Determining The Nature of Digital Communication in Public Law Sphere

Artem Zubko¹, Maksym Sokiran², Anna Danylenko³, Diana Levchenko⁴ and Vitaliy Oksin⁵

Abstract

The aim of the article is to disclose the content of a new view on the essence of digital communication, caused by changes in various aspects of social development and the need to draft effective management practices for digital technologies, digital communication, and artificial intelligence. Providing such an opportunity combines a complex and interdisciplinary approach, which represents a combination of methods and means of various scientific disciplines. The authors substantiate the thesis that the mandatory nature of the implementation of certain rules and norms arising from public law relations by State agencies and citizens creates special conditions for conflict in the context of digital communication. This is explained by the fact that the interests of the State and private individuals do not always coincide, especially regarding access to information, transparency of management processes and interaction with the public through digital channels. It is proposed to develop and implement mechanisms for regulating digital communication in the public law sphere based on a balance between the interests of the State, private individuals and the protection of human rights in the online environment. The need to use positive experience of the EU and other countries of the world, which have developed and adopted legal instruments governing the creation and use of artificial intelligence and standardized the digital transformation of their countries and the EU as a whole, is substantiated.

Keywords: Data Security, Confidentiality, Public Law Policy, Digital Technologies, Artificial Intelligence

INTRODUCTION

The modern world is experiencing a period of rapid technological development, which is continuously transforming our society in all spheres of life. Digital technologies have become an integral part of our everyday existence and affect all aspects of the present – economic, social, cultural, political and educational ones (Kuchmiiova, 2023 68). Such a thesis can be found in almost any discussion or study devoted to the impact of digital technologies on modern society. Its importance lies in the fact that everyone can feel the «consequences» of their influence on our everyday life when using a smartphone, smart watch or any other gadget to watch the news on the Internet, participate in virtual discussions or receive electronic services of government bodies for various transactions and information. A vivid example of the successful transition of public services to the convenient digital format is the project “Digital State” (Official Website “Diia”, 2024), the goal of which is to unite all State departments of Ukraine into a single suitable and effective online system. The EU also declared digital transformation as one of the EU’s priorities (European Parliament, 2024), which is based on the following pillars: 1) technology that works for the people 2) a fair and competitive digital economy; 3) an open, democratic and sustainable society (European Commission, 2020).

Undoubtedly, digital technologies simplify and facilitate communication between citizens and the State, broaden the framework for collaboration and partnership, and provide an opportunity for inclusive, innovative social development. This is all the way of the formation of the electronic State, the main conceptual idea of which is “round-the-clock information influence of the state on society and the interaction of the state with each specific citizen” (Burdin, 2021: p. 34). However, this is only one side of the problem, because technological development not only optimizes the ways of interaction between people and the State, but also changes the...

¹ Ph.D. in Law, Scientific Institute of Public Law (Kyiv, Ukraine). E-mail: Zubko18@gmail.com. https://orcid.org/0000-0003-2025-0202
² Ph.D. in Law, Lawyer (Kyiv, Ukraine). E-mail: maxim.sokiran@gmail.com. https://orcid.org/0000-0002-1682-2012
³ Ph.D. in Law, Researcher, Information Analysis Center for Aerospace Law (Kyiv, Ukraine). E-mail: a.danylenko07@ukr.net. https://orcid.org/0000-0001-8263-1364
⁴ Ph.D. in Law, Researcher, Analysis Center of Air and Space Law (Kyiv, Ukraine). E-mail: diana.levchenko5@gmail.com. https://orcid.org/0000-0001-8343-2260
⁵ Doctor of Law, Senior Researcher, Izmail State Humanitarian University (Izmail, Ukraine). E-mail: 6222410@ukr.net. https://orcid.org/0000-0001-6080-7752
very nature of this interaction, turning it into digital communication, which is not yet free of implementation shortcomings in the context of public law.

**METHODOLOGY**

This research is based on a complex and interdisciplinary approach, which represents a combination of methods and means of various scientific disciplines. The main components of this approach allow to cover various aspects of the investigated problem and provide a deeper and more objective understanding of the essence of digital communication in the public law sphere. In particular, the following approaches were used:

Legal analysis method made it possible to determine the legal factors influencing digital communication, as well as the balance of using the opportunities of digital communication while ensuring data security and privacy as inalienable rights of people.

Technical analysis method was used to identify individual technical characteristics and capabilities of digital technologies, determine their impact on communication processes and means of their protection.

The method of social and psychological analysis contributed to the study of the features of interaction between communication actors, their motivation and attitudes towards digital means of communication.

The method of systematization and evaluation of internal and external factors provided an opportunity to identify problems in various areas, as well as to determine the risks associated with the processing and transmission of information in the digital environment.

Dialectical method helped to explore in more detail the possibilities of digital technologies used in the Ukrainian project “Digital State” and the new European law on artificial intelligence; to highlight the following dialects of possible contradictions: confidentiality versus publicity; individual rights against the interests of national security; privacy versus government transparency.

**LITERATURE REVIEW**

Research into the determinism of digital communication in public law reflects a wide range of works and approaches to this issue. The transition of general communication into a form of digital communication formed Spitzberg (2000), Benson, Johnson and Kuchinke (2002), Bordi, Okkonen, Mäkiniemi and Heikkilä-Tammi (2018), Asunta and Mikkola (2019).

Regarding the direct determination of the essence of digital communication and its features, Roberts (2023) provides a comprehensive overview of digital communication, explaining its concepts on examples of real life. Yarema (2022) formed a methodological approach to the formation of the concept of digital communication.

In the context of the public law sphere, certain features of the impact of digital technologies on modern society were considered in the works by Kuchmiiova (2023), Burdin (2021), Kivalov (2015) and Tokareva (2021). When forming the specifics of digital communication, priority is given to the problem of data security and confidentiality, which was defined in the works of Ayed and Ghernaouti-Helie (2011), Custers, Calders, Schermer, and Zarsky (2013), Minkkinen, Auffermann, and Heinonen (2017), Bryzhko and Pylypchuk (2020).

The definition of the practical implementation of digital communication in the public law sphere was accompanied by the analysis of public policy, legal aspects of digital transformation and the application of artificial intelligence in the EU and Ukraine in the research by Soroka and Kurkova (2019), Soroka, Danylenko and Sokiran (2022) and Drozd (2023).

With the help of a wide range of sources covering various aspects of digital communication in the public law sphere, one can form an integrated understanding of the determinism of digital communication. Sources such as European Union documents play an important role in this regard, to help understand the international context and approaches to digital communication and artificial intelligence. The newest view on the essence of digital communication is driven by changes in various aspects of social development and the need to create effective management practices for digital technologies, digital communication and artificial intelligence.
RESULTS

Back in 2015, Kivalov (2015: 5) drew attention of the scientific community to the fact that the public law sphere from the beginning contains numerous contradictions considering the presence of «overlap» interests of the State and the individual. Perhaps because it is accompanied by the principle of imperative, which provides for the compliance with certain rules and regulations arising from public law relations by State agencies and citizens (Tokareva, 2021: 206). This creates special conditions for the emergence of contradictions since the interests of the State and private individuals do not always coincide.

The possibility of a contentious relationship in the context of implementation of interdepartmental interaction should be specified separately because the actors of communication may, for example, complicate (if not negate) mechanisms for the effective implementation of legal norms due to the lack of procedures for their incorporation or negligence.

Digital communication, as a component of the modern public law, strengthens these dynamic processes, mainly due to the instability of the legal regulation of the digital environment.

To confirm or refute this thesis, practical discourse on understanding the legal phenomenon “digital communication” should be elaborated in detail, as well as contradictions and problems in the mechanisms of its implementation within the public law area should be defined.

DISCUSSION

Essence and Features of Digital Communication as A Tool for Implementing Management

Communication is a form of interaction. The general nature of communication is ambiguous and ambivalent. This statement can be taken as a reference to characteristics that discredit good communication. The definition of «good» implies a link between ethics and pragmatic quality, and this provides a useful starting point for the discussion on communication competences. However, the question of what is "bad" and "good" is a rather controversial one in the field of communication and philosophy, as this issue naturally crosses ethics and ideology (Spitzberg, 2000). The question of what makes communication «bad» or «good» can cause controversy, therefore, the evaluation of communication requires attention to the ideological implications.

If we expand communication and form digital communication, today it is important to consider the latter in the context of ambivalence of communication, understanding how the positive aspects of digital communication can be balanced with challenges and risks it presents to the society. On the one hand, digital technologies expand the possibilities of communication, providing quick access to information and facilitating transparent exchange of thoughts and ideas. However, on the other one, they also raise questions about the quality of this communication and its impact on the society. For example, social networks can provide platforms for broad discussion of topics and ideas, but at the same time they can facilitate the spread of misinformation and the formation of isolated echo chambers where groups of people exchange only their own views.

Today, many countries of the world face the challenges of combating the spread of disinformation and fake news. One of the latest piece of such news is information about the death of the King of the Great Britain – Charles III. (The Guardian, 2024). Therefore, the reliability and validity of information circulating in the digital space is becoming more and more important, because it can influence public opinion and decision-making. New forms of digital communication require redefinition of ethical considerations, in particular, the protection of confidentiality and respect for human rights in the online environment.

The traditional interpretation of digital communication is the transfer of information and knowledge through any electronic device that can support the relevant data format. However, with the development of technology and the spread of the Internet, this concept has evolved significantly (Universidad Europea, 2023). Roberts believes that digital communication is “the process of exchanging information, messages and ideas using digital technologies and platforms. It involves the transmission and receipt of data through electronic devices and networks, enabling real-time interaction between the actors, instant messaging, video conferencing, and long-distance distribution of multimedia content” (Roberts, 2023). According to Asunta and Mikkola (2019), digital
communication consists of different types of communication technologies and collaboration platforms that allow staff to interact with text, audio, video, and graphics in an open and networked manner. The authors define the importance of digital communications in the present business environment, noting that they enable effective interaction, cooperation and strengthening of relationships between employees and parties outside the organization, because beyond email and instant messaging, digital communication allows sharing, editing and keeping information public, which facilitates the creation of new social connections and strengthens existing relationships in the workplace. The basic idea behind this position is that digital communications not only promote effective interaction and collaboration within organizations, but also beyond them. Digital communication makes it possible not only to exchange information, but also to expand and maintain existing social relations.

Ten years ago, there was no clear idea of what digital communications were; Since then, digital communication has become a powerful tool connecting people and organizations around the world. It has revolutionized the way we interact, collaborate and share information and revealed endless possibilities by eliminating geographical boundaries. The potential of digital communications has been highlighted during the pandemic: businesses without digital communications strategy could not survive this time; video conferencing has become a communication channel, e-mail – the new normal way of sending messages (Roberts, 2023).

Nowadays, digital communication takes place in more complex environments as users can interact through different channels in real time and virtually simultaneously. So, today's digital communication is not linear, but multi-level and multi-channel. Social networks are probably the best-known example of digital communication, but corporate blogs and videos are also digital means of interaction (Universidad Europea, 2023).

In our opinion, digital communication is the process of interaction, exchange of information, ideas and opinions using digital technologies and platforms. Digital communication enables real-time communication, instant messaging, and collaboration across geographic distances, creating opportunities for open dialogue and multi-stakeholder engagement on important issues. Digital communication facilitates mutual understanding, cooperation and problem-solving in various fields, including business, government, education and community activities. It encompasses a wide range of interactive tools, including websites, social networks, e-mail, video conferencing and other digital communication channels. Digital communication is a key element of the modern world, where speed, accessibility and efficiency of communication determine success in various fields of activity.

In the context of governance implementation, digital communication makes it possible to avoid time and space boundaries, save resources when searching for important information and send it to the addressee, quickly solve the problems, simultaneously perform complex tasks involving a significant number of participants, establish operational communication between the authorities and the public. On the other hand, in addition to numerous advantages, the governments of individual countries use the possibilities of digital communication not only to create fakes (as we have already indicated above), but also to manipulate public opinion, taking advantage of the lack of established skills for critical analysis of resources and data and the inability to clearly distinguish between virtual and real space (Yarema, 2022; Lolai et al., 2023).

Accordingly, digital communication as a management tool is an integrated set of technological means and practices aimed at establishing effective communication, information exchange and coordination between different levels of government among themselves and separately with the public. Digital tools in this context perform a number of important functions (in addition to directly ensuring interaction, they also help to monitor and analyze public opinion, solve problems and incorporate strategic initiatives considering the needs of society, ensure effective coordination of actions and tasks among the various government bodies, provide access to information, etc.). At the same time, the successful implementation of digital government communication requires the consideration of social, technical and organizational aspects, as well as constant improvement of communication strategies and tools, taking into account the development of technologies and the society needs.

When studying the features of digital communication as a tool for the implementation management, one should consider the possibility of the influence of the general process of digitalization on the activities of any structures. For example, digitization in the global work environment is now being used for improving performance and promoting organizational development and change (Benson, 2002). Therefore, the goal of the aforementioned
"Digital State" project is to make 100% of public services in Ukraine available online by the end of 2024 (Ministry of digital transformation 2024).

The features of digital communication as a tool for implementing management are formed on the basis of factors affecting this communication. First of all, it is the creation of unified standards for such communication (Soroka, 2019; Soroka, 2022). It should be noted that nowadays only a few countries in the world have adopted legal instruments governing the use of artificial intelligence and the digital transformation of public authorities. For example, the EU adopted such act only in 2023 (European Parliament, 2024); it establishes a common framework for the use and supply of AI systems in the EU (Future of Life Institute, 2024). Canada passed the Digital Charter Implementation Act of 2022, which enacted three acts: the Consumer Privacy Act, the Artificial Intelligence and Data Act, and the Personal Data and Personal Data Protection Tribunal Act (Government of Canada, 2022). Germany has a German Standardization Roadmap for Artificial Intelligence (Large, 2020).

Secondly, the quality of digital communication. This was pointed out by the authors of the article "Communication in the Digital Work Environment: Implications for Wellbeing at Work". They combined the first and second factors and proposed their own six factors affecting digital communication, including: 1) the amount of digital communication, 2) expectations of constant communication, 3) quality of messages, 4) adaptation of new tools, 5) technical problems and 6) flexibility of communication. Besides, the authors determined that the impact of digital communications on the well-being of certain activities, including governance, is largely determined by the development of effective communication standards and rules. After all, digital communications can be the source promoting a sense of control and autonomy; on the other hand, the aspects of digital communication limiting control can be the obstacle to ensuring well-being at work and in governance in particular (Bordi, 2018).

Accordingly, the factors affecting digital communication determine its features. It is also necessary to consider the sphere, in which digital communication is carried out. For example, this is public administration or justice (Drozd, 2023). Therefore, the features of digital communication as a tool for the implementation of management are:

– global reach (digital communication allows governments to communicate with citizens and other management structures not only at the local level, but also at the national and international ones, which expands opportunities for coordination and cooperation);

– interactivity (digital communication allows for interaction and enhanced communication between the government and citizens, creating opportunities for active involvement of the public in the management process);

– speed (digital communication allows government agencies to respond quickly to the events in real time, which helps increase the speed of problem solving and the efficiency of decision making);

– personalization capability (digital communication enables government to adjust communication with individual groups of citizens according to their interests and needs, which contributes to improving interaction and mutual understanding);

– increasing accessibility (digital communication makes it possible to make government services and information more accessible to citizens in any place and time, which helps to reduce barriers to access to government resources and services);

– adaptability (digital communication enables government structures to quickly respond to the changes in society and the economy, as well as to adapt their strategies and policies in accordance with new challenges and opportunities);

– the increased need to protect security and privacy (when using digital communication, governments need to pay special attention to protecting personal data and preventing cyber-attacks).
The last feature (increased need to protect security and privacy), as the war in Ukraine has indicated, is the most determining factor for effective and secure digital communication, as cyber-attacks allowed the war to expand to digital space.

**Security and Privacy Issues in Digital Communication in The Public Legal Sphere**

Security and privacy are one of the pressing issues of the digital age. New technologies and surveillance methods are constantly creating new threats to privacy. Nowadays, there is public debate about the desired future of society and the role of privacy in it. This debate requires serious consideration of the systemic linkages that challenge privacy, particularly when using digital communication tools (Minkkinen, 2017; Al-Hussein & Shahba, 2023). Therefore, ensuring security and protecting privacy is one of the key issues in the current digital transformation.

Privacy protection is perceived as a means, which will protect people’s identity, reduce identity theft and increase trust. In many initiatives to implement digital identifier management systems, privacy needs are considered only from a technical perspective and they are not regarded to be part of the basic requirements of the software from the beginning of the projects. However, as Ayed and Ghermaouti-Hélie (2011) correctly point out, confidentiality should be considered from the outset, using an integrated and interdisciplinary approach. Accordingly, it is impossible to talk about the development of digital communication capabilities without including the issues of security and privacy protection in an overall integrated and interdisciplinary approach.

The problem of privacy protection arose from the need to expand the possibilities of obtaining personal knowledge about people, which in some cases is necessary to protect security, but in other ones can directly violate people’s rights. Processing huge amounts of data can lead to situations where data controllers (government entities) obtain a lot of personal information. In some cases, these entities may know more about individuals than they know about themselves (Custers, 2013). Therefore, the balance between privacy and security of personal data is a complex issue that cannot be solved by politicians, lawyers, technical specialists, or special services on the basis of past-tense views. The protection of personal data is generally not limited to the requirements for ensuring the quality of technical data processing and strengthening interdiction measures to create an overall security environment (Bryzhko, 2020).

Thus, serious security and privacy issues may arise in the public legal sphere when using digital communication. In particular, the risk of violation of citizens’ privacy is increasing due to insufficient control over the collection and processing of personal data by government structures. Besides, the lack of adequate security of this data can contribute to cybercrime and unauthorized access to sensitive information. There is often a problem of underestimating the risks associated with the use of digital tools, which can lead to vulnerability of cyber-attacks. In addition, it is important to consider ethical aspects and justice issues in the processing of data by government structures to avoid discrimination and maintain the trust of citizens in public institutions. Ensuring security and confidentiality of digital communication in the public law sphere requires a comprehensive approach and the adoption of necessary measures to improve legal regulation and technological means of data protection.

All these challenges were considered when the EU Law on Artificial Intelligence was adopted; the EU Parliament defined the following priorities to overcome them: artificial intelligence systems used in the EU must be safe, transparent, traceable, non-discriminatory and environmentally friendly, and these systems must be controlled by people (European Parliament, 2024; Mazingue, 2023).

**CONCLUSIONS**

Determining the nature of digital communication in public law takes into account important aspects of its functioning and impact on the society and government structures. Digital communication in the public law sphere is a key tool of modern governance, which promotes effective interaction between management bodies and citizens. It reveals wide opportunities for fast and transparent exchange of information, promotes public involvement in management processes and stimulates active public participation in policy formation and decision-making. It also facilitates effective governance by using a variety of digital tools to analyze, monitor and respond to societal needs. Digital communication is an important communication channel to help solve
complex problems and shape development strategies, ensure open dialogue and mutual understanding between the government and citizens.

Along with the using digital communication in management, important issues of data security and confidentiality arise. Insufficient control over the collection and processing of citizens’ personal data by government structures can lead to privacy violations and leakage of confidential information. Government digital communication systems are vulnerable to cyber-attacks that can lead to unauthorized access to sensitive information or data loss. Besides, digital communication can be used to spread misinformation and manipulate public opinion, threatening democratic processes and trust in government institutions. Lack of adequate protection can contribute to cybercrime such as identity theft or fraud through digital channels. The unstable quality of information circulating through digital channels can lead to panic, mistrust, and wrong decisions on the part of the public and government authorities. The latter may underestimate the risks associated with digital communication and be unprepared to respond to them. Lack of clear data management policies and procedures may result in incorrect processing, alteration or loss. The general context of these problems requires an integrated approach to ensuring security and confidentiality in the public legal sphere, taking into account technical, legal, ethical and organizational aspects.

Therefore, rapid changes in technology, lack of specialized legal instruments, strategic planning and a number of other objective adverse factors are the key basis for confusion or ambiguity in the mechanisms for implementing the legal obligations and rights of participants in digital communication.

To solve the identified problems and ensure a proper balance between privacy and publicity, individual rights and national security interests, confidentiality and transparency of authorities, it is necessary to use positive experience of the EU and other countries of the world that have developed and adopted legal instruments governing the creation and use of artificial intelligence and standardized the digital transformation of their countries and the EU as a whole. Ukraine’s experience in the implementation of the national project “Digital State” also demonstrated that such projects can successfully resist cyber-attacks and be an easy and accessible digital tool for citizens and businesses, while achieving the specified balance.

REFERENCES


