ANDREICHENKO S. S.

International Humanitarian University,
Professor of the Department of International and European Law,
Doctor of Law, Associate Professor

THE ROLE OF THE EUROPEAN COURT'S PRACTICE IN PROTECTION OF THE RIGHT TO RESPECT OF PRIVATE AND FAMILY LIFE DURING THE ERA OF DIGITAL TECHNOLOGIES

Key words: *human rights, right to respect of private and family life, European Court of Human Rights, the information society.*

Does digital technology offer us fresh hope for the realization of human rights – or the Game is Over? Everyone is aware of the immense benefits that our digital era delivers in just about every area of life. Human rights perspective is not an exception. Social media and tools such as encrypted communications help to connect and grow the movements of human rights defenders. Human rights officers can gather information from social media sources, in addition to enhancing or supplementing human rights investigations by using satellite imagery and encrypted communications to ensure better monitoring, investigation and analysis. A wide range of applications have been developed to assist investigators to verify that the information they gather is genuine and accurate. Other digital tools help investigators identify patterns within their data that can be matched with other, open-source information sets. Digital tools can also help us with early warning. Spikes of hate speech and other online indicators of rising tensions can constitute a significant alert to impending violence. Human rights employees are not just using digital tools to detect violations: they are also employing that knowledge to prevent further violations. So, to this extent – and in many more ways – digital tools are our friends and allies in upholding people's rights [1].

At the same time, it becomes obvious that the rapid development of the digital sphere has negative aspects. The use of modern digital technologies by states may involve violation of the fundamental values of a democratic society, and in particular the right to respect of private and family life.

The problem of ensuring the right to respect of private and family life has received considerable attention in the European system of the human rights protection. It goes without saying that the core of this system is the Convention for the Protection of Human Rights and Fundamental Freedoms (Convention) (1950), in conjunction with a specially created and unique monitoring mechanism in the form of the European Court of Human Rights (ECHR). The right of individuals to apply to the ECHR is fairly considered as the cornerstone of the international system for the protection of human rights. Therefore, the analysis of the practice of the ECHR regarding the violation of Article 8 of the Convention in the context of the use of new information technologies is of great importance.

Article 8 declares that, everyone has the right to respect for his private and family life, his home and his correspondence. Moreover, there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others [2].

Here is an example from the recent ECHR practice in relation to Article 8 in the context of the use of digital data.

The case *«Benedik v. Slovenia»* (April 24, 2018) concerned the Slovenian police's failure to obtain a court order to access subscriber information associated with a dynamic IP address recorded by the Swiss law-enforcement authorities during their monitoring of users of a certain file-sharing network. This led to the applicant being identified after he had shared files over the network, including child pornography [3].

The applicant complained that his right to privacy had been breached because the Internet service provider (hereinafter «the ISP») had retained his alleged personal data unlawfully and the police had obtained subscriber data associated with his dynamic IP address and consequently his identity arbitrarily, without a court order, in breach of Article 8 of the Convention [4, para 73].

The Court reiterates that private life is a broad term not susceptible to exhaustive definition. Article 8 protects, inter alia, the right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of «private life» (see Uzun v. Germany, no. 35623/05, § 43, ECHR 2010-VI (extracts)) [4, para 119].

The Court concludes that the applicant's interest in having his identity with respect to his online activity protected falls with the scope of the notion of «private life» and that Article 8 is therefore applicable to this complaint [4, para 142].

The Court found in particular that the legal provision used by the police to obtain the subscriber information associated with the dynamic IP address had not met the Convention standard of being «in accordance with the law». The provision had lacked clarity, offered virtually no protection from arbitrary interference, had no safeguards against abuse and no independent supervision of the police powers involved. The Court holds, by six votes to one, that there has been a violation of Article 8 of the Convention.

In the case «K.U. v Finland» (2008) [5], concerns the use of criminal law in the protection of privacy, the ECHR found that the positive obligations of the Contracting States to ensure the protection of private life entailed an obligation to provide law enforcement agencies with the ability to obtain access to dynamic IP addresses and communication data in order to identify a private person who has violated another individual's right to private life. The ECHR judgment in K.U. v Finland contributes to the definition of the balance between the freedom and confidentiality of communications and anonymity

over the internet, and the requirements of privacy and limitations of anonymity and confidentiality of communications [6].

It should be emphasized that the Court found a positive obligation under Article 8 of the Convention, which was formulated as a negative obligation. International human rights law clearly establishes the responsibility of states for the protection, promotion and respect of human rights. This responsibility exists not only when the state directly violates human rights, but also when the state is not able to protect persons under its jurisdiction from such violation.

The European Court of Human Rights very often uses the notion of a positive obligation. The Court in its case-law has slated that States parties to the Convention must adopt measures necessary to protect human rights and freedoms specified by the ECHR with respect to both actions of a State and that of private persons and entities [7, p. 12].

Examples of the first «fundamental» cases concerning positive obligations under Art. 8 were Marckx v. Belgium (1979), X. and Y. v. Netherlands (1985) [8]. That being said, in the case of X. and Y. v. the Court recalled that although the purpose of Article 8 is mainly to protect the individual from arbitrary interference by the state, it does not simply oblige the state to refrain from such interference: this negative commitment may be supplemented by positive commitments, inalienable from true respect to private or family life. These obligations may include taking measures aimed at ensuring respect for private life even in the field of relations between individuals (para 23).

By determining whether a positive commitment exists, should be established balance between the interests of the entire society and the interests of individuals; the search for this balance is the purpose of the entire Convention.

Thus, states are obliged to respect and protect rights. They must not only refrain from violations through their agents and apparatus, but also make sure that the rights are not abused by other subjects. This requirement for the protection of human rights in a broader sense, of course, includes the obligation to prevent non-state subjects from violating human rights, although this obligation may be difficult to define and apply in practice.

In general, the practice of the ECHR in the use of information technologies demonstrates the application of traditional principles by the European Court such as: proportionality, proportionality of restrictions, respect for the balance of interests in the assessment of legislative measures and law enforcement practice. However, the expansion of intervention in the private life of a person by means of new state-of-the-art technologies indicates the need to develop new guarantees for the observance of human rights in the information society.

If humanity strives to fulfill the plan outlined in the Sustainable Development Agenda until 2030 and create a safer, more stable, fair and prosperous world for all, everyone needs to support human rights in all areas, including digital.

References:

1. Human Rights in a New Era. Speech at the University of Geneva by UN High Commissioner for Human Rights Michelle Bachelet. 14 November 2018. URL: https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=23874&LangID=E.
2. Convention for the Protection of Human Rights and Fundamental Freedoms (Convention) (1950). URL: https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c.
3. Police's accessing of subscriber information associated with a dynamic IP address needed court order; Slovenian law lacked clarity ECHR 160 (2018) 24.04.2018. URL: https://hudoc.echr.coe.int
4. Benedik v. Slovenia. Judgment of the European Court of Human Rights of April 24, 2018. URL : https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-182455%22]}.
5. K.U. v. Finland. Judgment of the European Court of Human Rights of December 2, 2008. URL: https://www.juridice.ro/wp-content/uploads/2016/07/K.U.-v.-FINLAND-en.pdf.
6. Tuomas Pöysti. Judgment in the case of K.U. v. Finland: The European Court of Human Rights Requires access to communications data to identify the sender to enable effective criminal prosecution in serious violations of private life. Digital Evidence and Electronic Signature Law Review, Vol 6, 2009. URL: https://sas-space.sas.ac.uk/5452/1/1855-2575-1-SM.pdf.
7. Ziemele I. Human Rights Violations by Private Persons and Entities : The Case-Law of International Human Rights Courts and Monitoring Bodies. EUI Working Papers. Academy of European Law. 2009. № 8. 25 p.
8. X. and Y. v. Netherlands. Judgment of the European Court of Human Rights of 26 March 1985. EHRR. Vol. 8. P. 235.

KHARITONOVA T. E.

National University «Odesa Law Academy»,
Head of the Department of Agrarian, Land and Environmental Law,
Doctor of Law, Associate Professor

PAVLYHA A. V.

National University «Odesa Law Academy»,
Student of the Faculty of Civil and Economic Justice

USE OF DRONES IN UKRAINE AS A METHOD OF DIGITALIZATION IN AGRICULTURE SECTOR

Key words: *agriculture sector, dronization, drones, digitalization.*

Until recently, agriculture was the most traditional economic sector. Any innovations here have taken root quite slowly. The development of modern technology forever changes our perceptions of the agricultural sector. The