

Vulnerabilities of New Technologies in the Work of Public Authorities and the Need for Cybersecurity

Elena Emilia Ștefan

Associate Professor, PhD, „Nicolae Titulescu” University, Bucharest, Romania
stefanelena@univnt.ro

ABSTRACT: Society as a whole is receptive to the new technologies because they make life easier. It is therefore the responsibility of decision-makers in public administration to identify people's social needs so that these can be met as safely as possible under the umbrella of a strong legal framework. The change in how public administration interacts with citizens, in light of the implementation of new technologies, also comes with challenges in terms of strong legislation and the ethics of administrative decisions. The scope of the paper is to present, in a personal manner, the legislative framework applicable to digitalization in public administration from the perspective of the vulnerabilities of new technologies that may call into question the need for cybersecurity. In terms of research methodology, the paper is structured as follows: Part I explores the legislation applicable to digitalization and cybersecurity from both European and national perspectives; Part II discusses two existing online platforms at the level of public authorities; and Part III, through a case study, highlights the vulnerabilities of new technologies in the work of public authorities and the need for cybersecurity. The conclusion emphasizes that, while digitalization contributes to a better quality of life, authorities still need to invest heavily in innovation to identify the best solutions for secure online platforms.

KEYWORDS: digitalization, public authorities, cyber security, SEAP, Romania

1. Introduction

In recent years, the trend in society has been to communicate remotely, to pay online, and to order various items necessary for daily life on various platforms and this has also extended to the relationship with public authorities. Since in order to make a payment, such as a property tax or a fine, the person has to go through several authentication steps, which involve filling in various fields with personal data, including the person's name, address, bank details etc., this operation must be carried out in complete security. In this context, data security is becoming increasingly important for both citizens and authorities.

Digitalization must be carried out within a solid regulatory framework that benefits from dedicated infrastructure and well-trained personnel with the digital skills required to implement and operate with the new technologies. In this regard, experts considered that "the impact of digitalization on the work of public administration (...) requires an in-depth analysis, as the general interest mission of public administration requires that the activity of public institutions and authorities be carried out electronically and in complete security (...)" (Cătană, 2022, p.115). In this background, the paper presents in a personal way the issue of digitalization in public administration, combining the theoretical component of the subject with a case study that highlighted the need for cybersecurity.

2. Brief considerations on the legislation applicable to digitalization

2.1. At the European level

The regulatory framework for digitalization is particularly complex and "the legal norm requires acceptance of and compliance with prescribed conduct" (Hegheș, 2022, p.153). The European Union has gone through several chronological stages in its approach to digitalization. It is worth noting in this respect the *First Digital Agenda for Europe 2010* [(COM 2010) 245 final]. The overall aim of the agenda is: "a vibrant digital single market; interoperability and standards; trust and security; fast and ultrafast internet access; research and innovation; enhancing digital literacy, skills and inclusion, developing social competences and inclusion (...)." Then come the *Second Digital Agenda 2020* [COM 2020) 67 final], the vision of which was the following: "The Commission wants a European society powered by digital solutions (...) that enrich the lives of all of us (...)."

Another important act is Regulation (EU) 2019/881 on cybersecurity (OJ L151, 7.6.2019). In common language, the legislation is known as the EU Cybersecurity Act. "Increased digitization and connectivity increase cybersecurity risks, thus making society as a whole more vulnerable to cyber threats (...)" [para. 3, Preamble]. The aim of Regulation 2019/881 is "to ensure the proper functioning of the internal market while aiming to achieve a high level of cybersecurity (...)." According to the documents, cybersecurity means "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats" [art. 1 item 1)].

2.2. At the national level

The first act we consider is the National Strategy in the field of artificial intelligence 2024-2027 (Government Resolution no. 832/2024). Furthermore, the doctrine has pointed out that "the protection of fundamental human rights is a direction that more and more countries are pursuing when allowing the development and use of AI technologies on their territory" (Stoica, 2025, p.35).

The aim of the strategy is to “contribute to Romania’s strategy on the adoption of digital technologies in the economy and society under conditions of respect for human rights and promotion of excellence and trust in AI.” Moreover, the strategy ensures an alignment of Romania’s endeavors with the strategic directions at the European level on common rules for digital services (Idem, Appendix no. 1).

The next act is *Law no. 58/2023 on Romania's cybersecurity and cyber defence* (2023), which establishes “the legal and institutional framework for the organization and conduct of activities in the areas of cybersecurity and cyber defence, cooperation mechanisms and the responsibilities of the institutions with powers in these areas” [art.1 para. (1)]. According to the law, “cybersecurity and cyber defence are achieved through the adoption and implementation of policies and measures to understand, prevent and address vulnerabilities, risks and threats in cyberspace” [art. 1 para. (2)]. In Romania, “in order to organize and carry out in a unified manner, at national level, the specific cybersecurity activities, the National Cybersecurity System - NSCS is established, with the role to coordinate the actions at national level to ensure cybersecurity” [art.6 para. (1)]. An important public authority in the digitalization process is the *Authority for the Digitalization of Romania - ADR* (Government Ordinance no. 89/2020) the role of which is to design strategies and public policies in the field of digital transformation and information society (...) [art.1 para. (1)].

3. Online platforms for public authorities

In this section, a documentary analysis has been carried out on several platforms providing digital public services managed by the Digitization Authority (ADR), given that “public services are undoubtedly a pillar of society” (Cliza, 2023, p. 49).

3.1. SEAP (Electronic Public Procurement System)

The Authority for the Digitalization of Romania provides technical support for the awarding of public procurement contracts by contracting authorities through an electronic procedure. The Electronic Public Procurement System is “a computerized system of public utility, accessible via the Internet at a dedicated address, used for the purpose of electronic application in the award procedures and for the publication of the contract notice at the national level” (Law No. 98/2016 on Public Procurement, art. 3, para. 1, letter nn). Specifically, through SEAP and its dedicated website, public procurement is carried out by electronic means. According to the law, “The contracting authority shall ensure by electronic means, through SEAP, direct, complete, unrestricted and free of charge access of economic operators to the procurement documents as of the date of publication of the contract notice” (art. 150). Furthermore, “Contracting authorities shall publish in the dedicated section of SEAP all amendments to public procurement contracts/ framework agreements, so that the duration and final price on

completion or termination of the contract/ framework agreement are indicated” (art. 222).

3.2. *Ghișeul.ro*

Payment obligations to the state budget can be fulfilled through the virtual payment counter called the National Electronic Online Payment System (SNEP), which is part of the National Electronic System (SEN) [art.1 para. (1), Government Resolution no. 1235/2010 approving the implementation of the national electronic system for online payment of taxes and duties].

According to the normative act, *ghișeul.ro* is the internet address where the National Electronic Online Payment System is available. The Authority for the Digitalization of Romania develops, implements, manages, and operates the National Electronic Online Payment System. SNEP is an electronic communication platform open to credit institutions and to the provision of services for accepting electronic payments or other means of payment established by law (art. 8). The legislation was amended in 2020 to allow the use of bank cards for online payments of taxes (Government Resolution no. 285/2020).

4. Vulnerabilities of new technologies in the work of public authorities and the need for cybersecurity

Specifically, in February 2025, due to problems with the electricity grid, networking equipment was affected, which caused the unavailability of several platforms managed by the Authority for the Digitalization of Romania (ADR), such as the tax payment platform *ghișeul.ro*, the Electronic Public Procurement System (SEAP), ROeID, and RO-Guvernare. According to public information, the restoration of these platforms followed two main lines of action: "restoration of the storage device affected by the power fluctuation; temporary restoration of the virtual machines related to the internal A.D.R. systems serving the SEAP system services" (Vasilache, 2025). These technical issues have prompted the authorities to accelerate the idea of migrating to the governmental cloud. As a result, on March 7, 2025, ADR published a notice in SEAP regarding the procurement of services for the migration of certain applications to the Governmental Private Cloud of Romania: I. Services for application migration to Governmental Private Cloud of Romania; II. Cybersecurity assessment services (*E-licitatie.ro* n.d.) Previously, there have been cases where city hall websites were hacked, compromising thousands of personal data, leading to a public perception of a clear state of danger. For example, according to public information of November 2024, the City Hall of District 5 of Bucharest was the target of such an attack. Hackers who broke into the servers of the City Hall of District 5 put up for sale the personal data of over 200,000 citizens, including their personal ID numbers and photographs (Fanatik.ro, 2024).

5. Conclusions

At the EU level the regulatory framework for digitalization is particularly strong and includes several regulations. Among them, we consider particularly important the Regulation on Cybersecurity. From this perspective, Romania has adopted Law No. 58/2023 on Romania's cybersecurity and cyber defence, which sets out in detail the issues analyzed.

At the same time, based on the documentation carried out, the paper also focused on two governmental platforms managed by the Authority for the Digitalization of Romania (ADR), namely SEAP and *Ghișeul.ro*, which were briefly presented to establish a link with the case study that involved them, from the perspective of the vulnerabilities of new technologies.

According to the research, a lack of power supply can cause digitized platforms to malfunction and result in the loss of users' data. In this light, "digitalization brings with it new issues of responsibility, legal liability, limits and respect for citizens' rights and freedoms" (Ștefan, 2024, p. 565).

In conclusion, although legislation exists, we believe that in practice, digitalization is taking a more difficult course due to the many challenges that can arise, such as: the lack of public access to online services, the lack of adequate infrastructure, and the risk of malicious actors hacking government websites and collecting data, which can then be sold on the black market.

References

- Cătană, E. L. (2022). Impactul digitalizării activității administrației publice asupra actului administrativ. Aspecte normative, jurisprudențiale și din perspectiva codificării procedurii administrative [The impact of the digitalisation of public administration on the administrative act. Normative, jurisprudential and legal aspects from the perspective of administrative procedure codification]. In *RDP* no. 3/2022:115.
- Cliza, M.C. (2023). Public services at the service of citizens - case study: cleaning services. *International Journal of Legal and Social Order* (1): 49, <https://doi.org/10.55516/ijlso.v3i1.130>
- Communication from the Commission to The European Parliament. The Council, The European Economic and Social Committee and The Committee of the Regions. A Digital Agenda for the Europe (COM 2010) 245 final, Brussels, 19.5.2010).
- Communication from The Commission to The European Parliament. The Council, The European Economic and Social Committee and The Committee of the Regions. Shaping Europe's Digital future (COM/2020/67/final, Brussels, 19.2.2020).
- Fanatik.ro. (2024). News: The hackers who broke into the Sector 5 City Hall servers put the personal data of over 200,000 citizens up for sale. <https://www.fanatik.ro/hackerii-care-au-spart-serverele-primariei-sectorului-5-au-scos-la-vanzare-datele-personale-a-pest-200-000-de-cetateni-sunt-pe-piata-inclusiv-cnp-urile-si-pozele-acestora-20891448>
- Government Resolution no. 1235/2010 approving the implementation of the national electronic system for online payment of taxes and duties. *Official Journal* no. 838 of 14 December 2010.
- Government Resolution no. 285/2020 for the amendment and supplementation of Government Resolution no. 1235/2010 approving the implementation of the national electronic system for online payment of taxes and duties. *Official Journal* no. 305 of 10 April 2020.

- Government Resolution no. 89/2020 on the organization and operation of the Authority for the Digitalization of Romania. *Official Journal* no. 113 of 13 February 2020.
- Government Resolution no. 832/2024 approving the National Strategy in the field of artificial intelligence 2024-2027. *Official Journal* no. 730 of 25 July 2024.
- Hegheș, N.-E. (2022). The non - retroactivity of new legal norms-fundamental principle of law. Exceptions. *International Journal of Legal and Social Order* (1):153-160. <https://ijlso.ccdsara.ro/index.php/international-journal-of-legal-a/article/view/74/60>
- Law no. 58/2023 on Romania's cyber security and cyber defence. *Official Journal* no. 214 of 15 March 2023.
- Law no. 98/2016 on public procurement. *Official Journal* no. 390 of 23 May 2006.
- Regulation (UE) 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 (...) (JO L151/15, 7.6.2019).
- SEAP (Electronic Public Procurement System). (n.d.). Notices. *E-licitatie.ro*. <https://www.e-licitatie.ro/pub/notices/c-notice/v2/view/100190660>
- Ștefan, E.E. (2024). Integrity and Transparency in the Work of Public Authorities. Aspects of Comparative Public Law. *Juridical Tribune – Review of Comparative and International Law* (14) no 4 (December 2024):565. DOI: 10.62768/TBJ/2024/14/4/03.
- Stoica, A. (2025). Inteligența artificială și drepturile și libertățile fundamentale constituționale [Artificial intelligence and fundamental constitutional rights and freedoms]. *Buletin de Informare Legislativă* no.1/35. http://www.clr.ro/download/buletine/buletin_informare_legislativa_2025/Buletin-nr.-1-2025.pdf
- Vasilache, A. (2025). Online payment of taxes through Ghișeul.ro. Public information. *Hotnews.ro*. <https://hotnews.ro/plata-online-a-taxelor-prin-ghiseul-ro-si-platforma-de-achizitii-publice-nu-vor-functiona-pana-saptamana-viitoare-1901040>