10.17951/sil.2025.34.1.29-52

Emilia Lucia Cătană
"Dunărea de Jos" University of Galați, Romania
"Dimitrie Cantemir" University of Târgu-Mureș, Romania
ORCID: 0000-0002-3216-2683
luciacatana@yahoo.fr

An Administrative Law Approach of Cybersecurity Rules: The Case of Romania in the Context of EU and International Law

Administracyjnoprawne podejście do zasad cyberbezpieczeństwa. Przypadek Rumunii w kontekście prawa unijnego i międzynarodowego

ABSTRACT

Considering insufficient legal research, from the perspective of administrative law, of current cybersecurity regulations, the overall purpose of the paper is an administrative law approach of cybersecurity regulations, with emphasis on the Romanian case in the context of European Union and international law. The research hypotheses of the interface between administrative law and the cybersecurity rules cover three dimensions: the regulation of cybersecurity institutional capacity, the regulation of administrative decision-making and, respectively, administrative and judicial remedies. Analytical and comparative methods are used, with the role of case law. In international law, the conclusions of the study highlight the rules established by international agreements. In EU law, the NIS 2 Directive establishes public administration entities of central government of the Member State as "essential entities", a set of administrative decision-making regulations and, respectively, administrative and judicial remedies. In Romania, the internal legal framework has been harmonized with EU law. The Law No. 58/2023 establishes responsibilities of public authorities and bodies which are "competent authorities" in this field. There are two categories of administrative acts in the administrative decision-making procedure established by this law, which can be appealed in administrative contentious.

Keywords: cybersecurity; administrative law; institutional capacity; decision-making procedure; administrative and judicial remedies

CORRESPONDENCE ADDRESS: Emilia Lucia Cătană, PhD, Professor, "Dunărea de Jos" University, Faculty of Law and Administrative Sciences, Doctoral School of Social and Human Sciences, State str., no. 111, Galați, Romania, and "Dimitrie Cantemir" University, Bodoni Sandor str., no. 3-5, Târgu-Mureș, Romania.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

INTRODUCTION

Cybersecurity is a complex multi-faceted issue, involving several areas such as law enforcement, national and international security, international relations, trade negotiations and sustainable development.[1]

Information and Communications Technologies (ICTs) are now woven into every facet of human activity, from operating nuclear arsenals to raising cows.[2] Dependence on information technologies is growing. For this reason, "malicious cyber operations can cause serious harm to individuals, industry and states"[3] and "cyber insecurity has become the new normal, making cybersecurity a global priority not just for ICTs companies but for nation-states, industry, and users generally".[4] The consequences of cyberattacks are devastating "for the civilian population of victim states, especially if directed at critical infrastructure".[5]

The implications of digital transformation vary on geographical and demographic criteria, so, "ideally a cross-border framework should be put into place to ensure that digitalization and datafication yield benefits not only to the few".[6]

In the United Nations (UN) Charter[7] the maintenance of "international peace and security" is a first purpose.[8] The 2015 UN report indicates that states "should not knowingly allow their territory to be used for internationally wrongful acts using ICTs".[9] Reaffirming the UN Global Counter-Terrorism Strategy[10] and its

---

[1] See International Telecommunication Union, *Strategic Engagement in Cybersecurity: Guide to Developing a National Cybersecurity Strategy*, Geneva 2021, p. 28.

[2] See M. Finnemore, D.B. Hollis, *Constructing Norms for Global Cybersecurity*, "American Journal of International Law" 2016, vol. 110, p. 425.

[3] N. Tsagouria, M. Farrell, *Cyber Attribution: Technical and Legal Approaches and Challenges*, "The European Journal of International Law" 2020, vol. 31(3), p. 941.

[4] M. Finnemore, D.B. Hollis, *Constructing Norms…*, p. 426.

[5] J.M. Lemnitzer, *Back to the Roots: The Laws of Neutrality and the Future of Due Diligence in Cyberspace*, "The European Journal of International Law" 2022, vol. 33(3), p. 790.

[6] See S. Peng, *The Uneasy Interplay between Digital Inequality and International Economic Law*, "The European Journal of International Law" 2022, vol. 33(1), pp. 206–207.

[7] Charter of the United Nations (adopted on 26 June 1945, entered into force on 24 October 1945).

[8] See D. Franchini, *Extraterritorial Sanctions in Response to Global Security Challenges: Countermeasures as Gap-Fillers in the United Nations Collective Security System*, "Cambridge International Law Journal" 2023, vol. 12(1), p. 131.

[9] United Nations, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 22.7.2015, A/70/174, § 13 (c), after A. Coco, T. de Souza Dias, *'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law*, "The European Journal of International Law" 2021, vol. 32(3), p. 772.

[10] Resolution adopted by the General Assembly on 8 September 2006: The United Nations Global Counter-Terrorism Strategy, A/RES/60/288.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

four pillars, the UN recognizes the principal responsibility of Member States to implement the Strategy.[11]

The great acceleration of government digitalization that the pandemic had engendered was irreversible, with profound effects on the sharing of data and information and public service delivery, as well as opportunities for collaboration within government and with citizens and other actors.[12] After the pandemic, the world is facing a multitude of crises, including security spectrums, and this involves accelerating international cooperation.[13] The uneven playing field in science and technology and the market dominance of some technology companies contributed to limiting options for governments in the application of artificial intelligence, neural networks, access to big data and other technologies and those factors introduced security vulnerabilities, which some governments were tackling by restricting access rather than cooperating[14] (dimensions of e-Procurement which demonstrates the involvement of competent institutions and the regulation of cybersecurity in this matter).

Thus, "the capacity-building for law enforcement in cybersecurity needs to be promoted".[15] Efforts to construct new and better cybernorms mean "accommodating or at least recognizing the existing contexts in which norms are sought".[16] Reality of "the lack of international rules"[17] and "the reluctance to invoke international law might suggest that law is weak – or worse, irrelevant – in holding state actors accountable for their cyber operations".[18] In particular, the World Trade Organization (WTO) law "could still be the proper framework in which States may seek harmonization of technical standards related to cybersecurity issues".[19] Also, GATT 1994,[20] (GATS)/

[11] Resolution adopted by the General Assembly on 22 June 2023: The United Nations Global Counter-Terrorism Strategy, A/RES/77/298.

[12] United Nations, *Committee of Experts on Public Administration: Report on the Twenty-First Session (4–8 April 2022)*, New York 2022, p. 24.

[13] United Nations, *The Sustainable Development Goals Report 2022*, New York 2022, p. 60.

[14] United Nations, *Committee of Experts on Public Administration: Report…*, p. 24.

[15] International Telecommunication Union, *Strategic Engagement in Cybersecurity…*, p. 49.

[16] T. Erskine, M. Carr, *Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace*, [in:] *International Cyber Norms: Legal, Policy & Industry Perspectives*, eds. A.-M. Osula, H. Rõigas, Tallinn 2016, pp. 87–88; M. Finnemore, D.B. Hollis, *Constructing Norms…*, p. 425.

[17] A. Oddenino, *Digital Standardization, Cybersecurity Issues and International Trade Law*, "Questions of International Law" 2018, vol. 51, p. 49.

[18] M. Finnemore, D.B. Hollis, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, "The European Journal of International Law" 2020, vol. 31(3), p. 973.

[19] A. Oddenino, *op. cit.*, pp. 49–50.

[20] General Agreement on Tariffs and Trade (GATT) 1994/WTO is contained in Annex 1A of the WTO Agreement. It incorporates by reference the provisions of the GATT 1947, a legally distinct international treaty applied provisionally from 1948 to 1995.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

WTO,[21] TRIPS[22] and GPA[23] "allow governments to take action when necessary in cases of essential security interest".[24] However, the WTO agreements (including GATS and TRIPS) "are largely considered inadequate to deal with the manifold and complex issues arising from the modern-day digital economy, if only due to the fact that they were adopted more than twenty years ago".[25] The WTO, a trade institution, "is not the best placed body to deal with several aspects of digital trade, such as setting standards on cybersecurity or data protection".[26]

Also, "in relation to digital evidence, it should be noted that its legal significance can be affected by the fact that its probity depends on verification and authentication".[27] For example, in international law are relevant the difficulties that may arise in judicial remedies, in particular "the collection of hard evidence" and "the state that has jurisdiction may not consent to or cooperate with such investigations".[28]

In the context of international law and multiple cybersecurity challenges, we believe that a multidisciplinary research endeavour on the complex and ever-expanding cybersecurity law, from the perspective of interference with other branches of law, is a necessity. The research hypotheses take into account that further research is needed from the perspective of the many interfaces between administrative law and cybersecurity rules. The research focuses in particular on the interface between administrative law and cybersecurity regulation, in the EU as well as in Romania, as an EU Member State.

For administrative law researchers, the principal challenge is to identify the many interfaces between administrative law and the emerging digital world.[29] In the approach of this study, taking into account the research hypotheses presented in the introductory part, methodologically, the interface between administrative law and cybersecurity rules is analysed under three dimensions, at the EU and Romanian level: the regulation of cybersecurity institutional capacity (responsible public authorities and institutions), the regulation of administrative decision-making procedure and administrative and judicial remedies. We use the analytical method and the comparative

[21] The General Agreement on Trade in Services (GATS)/WTO came into effect in 1995.

[22] The Trade-Related Aspects of Intellectual Property Rights (TRIPS)/WTO came into effect on 1 January 1995.

[23] The Agreement on Government Procurement (GPA); the first agreement on government procurement (sometimes referred to as the "Tokyo Round Code on Government Procurement") was signed in 1979 and entered into force in 1981.

[24] See S. Peng, *Cybersecurity Threats and the WTO National Security Exceptions*, "Journal of International Economic Law" 2015, vol. 18(2), p. 450.

[25] A. Oddenino, *op. cit.*, p. 49.

[26] *Ibidem*.

[27] N. Tsagouria, M. Farrell, *op. cit.*, p. 957.

[28] *Ibidem*.

[29] P. Daly, J. Raso, J. Tomlinson, *Researching Administrative Law in the Digital World*, [in:] *A Research Agenda for Administrative Law*, ed. C. Harlow, Aldershot 2023, p. 255.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

method, without ignoring the role of jurisprudential analysis. The study highlights cybersecurity in the context of international law, with a legal, literature and case-law approach, which we believe is meant to better understand compliance and enforcement of this issue by the EU and Member States (particularly Romania). Therefore, Romania as a particular subject of analysis is intended to conduct research into the details of the topic, as reflected in an EU Member State. Following the methodology detailed above, the study is structured as follows: an introductory part analyzes the international context of cybersecurity; a consistent section of research and results analyzes the interface between administrative law and the EU cybersecurity rules (first subsection) and, respectively, administrative law in the Romanian cybersecurity legal framework (second subsection); final section of discussion and conclusions.

RESEARCH AND RESULTS

1. The interface between administrative law and the EU cybersecurity rules

1.1. Institutional capacity (responsible public authorities and institutions)

The system of public administration has a key role in preventing and combating conflicts in society. According to the doctrine, this feature also attracts the vulnerability of legal and administrative system.[30] Therefore, the EU's concern for legislation which creates the framework for preventing and fighting these vulnerabilities is a necessary step.

Directive (EU) 2022/2555 (known as NIS 2)[31] entered into force in 2023, replacing the first Network and Information Systems (NIS) Directive (EU) 2016/1148.[32] In terms of cybersecurity institutional capacity (responsible public authorities and institutions), we notice that in the NIS 2 Directive public administration entities of central government are considered "essential entities".[33] In the sense of the NIS 2 Directive, "public administration entity" means "an entity recognised as such in a Member State in accordance with national law", not including "the judiciary, parliaments or central

[30] R. Sannerholm, *Legal, Judicial and Administrative Reforms in Post-Conflict Societies: Beyond the Rule of Law Template*, "Journal of Conflict & Security Law" 2007, vol. 12(1), p. 70.

[31] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333/80, 27.12.2022).

[32] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194/1, 19.7.2016).

[33] Article 3 and Article 2 (2) (f) (i) of the NIS 2 Directive.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

banks".[34] The NIS 2 Directive requires Member States "to designate or establish one or more competent authorities responsible for cybersecurity and for the supervisory tasks",[35] "to designate or establish one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises".[36]

The EU Cybersecurity Act[37] strengthens the EU Agency for Cybersecurity (ENISA). Considering the research topic we proposed, we emphasize that, according to the EU Cybersecurity Act, one of the important tasks of ENISA is to contribute to the development and implementation of EU law, including regarding supporting Member States in the implementation of EU specific cybersecurity regulations relating to data protection and privacy. We believe that reference is made especially to the General Data Protection Regulation (GDPR)[38] which is "the most consequential regulatory development in information policy in a generation".[39] We also believe that this task of ENISA emphasizes the responsibility of the Member States to respect the GDPR in the establishment and application of the legal provisions regarding cybersecurity, especially with regard to data protection and data security risks (e.g. in the particular case of long-term data storage).

Assuming the mission to achieve a high common level of EU cybersecurity, ENISA has developed guiding documents, e.g. in public procurement.[40] These measures are the consequence of the complex dimension of electronic public procurement (e-Procurement) at the EU level and Member States. It must be stated that the idea of electronic public procurement has been offered as one of possible avenues of institutional quality improvement.[41] Following the publication of a Green Paper

[34] Article 6 (35) of the NIS 2 Directive.

[35] Article 8 (1) of the NIS 2 Directive.

[36] Article 9 (1) of the NIS 2 Directive.

[37] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act) (OJ L 151/15, 7.6.2019).

[38] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119/1, 4.5.2016). It was established in 2016 but wasn't enforced until May 2018.

[39] C.J. Hoofnagle, B. van der Sloot, F.Z. Borgesius, *The European Union General Data Protection Regulation: What It Is and What It Means*, "Information & Communications Technology Law" 2019, vol. 28(1), p. 66.

[40] See European Union Agency for Cybersecurity, P. Kyranoudi, D. Liveri, A. Drougkas, A. Zisi, *Procurement Guidelines for Cybersecurity in Hospitals – Good Practices for the Security of Healthcare Services*, European Network and Information Security Agency, 2020.

[41] T.J. Emery, L. Mélon, R. Spruk, *E-Procurement and Institutional Quality: Friends or Foes? Evidence from Catalonia*, [in:] *Sustainability in Public Procurement, Corporate Law and Higher Education*, ed. L. Melon, London 2023, p. 122.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

in this field,[42] e-Procurement is reflected in the EU Public Procurement Directive.[43] The EU introduced a detailed e-Procurement timeline, finishing with mandatory use of eForms by the autumn of 2023. This involves "electronic invoicing systems, automated contract renewal, automated data input (robotisation), smart data gathering, automated answers to questions of suppliers, the use of AI (Artificial Intelligence) in the assessment of offers, and perhaps even automated tendering for simple purchases",[44] which, as we have already expressed, are dimensions of e-Procurement which demonstrates the involvement of competent institutions and the regulation of cybersecurity in this matter.

1.2. Administrative cybersecurity decision-making

On 9 September 2021, the JURI Committee[45] was authorised to draw up a legislative own-initiative report on digitalisation and administrative law,[46] which underlines recommendations, including a regulation laying down a general act relating to administrative procedure. According to this document, development and deployment of digital solutions is a process which should also recognize "a high level of cybersecurity" which must be insured "with a proactive approach" as well as measures which it should ensure the development and use of digital solutions to support "the rule of law and citizens' rights".

Since 2001, the European Parliament has been calling for an "open, efficient and independent" EU administration.[47] The problems identified remain, in particular, as regards digitalisation, e.g. the use of "automatic" decision-making, which "could raise concerns of compliance with fundamental rights, data protection, inclusiveness and non-discrimination, and with principles such as technological neutrality".[48] The term "automated systems" refers to different information technologies designed either to "produce measurements or assessments" regarding a particular case, or

[42] Green Paper from the European Commission of 18 October 2010 on expanding the use of e-Procurement in the EU, COM(2010) 571 final.

[43] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94/65, 28.3.2014).

[44] J. Grandia, L. Volker, *Ways Forward in Public Procurement*, [in:] *Public Procurement Theory, Practices and Tools*, eds. J. Grandia, L. Volker, Cham 2023, p. 141.

[45] The European Parliament's Committee on Legal Affairs.

[46] European Parliament, Procedure file 2021/2161(INL), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/2161(INL)&l=en (access: 29.4.2025).

[47] L. Jančová, M. Fernandes, *Digitalisation and Administrative Law: European Added Value Assessment*, Brussels 2022, p.1.

[48] European Parliament resolution of 20 May 2021 on shaping the digital future of Europe: removing barriers to the functioning of the digital single market and improving the use of AI for European consumers (2020/2216(INI)) (OJ C 15/204, 12.1.2022).

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

"designed to make an administrative decision in lieu of a human decision-maker".[49] According to the literature, "most existing administrative law principles can already accommodate the widespread adoption of automation throughout the administrative state",[50] but "digital government and automated government decisions can give rise to forms of situational vulnerability".[51]

A legal basis to regulate the EU administration so as to achieve "greater transparency, efficiency and independence"[52] can be found in Article 298 TFEU.[53] Also, Article 41 of the Charter of Fundamental Rights[54] provides for the right to good administration. This provision is based on general principles,[55] such as the right of every person to be heard or to have access to his/her file, the obligation to motivate public decisions. The Court of Justice of the European Union (CJEU) has stated that these principles do apply to individual Member States.[56]

The main focus of any potential regulation based on Article 289 TFEU should remain on providing default administrative procedures and building on certain existing rules regulating digital activity.[57]

However, we note that the NIS 2 Directive establishes a set of decision-making rules, such as:

- the "notification" procedure: the Member States must ensure that essential[58] and important entities "notify" its competent authority, of any significant incident, and the European Commission may adopt "implementing acts"

[49] M.H. Cheng, H.C. Kuen, *Towards a Digital Government: Reflections on Automated Decision-Making and the Principles of Administrative Justice*, "Singapore Academy of Law Journal" 2019, vol. 31(2), p. 878.

[50] C. Coglianese, *Administrative Law in the Automated State*, "Daedalus" 2021, vol. 150(3), p. 105.

[51] S. Ranchordás, *Empathy in the Digital Administrative State*, "Duke Law Journal" 2022, vol. 71(6/4), p. 1362.

[52] L. Jančová, M. Fernandes, *op. cit.*, p. 15.

[53] Treaty on the Functioning of the European Union, consolidated version (OJ C 326/47, 26.10.2012).

[54] Charter of Fundamental Rights of the European Union (OJ C 326/391, 26.10.2012).

[55] In administrative law, legal principles are defined as "the basic lever of the whole administrative procedure", which must be strictly adhered to in the application of the law, with the purpose of "guaranteeing the correct application of the law" and "protecting the legitimate rights and interests of the parties". See I. Borković, *Upravno pravo*, Zagreb 2002, p. 403; M. Keršić, *Legal Principles in Croatian Legal Science: Fundamental Character and Indeterminacy*, "Pravni vjesnik" 2020, vol. 36(1), p. 72.

[56] European Public Administration Network, *Good Administration in European Countries*, 2023, https://www.eupan.eu/wp-content/uploads/2023/04/Annex-1.-Good-administration-in-European-countries.pdf (access: 29.4.2025), p. 16.

[57] L. Jančová, M. Fernandes, *op. cit.*, p. 15.

[58] As we have shown previously, according to the NIS 2 Directive, public administration entities of central government as defined by a Member State in accordance with national law are considered "essential entities".

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

indicating "the type of information, the format and the procedure of a notification";[59]

- the "delegated" and "implementing" acts procedure: according to Article 24 (2) of the NIS 2 Directive the European Commission is empowered to adopt "delegated acts"[60] to "supplement" this Directive, e.g. to obtain a "certificate" under a European cybersecurity certification scheme; the adoption of these acts implies in advance compliance with the procedures of "an impact assessment" and "consultations".

The power to adopt delegated acts according to Article 24 (2) of the NIS 2 Directive is conferred on the European Commission for 5 years from 16 January 2023. The "delegation of power" may be "revoked" by the European Commission or by the Council via a "decision to revoke". The delegated act shall be notified simultaneously to both the European Parliament and the Council and shall enter into force only if "no objection has been expressed" within a period of 2 months of notification (period which may be extended by 2 months), or if, before the expiry of that period, both the European Parliament and the Council inform the European Commission that they have no objections.

1.3. Administrative and judicial remedies

The judicial review of administrative acts is interpreted in the literature as "a tool of the separation of powers and as an element of the checks and balances".[61]

The EU Charter of Fundamental Rights in Article 47 provides the right to an effective remedy and to a fair trial for everyone whose rights guaranteed by EU law have been violated.[62]

In the particular case of cybersecurity regulations, we notice that Chapter VII of the NIS 2 Directive, titled "Supervision and Enforcement", contains express provisions about the administrative and judicial cybersecurity remedies system. Article 31 (4), (5), (7) and (8) provides, as general regulation, the application of the principles of EU law by public administration entities with supervisory and law

[59] Article 23 (1) and (11) of the NIS 2 Directive.

[60] It is about delegation of power, whereby the administrative authority transfers its decision-making power to another authority. According to doctrine, this measure "must be limited to what is strictly necessary", that is why it has a special legal regime. See J. Waline, G. Eckert, É. Muller, *Droit administratif*, Dalloz 2023, p. 308.

[61] I. Hoffman, *Application of Administrative Law in the Time of Reforms in the Light of the Scope of Judicial Review in Hungary*, "Studia Iuridica Lublinensia" 2020, vol. 29(3), p. 101.

[62] Z. Szente, *Conceptualising the Principle of Effective Legal Protection in Administrative Law*, [in:] *The Principle of Effective Legal Protection in Administrative Law: A European Comparison*, eds. Z. Szente, K. Lachmayer, London 2017, p. 5.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

enforcement duties, included "the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence".

According to the NIS 2 Directive, the administrative and judicial remedy system involves "supervisory and enforcement measures in relation to essential entities".[63] For example, Article 32 (4) provides that Member States have the power at least to: adopt "binding instructions", including the necessary measures to "prevent" or "remedy" an incident and, also, a "time-limits" for the "implementation" of such measures; order the entities concerned "to inform" the natural or legal persons with regard "any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat"; "impose", or "request the imposition" by the "relevant bodies, courts or tribunals", in accordance with national law, of an "administrative fine pursuant" in addition to any of the others measures referred to.

After a "deadline" procedure established by Article 32 (5) of the NIS 2 Directive, where some of the enforcement measures adopted are ineffective, if the requested action is not taken within the time limit set, Member States shall ensure that their authorities are competent, in accordance with national law, to: "temporarily suspend", or request a "certification or authorisation body", or "a court or tribunal"; "request" that the "relevant bodies, courts or tribunals", "temporarily prohibit" any person who is responsible for carrying out managerial responsibilities (expressly provided in this article) from exercising in that entity managerial functions.[64]

Also, Regulation (EU) 2022/2554[65] contains specific rules about administrative and judicial remedies on digital operational resilience of the financial sector. We noticed, e.g., the obligation of a "competent authority", established in Article 54 (5), to publish on their official website the information about a "decision imposing an administrative penalty" against which there is an "appeal before the relevant judicial authorities".

As regards the remedies provided for in Regulation (EU) 2016/679, the CJEU decided that Article 77 (1), Article 78 (1) and Article 79 (1) of this Regulation must be interpreted as permitting the remedies provided for in Article 77 (1) and Article 78 (1), on the one hand, and Article 79 (1) thereof, on the other, "to be exercised concurrently with and independently of each other".[66] The Member States will "lay down detailed rules as regards the relationship between those remedies" in order to ensure "the right to an effective remedy before a court or tribunal".[67]

---

[63] Article 32 of the NIS 2 Directive.

[64] Article 32 (5) (b) of the NIS 2 Directive.

[65] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1011 (OJ L 333/1, 27.12.2022).

[66] Judgment of the Court (First Chamber) of 12 January 2023 in case C-132/21, *Nemzeti Adatvédelmi és Információszabadság Hatóság/Budapesti Elektromos Művek Zrt.*, ECLI:EU:C:2023:2.

[67] *Ibidem*.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

2. Administrative law in the Romanian cybersecurity legal framework

2.1. An overview from the perspective of the Romanian cybersecurity public policy

By implementing the Romania's Recovery and Resilience Plan (RRRP),[68] Pillar 7 (Digital transformation) – Reform 3 (Ensuring cybersecurity for public and private entities which hold critical infrastructure), flagpole 151, Romania undertook establishing the legal and institutional framework for organising and carrying out activities in the field of cybersecurity and cyber defence, the cooperation mechanisms as well as institutional responses in these fields. According to the Annex to the Decision to Implement the Council for the Approval and Assessment of RRRP,[69] Law No. 58/2023 regarding Romania's cybersecurity and cyber defence, as well as the alteration and completion of certain normative acts, was adopted.[70]

Before Law No. 58/2023, the internal legal framework was harmonized with EU regulations; Directive (EU) 2016/1148 was integrally transposed into internal legislation via Law No. 362/2018.[71] At the same time, in force Romania's Cybersecurity Strategy[72] lists a consolidated legal and institutional framework among the goals of strategic importance in the field of cybersecurity.

2.2. The interface between administrative law and the Romanian legal cybersecurity framework

2.2.1. Institutional capacity (responsible public authorities and institutions)

According to Article 3 (c) of Law No. 58/2023, in the field of cybersecurity, this law applies inclusively to the information networks and systems which are held, organised, managed or used by authorities and institutions of the central and local public administration, other than those specified under letter a of this Article (we note that letter a mentions information networks and systems held, organised, managed, used by or under the jurisdiction of public authorities and institutions in the

[68] Romania's Recovery and Resilience Plan (RRRP), approved by the EU Council on 28 October 2021, is available at https://mfe.gov.ro/wp-content/uploads/2022/04/e6d481b413d-b9e7384a946c92e833d45.pdf (access: 29.4.2025).

[69] SWD(2021) 276 final.

[70] Official Journal of Romania no. 214 of 15 March 2023.

[71] Law No. 362/2018 on ensuring common high security for informatic networks and systems (Official Journal of Romania no. 21 of 9 January 2019).

[72] Government Decision No. 1321/2021 on approving Romania's cybersecurity strategy for 2022–2027, as well as the Action Plan for implementing Romania's cybersecurity strategy for 2022–2027 (Official Journal of Romania no. 2 of 3 January 2022).

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

field of defence, public order, national security, justice, emergency situations, the National Registry of Secret State Information Office)[73]; the information networks and systems which are held, organised, managed or used by natural or legal persons which provide public or public interest services, other than those specified under letter b of the same Article; we note that letter b mentions information networks and systems held by private law natural or legal entities and used for the purpose of providing electronic communication services to the public entities of the central and local public administration.

The entities specified in Article 10 of Law No. 58/2023, generically named in the law "competent authorities", which have access to the National Platform for reporting cybersecurity incidents and upon the request of which the entities specified in Article 3 (1) (c) have the obligation to disclose data and information provided by the law, are as follows:

a) the National Directorate for Cybernetic Security, for the civil national cyber space;
b) the Ministry of Research, Innovation and Digitalisation, for drawing up and initiating laws and national public policies in the field of cybersecurity, digital transformation, informational society, communication, research, development and innovation;
c) the National Authority for Administration and Regulation in Communications, for coordinating activities carried out in order to ensure the cybernetic security of own informatics networks and systems, as well as the cybernetic security of the informatics networks and systems owned by private law natural and legal persons and used for the purpose of providing electronic communication services to the authorities and institutions of the central and local public administration;
d) the Ministry of National Defence, the Ministry of Internal Affairs, the Ministry of External Affairs, the Romanian Information Service, the External Information Service, the Special Telecommunication Service, the Protection and Security Service and the Office of the National Register of Secret State Information.[74]

An analysis of these legal provisions leads to the conclusion that this law applies to all authorities and institutions of the central and local public administration which hold, organise, manage and use information networks and systems. The

[73] National Registry of Secret State Information Office is a public institution with legal personality, subordinated to the Romanian Government and directly coordinated by the Prime Minister, with national authority in the field of classified information security. See Article 1 (10) of the Emergency Government Ordinance No. 153/2002 (Official Journal of Romania no. 826 of 15 November 2002), approved by Law No. 101/2003.

[74] Their responsibilities in the matter of cybersecurity are explicitly provided in Articles 11–18 of Law No. 58/2023.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

concept of public authority is consecrated in Title III of the Romanian Constitution, republished, defined as the totality of the structural forms called upon to exercise public power prerogatives, both at the state and the local community level.[75] The Administrative Code[76] defines this phrase in Article 5 (k), according to which public authority is an organ of the state or of the administrative-territorial unit[77] which acts as a public power in order to satisfy a public interest.

With regard to the phrase "natural and legal persons providing public or public interest services" stated in Article 3 (1) (c) of Law No. 58/2023, we believe that the grounds for including these in the law are the consolidation of the public-private partnership in the field of cybersecurity, retained even in Romania's Cybernetic Security Strategy. As stated before,[78] we believe that a necessary consolidation of this partnership must take into account the type of public interest activity which the natural or legal persons carry out, namely for these entities to be public or private entities providing essential services for the support of "critical infrastructure" (as stated in Pillar 7 – Digital transformation – Reform 3, RRRP). In this context, we note that "critical infrastructure" was identified and assigned at the EU level by Council Directive 2008/114/EC,[79] transposed in internal legislation by Emergency Government Ordinance (EGO) No. 98/2010, approved by Law No. 18/2011.[80]

According to Article 3 (c) of EGO No. 98/2010, protecting critical infrastructure involves a cohesive set of processes and activities organised and carried out for the purpose of ensuring the functionality and continuity of services and the integrity of the national and European critical infrastructure, in order to discourage, diminish

[75] V. Vedinaș, *Drept administrativ*, Bucharest 2022, p. 103.

[76] Emergency Government Ordinance No. 57/2019 on the Administrative Code (Official Journal of Romania no. 555 of 5 July 2019). Romania is thus the only country in the European Union that has an administrative code, within the meaning of a normative act that regulates in a unitary way the major institutions of public law. See V. Vedinaș, *La responsabilité financière de la gestion publique en Roumanie*, [in:] *Responsabilité financière des gestionnaires publics. Approches internationales*, ed. S. Damarey, Paris 2023, p. 258.

[77] These territorial units govern themselves through two kinds of directly elected authorities, which are expressly enshrined in the Constitution of Romania: the mayor and the local council. See A. Murphy, F. Ghencea, *The Legal Framework for Local Intergovernmental Coordination in Romania*, "Studia Iuridica Lublinensia" 2023, vol. 32(5), p. 109.

[78] See E.L. Cătană, *Serviciile publice și spațiul cibernetic. Implicații ale Legii nr. 58/2023*, "Pandectele Române / Romanian Pandects" 2023, no. 4, p. 24.

[79] 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 (OJ L 345/75, 23.12.2008), repealed by Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333/164, 27.12.2022).

[80] Emergency Government Ordinance No. 98/2010 on the identification, designation and protection of critical infrastructures (Official Journal of Romania no. 757 of 12 November 2010), approved by Law No. 18/2011 (Official Journal of Romania no. 183 of 16 March 2011).

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

and neutralise a threat, a risk or a weak point. This set comprises several activities, listed non-exhaustively in the EGO, among which is "ensuring the protection of sensitive information specific to the domain" (Article 3 letter c).

Therefore, by corroborating the provisions of Law No. 58/2023 with the RRRP and the provision of EGO No. 98/2010, approved by Law No. 18/2011, which transposes Council Directive 2008/114/EC, we believe one could draw the conclusion that the phrase "natural and legal persons providing public or public interest services" stated in Article 3 (1) (c) of this Law must be interpreted in a limitative manner, by relating it to the type of public interest activity which they carry out; to this end, one takes into account public and private entities which provide essential services for the support of "infrastructure of a critical nature" (as stated in Pillar 7 – Digital Transformation – Reform 3, RRRP), defined at the EU level by the previously mentioned directive.

Under the generic title of "competent authorities" Law No. 58/2023 provides both authorities of the specialised central public administration (responsible for national public services such as digitalisation, defence, internal and external affairs) and specialised structures of the central public administration and autonomous public authorities (the General Directorate for Cybernetic Security,[81] the National Authority for Administration and Regulation in Communications[82]) as well as public institutions, specialised state structures and autonomous administrative authorities (the Romanian Information Service,[83] the External Information Service,[84] the Special Telecommunication Service,[85] the Protection and Security

[81] The National Directorate for Cybernetic Security was founded by E.G.O. No. 104/2021 (Official Journal of Romania no. 918 of 24 September 2021), approved by Law No. 11/2022. It is a specialised structure of the central public administration, within the Government's organisation, coordinated by the Prime Minister. It has a legal personality.

[82] The National Authority for Administration and Regulation in Communications was founded by E.G.O. No. 22/2009 (Official Journal of Romania no. 174 of 19 March 2009), approved by Law No. 113/2010. It is an autonomous public authority, with legal personality, under parliamentary control.

[83] The Romanian Information Service was founded by Law No. 14/1992 (Official Journal of Romania no. 33 of 3 March 1992) as a specialised state structure in the field of information on Romania's national security, an integral part of the national defence system. Its activity is organised and coordinated by the Supreme Council of National Defence.

[84] The External Information Service is organised and operates as an autonomous administrative authority. Its activity is organised and coordinated by the Supreme Council of National Defence. See Law No. 1/1998 on the organisation and operation of the External Information Service (Official Journal of Romania no. 511 of 18 October 2000).

[85] The Special Telecommunications Service is the central specialised structure, with legal personality, which organises, manages, carries out, controls and coordinates activities in the field of special telecommunications for Romania's public authorities and for other users. See Law No. 92/1996 on the organisation and operation of the Special Telecommunications Service (Official Journal of Romania no. 169 of 30 July 1996).

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

Service,[86] the Office of the National Register of Secret State Information[87]). We note that these authorities' competence and responsibilities are established by Law No. 58/2023, Article 19 of which refers to the founding, organisation and subsequent operation, by way of administrative act issued by the heads of these authorities, of other structures specialised in cybersecurity auditing or cybersecurity structures specialised in managing cybernetic threats on the networks and systems in their care.[88] Also Article 3 (2) of Order No. 100/2024 issued by the National Directorate for Cybernetic Security (NDCS)[89] established that, in order to carry out their responsibilities, the authorities have access to the National Platform for Reporting Cybernetic Security. Incidents treat all the data received as being confidential and grant access to data only to specially assigned personnel. We draw the conclusion that these provisions are given with the purpose of respecting the fundamental rights and principles recognised especially by the EU Charter of Fundamental Rights, as well as by the GDPR.

2.2.2. The administrative decision-making regulations – categories of administrative acts

Article 48 of Law No. 58/2023 provides two categories of administrative acts which are issued in the contraventional procedure established by this law, with various issuing parties, depending on the type of offence noted and applied.

The first category – with regard to offences detailed by Article 48 (1) (a) and (b) of Law No. 58/2023 – is the administrative act of identifying an infringement and applying a sanction, issued by the control staff of the NDCS and applied through the "decision" of the head of NDCS.

The second category – with regard to the offences detailed in Article 48 (1) (c) of Law No. 58/2023 – is the administrative act of identifying an infringement and applying a sanction, issued by the specifically assigned control staff within the

[86] The Protection and Security Service is a state structure with responsibilities in the field of national security, specialised in ensuring protection for Romanian high officials, foreign high officials and their families during their stay in Romania, within the confines of legal jurisdiction, as well as in guarding their registered offices and residences, as per the decision of the Supreme Council of National Defence. See Article 1 of Law No. 191/1998 on the organisation and operation of the Protection and Security Service (Official Journal of Romania no. 402 of 22 October 1998).

[87] The Office of the National Register of Secret State Information is a public institution with legal personality, subordinated to the Government. See Government Decision no. 404/2004 on the organisation and operation of the Government's structures (Official Journal of Romania no. 267 of 26 March 2004).

[88] See E.L. Cătană, *Serviciile publice…*, pp. 26–27.

[89] Order No. 100/2024 of the National Directorate for Cybernetic Security on the approval of confidentiality and transparency policies of the National Platform for Reporting Cybersecurity Incidents (Official Journal of Romania no. 120 of 12 February 2024).

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

authorities named in the law "competent authorities" (according to Article 10) and applied by the control staff especially assigned by the head of these authorities.

By waiver from the provisions of the Romanian common law contraventional procedure,[90] these administrative acts are communicated to the offender within 15 days from the date of issue. At the same time as the administrative act of applying a sanction, the offender is also notified of any fine, mentioning the obligation to pay it within 30 days from the date the act was communicated (Article 49 (5) and (6)). Enforcing the contraventional sanctions applied is barred by limitation if the administrative act was not communicated to the offender within 15 days from the date the sanction was applied (Article 49 (10)).

2.2.3. Administrative and judicial remedies rules

Administrative acts and decisions adopted as per the provisions of Law No. 58/2023 can be brought before an administrative court at the Bucharest Court of Appeal, without going through the preliminary procedure (administrative appeal), within 30 days from the date they were communicated.

We can therefore note that we are in the presence of an exception from the rule of contravention complaint which, according to Romanian common law contraventional procedure, is filed and solved, on the grounds of special material jurisdiction and alternative territorial jurisdiction, at the court under the jurisdiction of which the contravention was committed, or the court in the geographic area of which the offender resides.

Also we are in the presence of an exception from the rule of material jurisdiction established by the Law of Administrative Contentious No. 554/2004, which states in Article 10 (1) that the courts competent to solve administrative contentious cases are administrative-fiscal courts, and for appeals, the administrative contentious and fiscal departments of courts of appeal.

Moreover, we are in the presence of an exception from the rule of territorial jurisdiction of administrative contentious courts, taking into account that Article 10 (3) of Law No. 554/2004 provides exclusive territorial jurisdiction, according to the criterion of the nature of the parties involved, as follows: the claimant who is a natural or legal person exclusively addresses the court of their domicile or registered office;[91] the claimant who is a public authority, public institution or assimilated to the former, exclusively addresses the court of the offender's domicile or registered office.

[90] In Romanian law, the common law contravention procedure is regulated by Government Ordinance No. 2/2001 on the legal nature of contraventions (Official Journal of Romania no. 410 of 25 July 2001).

[91] In the jurisprudence of Romanian contentious courts, see decision no. 1005 of the High Court of Cassation and Justice, Administrative and Fiscal Contentious Department of 18 February 2021.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

On the other hand, we are in the presence of an exception from the rule of preliminary administrative procedure (the administrative appeal[92]) regulated by Article 7 of Law No. 554/2004.

Law No. 58/2023 provides the deadline for initiating judicial review against the administrative acts is 30 days from the date of their communication, thus waiving the provisions of Article 11 of Law No. 554/2004, which state that the judicial review is filed within 6 months, which flows differently and which is a limitation period, but no longer than one year, which also flows differently and is a deterioration period.[93]

Administrative acts regulated by Law No. 58/2023, as well as the definitive court decision by which the appeal was solved in the administrative contentious, are enforceable titles, with no other formality. The administrative contentious appeal suspends enforcement only with regard to paying the fine, until the court issues a definitive decision.

The sums derived from fines applied in accordance with the provisions of Law No. 58/2023 flow integrally into the state budget, and enforcement is carried out in accordance with the legal provisions regarding foreclosure of fiscal debt. In order to enforce a sanction, the competent authorities automatically notify to specialised structures of the National Fiscal Administration Agency, the administrative act not appealed within the lawful deadline, after the period stated on the demand for payment has expired, or after the court decision which solved the administrative appeal has remained definitive.

DISCUSSION AND CONCLUSIONS

In international law, the conclusions of the study highlight the rules established by the UN Charter, the UN Global Counter-Terrorism Strategy, and WTO agreements. The maintenance of "international peace and security" is listed as the first purpose of the UN Guide to Developing a National Cybersecurity Strategy to promote capacity-building for law enforcement. Also a literature overview highlights that the pandemic has caused increased demand for virtual service delivery and public sector operations, a new impetus of government digitalization, a multitude of crises including security ones, which require international cooperation. We

[92] In administrative law, there are two major ways of contesting allegedly unlawful decisions/acts: the administrative appeal and the judicial review (court action). See D.C. Dragoș, *Administrative Appeal*, [in:] *Global Encyclopedia of Public Administration, Public Policy and Governance*, ed. A. Farazmand, Cham 2016, p. 1.

[93] See E.L. Cătană, *Drept administrativ*, București 2023, pp. 368–373.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

conclude that this approach of the study, from the perspective of international law is meant to better understand, comply with and enforce this issue.

In the context of international law and multiple cybersecurity challenges, we mentioned the necessity for multidisciplinary research on the complex and ever-expanding cybersecurity law, from the perspective of its interference with other branches of law. The research hypotheses took into account that further research was needed on the many interfaces between administrative law and cybersecurity rules. Research was focused in particular on the interface between administrative law and cybersecurity rules, in the EU and in Romania as a Member State. Taking into account the research hypotheses presented in the introductory part, the interface between administrative law and cybersecurity rules was analysed methodologically under three dimensions, at the EU and Romanian level: the regulation of the institutional capacity for cybersecurity (responsible public authorities and institutions), the regulation of administrative decision-making procedure, as well as administrative and judicial remedies.

In EU law, taking into account the research hypotheses, the conclusion is that NIS 2 Directive establishes: public administration entities of central government of the Member State as "essential entities", a set of administrative decision-making regulations (the "notification" procedure; "delegated" and "implementing" acts procedure), as well as administrative and judicial remedies (e.g. binding instructions or orders, as well as "any possible protective or remedial measures" which can be taken in response to the threat; "administrative fine pursuant"; a "deadline" procedure when some enforcement measures adopted are ineffective; the power to "temporarily suspend", or "request a certification or authorisation body", or "a court or tribunal", in accordance with national law; to "temporarily suspend a certification or authorisation). Also ENISA developed guiding documents, e.g. in public procurement. The research results show that there are rules of administrative law in particular cases of cybersecurity regulation, such as administrative and judicial remedies established by Regulation (EU) 2022/2554 and the remedies provided for in Regulation (EU) 2016/679, whose interpretation and application was decided by the CJEU.

In Romania, it can be noticed that the adoption of the National Cybersecurity Strategy respects the Guide issued at the European level, which promotes "capacity-building for law enforcement" as a focus of the national strategy. The internal legal framework has been harmonized with EU law. We have analytically researched this matter of "harmonisation" of the Romanian cybersecurity law with EU law from the perspective of administrative law. The Law No. 58/2023 establishes the organization and development of activities in the fields of cybersecurity and cyber defence, mechanisms of cooperation and responsibilities of public authorities and bodies. Research results lead to the conclusion that, by Law No. 58/2023, Romania has created "competent authorities" in this field, thus meeting the need to trans-

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

pose international and EU norms into internal law regarding institutional capacity (responsible public authorities and institutions). Also, there are two categories of administrative acts in the administrative decision-making procedure established by this law (the administrative act of identifying an infringement and applying a sanction, issued by the control staff of the NDCS and applied through the "decision" of the head of NDCS; the administrative act of identifying an infringement and applying a sanction, issued by the specifically assigned control staff within the authorities named in the law "competent authorities" and applied by the control staff especially assigned by the head of these authorities), which can be appealed in administrative contentious, in accordance with a special judicial competence and procedure.

Our research results lead to the conclusion that the legal provisions which establish litigation regarding administrative acts issued according to Law No. 58/2023 as being under the jurisdiction of the administrative contentious court confirm the special legal status which Romanian lawmakers decided to establish in the case of remedy rules established by this Law. These legal provisions, depart from the provisions of Law of Administrative Contentious No. 554/2004, as they establish the exclusive jurisdiction of the Bucharest Court of Appeal, exclude preliminary administrative procedure (administrative appeal) and give a special deadline for judicial review in administrative contentious. Last but not least, our research results lead to the conclusion that the provisions of Order No. 100/2024 issued by the NDCS – which establishes that, in order to fulfil their duties, authorities which have access to the National Platform for Reporting Cyber Security Incidents treat all data received as confidential and grant access to data only to specially assigned personnel – are given for the purpose of respecting the fundamental rights and principles.

We finally conclude that, through the results of the research of this study, we make a contribution primarily to the development of the science of administrative law, its modernization in the era of digital development being a certainty, on the background of the growing role of international bodies and the State, the diversification of institutions, administrative decision-making procedure as well as administrative and judicial remedies. Secondly, we believe that the results of this research lead to the development of cybersecurity law, which, as we have demonstrated, has a significant area of administrative law rules. Thirdly, the results of the research conclude the impact of international, EU and Member States law (as we have already submitted, Romania as a particular subject of analysis is intended to conduct research into the details of the topic, as reflected in an EU Member State), which promote global cooperation on the background of cybersecurity challenges.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

REFERENCES

Literature

Borković I., *Upravno pravo*, Zagreb 2002.

Cătană E.L., *Drept administrativ*, București 2023.

Cătană E.L., *Serviciile publice și spațiul cibernetic. Implicații ale Legii nr. 58/2023*, "Pandectele Române / Romanian Pandects" 2023, no. 4.

Cheng M.H., Kuen H.C., *Towards a Digital Government: Reflections on Automated Decision-Making and the Principles of Administrative Justice*, "Singapore Academy of Law Journal" 2019, vol. 31(2).

Coco A., Souza Dias T. de, *'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law*, "The European Journal of International Law" 2021, vol. 32(3), **DOI: https://doi.org/10.1093/ejil/chab056**.

Coglianese C., *Administrative Law in the Automated State*, "Daedalus" 2021, vol. 150(3), **DOI: https://doi.org/10.1162/daed_a_01862**.

Daly P., Raso J., Tomlinson J., *Researching Administrative Law in the Digital World*, [in:] *A Research Agenda for Administrative Law*, ed. C. Harlow, Aldershot 2023, **DOI: https://dx.doi.org/10.2139/ssrn.4008531**.

Dragoș D.C., *Administrative Appeal*, [in:] *Global Encyclopedia of Public Administration, Public Policy and Governance*, ed. A. Farazmand, Cham 2016, **DOI: https://doi.org/10.1007/978-3-319-31816-5_1033-1**.

Emery T.J., Mélon L., Spruk R., *E-Procurement and Institutional Quality: Friends or Foes? Evidence from Catalonia*, [in:] *Sustainability in Public Procurement, Corporate Law and Higher Education*, ed. L. Melon, London 2023, **DOI: https://doi.org/10.4324/9781003252153-8**.

Erskine T., Carr M., *Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace*, [in:] *International Cyber Norms: Legal, Policy & Industry Perspectives*, eds. A.-M. Osula, H. Rõigas, Tallinn 2016.

European Union Agency for Cybersecurity, Kyranoudi P., Liveri D., Drougkas A., Zisi A., *Procurement Guidelines for Cybersecurity in Hospitals – Good Practices for the Security of Healthcare Services*, European Network and Information Security Agency, 2020, **DOI: https://data.europa.eu/doi/10.2824/943961**.

Finnemore M., Hollis D.B., *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, "The European Journal of International Law" 2020, vol. 31(3), **DOI: https://doi.org/10.1093/ejil/chaa056**.

Finnemore M., Hollis D.B., *Constructing Norms for Global Cybersecurity*, "American Journal of International Law" 2016, vol. 110.

Franchini D., *Extraterritorial Sanctions in Response to Global Security Challenges: Countermeasures as Gap-Fillers in the United Nations Collective Security System*, "Cambridge International Law Journal" 2023, vol. 12(1), **DOI: https://doi.org/10.4337/cilj.2023.01.08**.

Grandia J., Volker L., *Ways Forward in Public Procurement*, [in:] *Public Procurement Theory, Practices and Tools*, eds. J. Grandia, L. Volker, Cham 2023, **DOI: https://doi.org/10.1007/978-3-031-18490-1_8**.

Hoffman I., *Application of Administrative Law in the Time of Reforms in the Light of the Scope of Judicial Review in Hungary*, "Studia Iuridica Lublinensia" 2020, vol. 29(3), **DOI: https://dx.doi.org/10.17951/sil.2020.29.3.101-116**.

Hoofnagle C.J., Sloot B. van der, Borgesius F.Z., *The European Union General Data Protection Regulation: What It Is and What It Means*, "Information & Communications Technology Law" 2019, vol. 28(1), **DOI: https://doi.org/10.1080/13600834.2019.1573501**.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

International Telecommunication Union, *Strategic Engagement in Cybersecurity: Guide to Developing a National Cybersecurity Strategy*, Geneva 2021.

Jančová L., Fernandes M., *Digitalisation and Administrative Law: European Added Value Assessment*, Brussels 2022, **DOI: https://doi.org/10.2861/643042**.

Keršić M., *Legal Principles in Croatian Legal Science: Fundamental Character and Indeterminacy*, "Pravni vjesnik" 2020, vol. 36(1), **DOI: https://doi.org/10.25234/pv/8273**.

Lemnitzer J.M., *Back to the Roots: The Laws of Neutrality and the Future of Due Diligence in Cyberspace*, "The European Journal of International Law" 2022, vol. 33(3), **DOI: https://doi.org/10.1093/ejil/chac053**.

Murphy A., Ghencea F., *The Legal Framework for Local Intergovernmental Coordination in Romania*, "Studia Iuridica Lublinensia" 2023, vol. 32(5), **DOI: https://dx.doi.org/10.17951/sil.2023.32.5.105-115**.

Oddenino A., *Digital Standardization, Cybersecurity Issues and International Trade Law*, "Questions of International Law" 2018, vol. 51.

Peng S., *Cybersecurity Threats and the WTO National Security Exceptions*, "Journal of International Economic Law" 2015, vol. 18(2), **DOI: https://doi.org/10.1093/jiel/jgv025**.

Peng S., *The Uneasy Interplay between Digital Inequality and International Economic Law*, "The European Journal of International Law" 2022, vol. 33(1), **DOI: https://doi.org/10.1093/ejil/chac019**.

Ranchordás S., *Empathy in the Digital Administrative State*, "Duke Law Journal" 2022, vol. 71(6/4).

Sannerholm R., *Legal, Judicial and Administrative Reforms in Post-Conflict Societies: Beyond the Rule of Law Template*, "Journal of Conflict & Security Law" 2007, vol. 12(1), **DOI: https://doi.org/10.1093/jcsl/krm004**.

Szente Z., *Conceptualising the Principle of Effective Legal Protection in Administrative Law*, [in:] *The Principle of Effective Legal Protection in Administrative Law: A European Comparison*, eds. Z. Szente, K. Lachmayer, London 2017.

Tsagouria N., Farrell M., *Cyber Attribution: Technical and Legal Approaches and Challenges*, "The European Journal of International Law" 2020, vol. 31(3), **DOI: https://doi.org/10.1093/ejil/chaa057**.

Vedinaș V., *Drept administrativ*, Bucharest 2022.

Vedinaș V., *La responsabilité financière de la gestion publique en Roumanie*, [in:] *Responsabilité financière des gestionnaires publics. Approches internationales*, ed. S. Damarey, Paris 2023.

Waline J., Eckert G., Muller É., *Droit administratif*, Dalloz 2023.

Online sources

European Parliament, Procedure file 2021/2161(INL), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/2161(INL)&l=en (access: 29.4.2025).

European Public Administration Network, *Good Administration in European Countries*, 2023, https://www.eupan.eu/wp-content/uploads/2023/04/Annex-1.-Good-administration-in-European-countries.pdf (access: 29.4.2025).

Romania's Recovery and Resilience Plan (RRRP), approved by the EU Council on 28 October 2021, https://mfe.gov.ro/wp-content/uploads/2022/04/e6d481b413db9e7384a946c92e833d45.pdf (access: 29.4.2025).

Documents, reports

Green Paper from the European Commission of 18 October 2010 on expanding the use of e-Procurement in the EU, COM(2010) 571 final.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

United Nations, *Committee of Experts on Public Administration: Report on the Twenty-First Session (4–8 April 2022)*, New York 2022.
United Nations, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 22.7.2015, A/70/174.
United Nations, *The Sustainable Development Goals Report 2022*, New York 2022.

Legal acts

Charter of Fundamental Rights of the European Union (OJ C 326/391, 26.10.2012).
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 (OJ L 345/75, 23.12.2008).
Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94/65, 28.3.2014).
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194/1, 19.7.2016).
Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333/80, 27.12.2022).
Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333/164, 27.12.2022).
Emergency Government Ordinance No. 153/2002 (Official Journal of Romania no. 826 of 15 November 2002).
Emergency Government Ordinance No. 22/2009 (Official Journal of Romania no. 174 of 19 March 2009).
Emergency Government Ordinance No. 98/2010 on the identification, designation and protection of critical infrastructures (Official Journal of Romania no. 757 of 12 November 2010).
Emergency Government Ordinance No. 57/2019 on the Administrative Code (Official Journal of Romania no. 555 of 5 July 2019).
Emergency Government Ordinance No. 104/2021 (Official Journal of Romania no. 918 of 24 September 2021).
European Parliament resolution of 20 May 2021 on shaping the digital future of Europe: removing barriers to the functioning of the digital single market and improving the use of AI for European consumers (2020/2216(INI)) (OJ C 15/204, 12.1.2022).
Government Decision No. 404/2004 on the organisation and operation of the Government's structures (Official Journal of Romania no. 267 of 26 March 2004).
Government Decision No. 1321/2021 on approving Romania's cybersecurity strategy for 2022–2027, as well as the Action Plan for implementing Romania's cybersecurity strategy for 2022–2027 (Official Journal of Romania no. 2 of 3 January 2022).
Government Ordinance No. 2/2001 on the legal nature of contraventions (Official Journal of Romania no. 410 of 25 July 2001).
Law No. 92/1996 on the organisation and operation of the Special Telecommunications Service (Official Journal of Romania no. 169 of 30 July 1996).
Law No. 191/1998 on the organisation and operation of the Protection and Security Service (Official Journal of Romania no. 402 of 22 October 1998).
Law No. 1/1998 on the organisation and operation of the External Information Service (Official Journal of Romania no. 511 of 18 October 2000).

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

Law No. 18/2011 (Official Journal of Romania no. 183 of 16 March 2011).
Law No. 362/2018 on ensuring common high security for informatic networks and systems (Official Journal of Romania no. 21 of 9 January 2019).
Law No. 58/2023 on Romania's cyber security and defense, and for amending and completing some normative acts (Official Journal of Romania no. 214 of 15 March 2023).
Order No. 100/2024 of the National Directorate for Cybernetic Security on the approval of confidentiality and transparency policies of the National Platform for Reporting Cybersecurity Incidents (Official Journal of Romania no. 120 of 12 February 2024).
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119/1, 4.5.2016).
Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act) (OJ L 151/15, 7.6.2019).
Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1011 (OJ L 333/1, 27.12.2022).
Resolution adopted by the General Assembly on 8 September 2006: The United Nations Global Counter-Terrorism Strategy, A/RES/60/288.
Resolution adopted by the General Assembly on 22 June 2023: The United Nations Global Counter-Terrorism Strategy, A/RES/77/298.
Treaty on the Functioning of the European Union, consolidated version (OJ C 326/47, 26.10.2012).

Case law

Decision no. 1005 of the High Court of Cassation and Justice, Administrative and Fiscal Contentious Department of 18 February 2021.
Judgment of the Court (First Chamber) of 12 January 2023 in case C-132/21, *Nemzeti Adatvédelmi és Információszabadság Hatóság/Budapesti Elektromos Művek Zrt.*, ECLI:EU:C:2023:2.

ABSTRAKT

Z uwagi na niedostatek badań z perspektywy prawa administracyjnego dotyczących obecnych regulacji w zakresie cyberbezpieczeństwa ogólnym celem artykułu jest podejście administracyjnoprawne do przepisów dotyczących cyberbezpieczeństwa, ze szczególnym uwzględnieniem przypadku rumuńskiego w kontekście prawa Unii Europejskiej i prawa międzynarodowego. Hipotezy badawcze dotyczące styku prawa administracyjnego i zasad cyberbezpieczeństwa obejmują trzy wymiary. Są to: regulacja zdolności instytucjonalnej w zakresie cyberbezpieczeństwa, regulacja procesów decyzyjnych oraz odpowiednio administracyjne i sądowe środki prawne. Zastosowano metody analityczne i porównawcze z uwzględnieniem orzecznictwa. Co do prawa międzynarodowego, we wnioskach z badań podkreślono zasady ustanowione w drodze umów międzynarodowych. W prawie unijnym dyrektywa NIS 2 określa podmioty rządowej administracji publicznej państwa członkowskiego jako „podmioty kluczowe", zbiór administracyjnych przepisów decyzyjnych oraz odpowiednio administracyjnych i sądowych środków odwoławczych. Krajowe ustawodawstwo rumuńskie zostało zharmonizowane

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 25/11/2026 11:31:38

z prawem unijnym. Ustawa nr 58/2023 wprowadza obowiązki władz i organów publicznych, które są „właściwymi organami" w tej dziedzinie. W ustanowionej tą ustawą administracyjnej procedurze decyzyjnej występują dwie kategorie aktów administracyjnych, od których można się odwołać w administracyjnym postępowaniu spornym.

Słowa kluczowe: cyberbezpieczeństwo; prawo administracyjne; zdolność instytucjonalna; procedura decyzyjna; administracyjne i sądowe środki odwoławcze

UMCS

Ministerstwo Nauki i Szkolnictwa Wyższego
Doskonała Nauka II

Projekt dofinansowany ze środków budżetu państwa, przyznanych przez Ministra Edukacji i Nauki w ramach Programu „Doskonała Nauka II"