

INTERNATIONAL PROTECTION OF EMPLOYEE'S PRIVACY UNDER THE EUROPEAN CONVENTION ON HUMAN RIGHTS

Assoc. Prof. Dr. Elena Sychenko *

UDK: 347.94:349.2(4)

342.734(4)

341.231.14(4)

Pregledni znanstveni rad

Primljeno: listopad 2016.

In the diversity of national approaches to the problem of protection of employees' privacy at work, the jurisprudence of the European Court of Human Rights provides a priceless framework for the consideration of cases concerning employee's privacy. Even though the term "privacy" was not used by the Strasbourg Court, its broad interpretation of the right to respect for private life significantly contributed to the protection of personal data, elaborating positive obligations of the states. The article researches how the European Convention on Human Rights is adapted to protect employees' personal data, to restrict unauthorized video surveillance, searches, interception of telephone calls at work and takes into account the most recent case, Bărbulescu v. Romania, considered in 2016. It focuses on the Court's approach to the lawfulness and necessity of the interference with employee's privacy, as it has particular value for the employee's protection on the national level in the countries of the Council of Europe.

Keywords: privacy, employment, European Court of Human Rights, data protection, reasonable expectation of privacy

* Elena Sychenko, Ph. D., Associate Professor, Faculty of Law, Saint Petersburg State University, ul. K. Marksa, d. 36a, kv. 21, Gatchina, Leningrad region, Russia; e.sychenko@mail.ru;
ORCID ID: orcid.org/0000-0002-7045-9218

I. INTRODUCTION

As early as in 1890, the famous Judge Brandeis and Samuel D. Warren wrote that the right to life should be understood in an evolutionary way and include the right to be let alone.¹ The authors justified their conclusion by referring to the intensity and complexity of life, arguing that solitude and privacy had become more essential to the individual due to modern enterprise invading upon his privacy and by which such intrusion subjected an individual to mental pain and distress, such pain being far greater than could be inflicted by mere bodily injury.² It is interesting to note that contemporary scholars also refer to the analogous circumstances for urging the protection of privacy, adding globalisation and the threats of terrorism to the mix.³

More than 100 years have passed since the publication of that article but neither scholars nor case law have elaborated a unique definition of privacy or private life. Some European scholars perceive privacy as the logic of self-determination and of informational control on personal data⁴, or as a sphere that ought to be free from State intrusion.⁵ These opinions are, however, in line with the understanding of privacy as personal autonomy. The same approach has also been proposed by Russian scholars.⁶

The protection of private life in the context of employment relations is a very interesting subject, as the workplace is not a “private” place in the strict sense. The peculiarity of employment relations, namely the requirement for subordination of the employee and control of the employer over the employee, are other factors highlighting the unique approach that needs to be taken to protecting the private life of an employee. Researching the extent of a worker's right to privacy, Prof. Hendrickx pointed out that the employee's right to

¹ Warren, S. D.; Brandeis, L. D., *The Right to Privacy*, Harvard Law Review, Vol. 4, No. 5, 1890, p. 193.

² *Ibid.*, p. 196.

³ See Pagallo, U., *La tutela della privacy negli Stati Uniti d'America e in Europa: modelli giuridici a confronto*, Milano, Giuffrè Editore, 2008, p. 37.

⁴ Arnaud, S., *Analyse économique du droit au respect de la vie personnelle: application à la relation de travail en France*, Revue internationale de droit économique, Vol. XXI, No. 2, 2007, p. 130.

⁵ Löhmus, K., *Caring Autonomy: European Human Rights Law and the Challenge of Individualism*, Cambridge, Cambridge University Press, 2015, p. 48.

⁶ Zykina, T. A., *The right of employees to private life protection* [Pravo rabotnika na neprikosновенost' lichnoy (chastnoy) zhizni], Pravovedeniye, No.1, 2007, pp. 81 – 87.

privacy is qualified by the employer-employee relationship and therefore the employee's privacy expectations must necessarily be accordingly reduced.⁷

Article 8 of the European Convention on Human Rights provides a general basis for privacy protection in the countries of the Council of Europe. It guarantees the right to respect for private life and privacy protection is one of the facets of this right. Scholars note that the material scope of the right to privacy as a part of the right to respect for private life has been extended considerably.⁸ In this article the development of the Court's approach to employee's privacy protection will be traced, analysing successively the main concepts, used in the adjudication of such cases. Chapter 2 will research the concept of the "reasonable expectation of privacy", chapters 3 and 4 will analyse the steps of consideration of "privacy" cases. The positive obligations of the states in the field of employees' privacy protection will be formulated in chapter 5. The last chapter will emphasize the value of the Court's conclusions for the enhancement of employees' privacy protection.

2. REASONABLE EXPECTATION OF PRIVACY

The European Court of Human Rights (ECtHR) repeatedly stated that it is impossible and unnecessary to attempt an exhaustive definition of what "private life" in Article 8 means.⁹ Such an approach permitted the Court to consider cases on data protection, on access to information, on the interception of phone calls and video surveillance at work etc.

The roots of the Strasbourg protection of the employee's private life can be found in *Niemietz v. Germany*.¹⁰ The ECtHR considered the application of the lawyer who claimed that the search of his office amounted to the violation of

⁷ Hendrickx, F.; Van Bever, A., *Article 8 ECHR: judicial patterns of employment privacy protection*, in: Dorsemont, F.; Lörcher, K.; Schömann, I. (eds.), *The European Convention on Human Rights and the Employment Relation*, Oxford, Hart Publishing, 2013, p. 185.

⁸ Van der Sloot, B., *Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"*, *Utrecht Journal of International and European Law*, Vol. 31, No. 80, 2005. Available at: <http://www.ivir.nl/publicaties/download/1555> (accessed 20.05.2015); Ryssdal, R., *Data Protection and the European Convention on Human Rights*, in: *Data Protection, Human Rights and Democratic Values, Proceedings of the 13th Conference of Data Protection Commissioners held 2-4 October 1991 in Strasbourg*, Strasbourg, CoE, 1992, p. 42.

⁹ ECtHR, *Niemietz v. Germany* (13710/88) 16/12/1992, para. 29.

¹⁰ *Ibid.*

respect of private life. It acknowledged that the notion of “private life” should include activities of a professional or business nature “since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world”.¹¹ Such an interpretation was found to be consistent with the essential object and purpose of Article 8.

The ECtHR’s conclusions, as expressed in *Peck v. UK*¹², are also valuable for the protection of employees’ privacy in so far as this case concerned the protection of privacy in public places. The ECtHR stated that even interpersonal relations conducted in a public context may fall within the scope of “private life”. The focus of the ECtHR on the lawfulness and necessity of interference with an employee’s private life, as well as its consideration of the concept of a “reasonable expectation of privacy”, provides national courts with a range of tools by which to consider such cases.

Cases on employee’s privacy as adjudicated by the ECtHR can be divided into two main groups – data protection, in which the Court deals with the legality of it being collected, used and disclosed; and the protection from interference with private life by activities such as workplace monitoring using video surveillance, searches of offices and equipment and the interception of workplace telephone calls.

The establishment of the employee’s reasonable expectation of privacy is the main instrument for determining the interference with the applicant’s private life. It was always used in the adjudication of the second group of cases. In contrast, the ECtHR referred to this factor only briefly in one case dealing with the use of personal information. Thus, in *Pay v. UK*¹³, considering the application by a probation officer who was dismissed for being engaged with the activities of BDSM community (bondage, domination and sadomasochism), the ECtHR stated that when people knowingly participate in activities which may be recorded or reported in a public manner, a person’s reasonable expectations as to privacy may be a significant, though not necessarily conclusive, factor.¹⁴

Scholars note that the establishment of the “reasonable expectation of privacy” by the ECtHR is based on concrete context of a given situation and

¹¹ *Ibid.*, para. 31.

¹² ECtHR, *Peck v. the United Kingdom* (44647/98) 28/01/2003, para. 57.

¹³ ECtHR, *Pay v. the United Kingdom* (32792/05) inadmissible 16/09/2008.

¹⁴ *Ibid.*

the relevant facts. The reasonableness of these expectations depends, amongst other things, on the questions of whether the employee was informed about the fact that an interference with his right to privacy was possible; the presence of specific indications of the possibility of such interference; or the (permanent) nature and the impact of the interference.¹⁵ The ECtHR's jurisprudence provides several examples of an employee's reasonable expectation of privacy.

In *Halford v. UK*¹⁶ the ECtHR held that the applicant, who claimed that the interception of telephone calls made from the workplace violated her right to respect for private life, had a reasonable expectation of privacy with respect to calls made from her work telephone. The applicant, who was at the relevant time the highest-ranking female police officer in the United Kingdom, brought discrimination proceedings after being denied promotion to the rank of Deputy Chief Constable over a period of seven years. She alleged that her telephone calls had been intercepted with a view to obtaining information to use against her in the course of the proceedings, the respondent State did not contest this point.¹⁷ The ECtHR found that telephone calls made from business premises may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8.¹⁸ In order to establish the expectation of privacy, the ECtHR gave weight to the following details: the applicant was not warned about the possibility that her calls might be intercepted; one of the telephones in her office was specifically designated for her private use; and she had been given the assurance that she could use her office telephones for the purposes of her sex-discrimination case.

In a similar case considered 10 years later, *Copland v. UK*¹⁹, the ECtHR applied the same line of reasoning to the collection and storage of personal information relating to the use of the telephone, e-mail and internet at the workplace. The applicant was employed by Carmarthenshire College, a statutory body administered by the State. She became aware that enquiries were being made into her use of e-mail at work when her step-daughter was contacted by the College and asked to supply information about e-mails that she had sent to the College. According to the State, the employer was monitoring the applicant's phone calls, e-mails and internet usage in order to ascertain whether

¹⁵ Hendrickx, F.; Bever, A.V., supra note 7, p. 189.

¹⁶ ECtHR, *Halford v. the United Kingdom* (20605/92) 25/07/1997.

¹⁷ *Ibid.*, para. 47.

¹⁸ *Ibid.*, para. 44.

¹⁹ ECtHR, *Copland v. the United Kingdom* (62617/00) 03/04/2007.

the applicant was making excessive use of College facilities for personal purposes. The ECtHR stated that the applicant had a reasonable expectation as to the privacy of calls made from her work telephone, as well as in relation to her use of e-mail and the internet²⁰ because she had not been warned about the possibility of this use being monitored²¹, and telephone calls from business premises, e-mails sent from work and information derived from the monitoring of personal internet usage are protected under Article 8. The establishment of the interference with the right to respect for private life required the ECtHR to proceed to consider whether the interference was lawful. As there were no provisions at the relevant time, either in general domestic law or in the governing instruments of the College, regulating the circumstances in which employers could monitor employees' use of telephone, e-mail and internet, the ECtHR concluded that the interference was not "in accordance with the law" as required by Article 8-2 of the ECHR.²²

In *Peev v. Bulgaria*²³, the ECtHR applied the test of a reasonable expectation of privacy in a case involving unauthorised searches undertaken by an employer in the applicant's office. The applicant, an expert at the Criminology Studies Council of the Supreme Cassation Prosecutor's Office, wrote a letter which was published in a daily newspaper. In that letter, he criticised the Chief Prosecutor. After the letter was published his office was sealed off and searched. During the search, a draft resignation letter was found and that draft was then used as the basis for formally terminating his employment.

The ECtHR had to consider whether the applicant had a reasonable expectation of privacy at his workplace. In the ECtHR's opinion, the applicant had such an expectation, if not in respect to the entirety of his office, then at least in respect to his desk and his filing cabinets where a great number of personal belongings were stored. The ECtHR presumed that the privacy of a workplace desk was implicit in habitual employer-employee relations. As the employer did not adopt any regulation or policy discouraging employees from storing personal papers and effects in their desks or filing cabinets, there were no arguments to demonstrate that the applicant's expectation was unwarranted or unreasonable.²⁴

²⁰ *Ibid.*, para. 42.

²¹ ECtHR, *Copland v. the United Kingdom* (62617/00) 03/04/2007.

²² *Ibid.*, para. 48.

²³ ECtHR, *Peev v. Bulgaria* (64209/01) 26/07/2007.

²⁴ *Ibid.*, para. 43.

In the more recent case of *Köpke v. Germany*²⁵ the ECtHR, for the first time, found that video surveillance of an employee made without her consent was permissible and not a violation of her rights under Article 8. The applicant, a supermarket cashier, was dismissed without notice for theft, following a covert video surveillance operation carried out by her employer with the help of a private detective agency. The ECtHR, in contrast to its decisions in *Peev*, *Halford* and *Copland*, did not enter into an analysis of the applicant's reasonable expectation of privacy. Instead, it briefly noted that this was not a necessarily conclusive factor. The ECtHR in this case seems to develop the idea, set out earlier in *Copland*, that: "the monitoring of an employee's telephone, e-mail or Internet usage at the place of work may be considered "necessary in a democratic society" in certain situations in pursuit of a legitimate aim".²⁶

As the applicant was employed by a private employer, the ECtHR considered the case in light of the positive obligation of the State to strike a fair balance between the applicant's right to respect for her private life at work versus both her employer's interest in protecting its property rights, guaranteed by Article 1 of Protocol no. 1 to the ECHR, and the public interest in the proper administration of justice. The ECtHR found that the State did not fail to provide a legal framework for privacy protection, as the relevant domestic courts considered the case in accordance with the developed case law of the Federal Labour Court, which provided a mechanism for striking the balance between competing rights of an employer and those of an employee.

Having satisfied itself as to the reasoning of the State's domestic courts, the ECtHR emphasised the following factors which they said the State had correctly evaluated in the process of balancing property rights versus employee's privacy:²⁷

1. The video surveillance was only carried out after losses had been detected during stocktaking in the department in which she worked;
2. The surveillance measure was limited in time and restricted in respect of the area;
3. The footage obtained was processed by a limited number of persons and used solely for the purposes of terminating the applicant's employment;

²⁵ ECtHR, *Köpke v. Germany* (420/07) inadmissible 05/10/2010.

²⁶ *Ibid.*

²⁷ *Ibid.*, para. 2.

4. The covert video surveillance of the applicant served to clear from suspicion the other employees who were not guilty of any offence;
5. There had not been any other equally effective means to protect the employer's property rights which would have interfered to a lesser extent with the applicant's right to respect for her private life.

Having regard to the due consideration of all these circumstances by national courts the ECtHR concluded that the domestic authorities had struck a fair balance between the applicant's right to respect for her private life under Article 8 and both her employer's interest in the protection of its property rights and the public interest in the proper administration of justice. It therefore dismissed the application as manifestly ill-founded.

Another interesting case concerning an employee's privacy was recently considered by the European Court. In *Bărbulescu v. Romania*²⁸ the applicant, an engineer in charge of sales working for a private company, was dismissed for using the company's internet for personal purposes during work hours in breach of internal regulations. The case concerned private messages, which were discovered by the employer while monitoring the use of a corporate Yahoo messenger account and its transcripts were used as a piece of evidence in the domestic labour court dismissal proceedings.²⁹

As it was demonstrated above, in such cases the Court traditionally investigates whether the applicant had a reasonable expectation of privacy, in other words, whether he might have expected that his communications would not be monitored.

In *Bărbulescu v. Romania*, the Court did not concentrate on the reasonableness of the employee's expectation of privacy. It pointed that the fact of previous notice about the possibility of Yahoo messenger monitoring remained disputable, as the notice presented by the Government did not bear the employee's signature. Dissenting Judge Pinto De Albuquerque noted that this case was an excellent occasion for the Court to develop its case-law in the field of protection of privacy with regard to employees' Internet communications³⁰ and attached attention to the lack of previous notice which, in his view, should have a decisive meaning in this case and should lead to the finding of a

²⁸ ECtHR, *Bărbulescu v. Romania* (61496/08) 12/01/2016.

²⁹ *Ibid.*, para. 44, 45.

³⁰ Partly Dissenting Opinion of Judge Pinto De Albuquerque, paras 1,10-12.

violation of the applicant's right to privacy.³¹ The majority, however, did not focus on the lack of a previous notice³² attaching more weight to balancing the applicant's right to respect for his private life and his employer's interests. The Court narrowed the scope of the application to the monitoring of the applicant's communications within the framework of disciplinary proceedings³³, leaving aside the applicant's arguments that his communications of personal and sensitive nature were disclosed to other employees and were publicly discussed.³⁴

The Court further confirmed the conclusion of national courts that the employer did not have another method to verify whether the applicant infringed internal policy as the applicant contested the fact of personal use of the Yahoo messenger.³⁵ It found that the employer acted within its disciplinary powers and pointed that the monitoring was limited in scope and proportionate.³⁶

³¹ Judge Pinto De Albuquerque referred to other international instruments, such as OECD Guidelines, Council of Europe Recommendation No. R (89)2, ILO Code of Practice, Council of Europe Recommendation Rec (2015), which provide the principle of informed and explicit consent for monitoring procedure.

³² ECtHR, *Bărbulescu v. Romania* (61496/08) 12/01/2016, para. 43.

³³ *Ibid.*, para. 55.

³⁴ *Ibid.*, para 31, 55. Dissenting Judge Pinto De Albuquerque, this point was not disputed by the Government.

³⁵ ECtHR, *Bărbulescu v. Romania* (61496/08) 12/01/2016, para. 60

³⁶ After the submission of the article the Chamber judgment in *Bărbulescu* was referred to the Grand Chamber which considered the case on the 30th November 2016 and delivered the judgment on the 5th September 2017. It seems that the Grand Chamber has followed the advice of Judge Pinto De Albuquerque to elaborate a comprehensive approach to the privacy of internet communications at work and pay particular attention to the absence of the advance notice about the possibility of communication monitoring. The Grand Chamber carried out an extensive overview of relevant international legislation and comparative law (para. 37-54, 13 pages out of 58 pages of the judgment). It further pointed out a number of new factors which should be essential for the national courts, considering relevant cases: (i) whether the employee has been notified of the possibility that the employer might take measures to monitor correspondence and other communications, and of the implementation of such measures. It also stated that the notification should normally be clear about the nature of the monitoring and be given in advance; (ii) the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy (monitoring of the flow of communications and of their content should be treated differently); (iii) whether the employer has provided legitimate reasons to justify monitoring the communications and accessing their actual content, requiring a weightier justification for the content monitoring; (iv) whether it would have been possible to establish a monitoring system based on less intrusive

3. ESTIMATING THE COMPLIANCE OF THE INTERFERENCE WITH LAW

In broadening the scope of private life in *Niemitz*, the ECtHR noted that the coverage of professional activities would not unduly hamper the Contracting States, for they would retain their entitlement to “interfere” to the extent permitted by Article 8-2.³⁷ Therefore the interference is permissible if it is in accordance with the law, pursues a legitimate aim and is necessary in democratic society.

The first test is particularly interesting in the cases on protecting an employee's privacy. The ECtHR had stated that the phrase “in accordance with the law” requires, at a minimum, compliance with domestic law. The quality of that law was also relevant, because it was expected to provide protection against arbitrary interference with individuals' rights under Article 8 and be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which the State would be entitled to resort to measures affecting those rights.³⁸ The ECtHR also

methods and measures than directly accessing the content of the employee's communications; (v) the consequences of the monitoring for the employee subjected to it; (vi) whether the employee had been provided with adequate safeguards, especially when the employer's monitoring operations were of an intrusive nature (ECtHR, *Bărbulescu v. Romania* (61496/08) Grand Chamber 05/09/2017, para 121). As national courts did not evaluate all these factors the Grand Chamber by 11 votes to 6 decided that the State has violated its positive obligations under Article 8 as domestic authorities did not afford adequate protection of the applicant's right to respect for his private life and correspondence and consequently failed to strike a fair balance between the interests at stake. This judgment in fact raises a concern about the consistency of the Court's approach to workplace privacy. The “reasonable expectation of privacy” traditionally used by the Court to determine if there had been an interference with the right to private life was not attached any weight in the present case. The GC stated that “it is open to question whether – and if so, to what extent – the employer's restrictive regulations left the applicant with a reasonable expectation of privacy” (*ibid.*, para. 80) and went on establishing factors relevant for the evaluation of the case under Article 8. Even if these factors are of undisputable value for the national courts they should be assessed after the conclusion on the reasonable expectation of privacy. The Grand Chamber missed this stage, while the dissenting 6 judges did not and came to the opposite conclusion (Joint dissenting opinion of Judges Raimondi, Dedov, Kjølbros, Mits, Mourou-Vikström and Eicke. ECtHR, *Bărbulescu v. Romania* (61496/08) Grand Chamber 05/09/2017).

³⁷ ECtHR, *Niemitz v. Germany* (13710/88) 16/12/1992, para. 31.

³⁸ ECtHR, *Malone v. the United Kingdom* (8691/79) 02/08/1984, para. 68.

required that the law in question be accessible to the individual concerned; moreover, the individual should be able to foresee the consequences of those laws for him or herself.³⁹

In four cases lodged by public servants, the ECtHR found that there had been a lack of provisions aimed at protecting employees against interferences with their rights to respect for private life and correspondence. Accordingly, in all 4 cases the ECtHR found the violation of Article 8.⁴⁰

In *Köpke v. Germany*, the ECtHR implied that a legal framework must be proportionate to the severity of the threat to human rights; more serious threats required more serious safeguards.⁴¹ It found that as covert video surveillance at the workplace on suspicions of theft did not affect essential aspects of private life, the requirement of lawfulness could be satisfied by reference to the jurisprudence of the German Federal Labour Court. That jurisprudence elaborated important limits on the admissibility of such video surveillance, safeguarding employees' privacy rights against arbitrary interference by domestic courts.

In *M.M. v. UK*⁴², the ECtHR, taking into account the seriousness of the interference with applicant's private life, conducted a particularly rigorous analysis of the safeguards in the system by which criminal records were retained and could be disclosed. This case is a remarkable example of the application of severe qualitative requirements to the relevant provisions. The applicant was cautioned for kidnapping her grand-son in 2000; this information had to be retained for 5 years but was later extended to her life-span according to changes in practice of the Police Service in Northern Ireland. In 2006, the applicant was offered employment as a Health Care Family Support Worker, subject to vetting. She was asked to disclose details of prior convictions and cautions. She accordingly disclosed information about her actions in 2000, as well as the fact that she had been cautioned for the incident. As was required by the form she was asked to complete, she also consented to being the su-

³⁹ ECtHR, *Madsen v. Denmark* (58341/00) inadmissible 07/11/2002.

⁴⁰ ECtHR, *Halford v. the United Kingdom* (20605/92) 25/06/1997, para. 44; *Copland v. the United Kingdom*, para. 48; *Peev v. Bulgaria* (64209/01) 26/07/2007, para. 44; *Radu v. Moldova* (50073/07) 15/04/2014, para. 29-32.

⁴¹ Lavrysen, L., *Protection by the Law: The Positive Obligation to Develop a Legal Framework to Adequately Protect ECHR Rights*, in: Haeck, Y.; Brems, E. (eds.), *Human Rights and Civil Liberties in the 21st Century*, Dordrecht, Springer Science & Business Media, 2013, p. 96.

⁴² ECtHR, *M.M. v. the United Kingdom* (24029/07) 13/11/2012, para 198.

ject of a criminal record check. Her potential employer obtained the criminal record check and withdrew the offer of employment, taking into account the caution for child abduction. The applicant argued that retention of the caution data engaged her right to respect for her private life because it had affected her ability to secure employment in her chosen field.

The ECtHR established that there were no relevant domestic statutory provisions on the retention and disclosure of cautions. The recording of cautions in Northern Ireland was made under the police's common law powers to retain and use information for police purposes. The ECtHR noted that both the recording and, at least, the initial retention of all relevant data are intended to be automatic.⁴³ No distinction regarding how the information was to be stored, or how long it was required to be stored, was made based on the seriousness or the circumstances of the offence, the time which has elapsed since the offence was committed and whether the caution was spent.⁴⁴ The ECtHR highlighted the absence of clear legislative framework for the collection and storage of data, the lack of clarity as to the scope, extent and restrictions of the common law powers of the police to retain and disclose caution data, as well as the absence of any mechanism for independent review of a decision to retain or disclose data.

"The cumulative effect of these shortcomings" led the ECtHR to conclude that the retention and disclosure of the applicant's caution data in this instance could not be regarded as being in accordance with the law and therefore violated her rights under Article 8.⁴⁵ The ECtHR has thus set a high standard for provisions on retention and disclosure of police data, and underlined the need of flexibility in approach to relevant issues such that different circumstances can be taken into account accordingly. This case can be seen as a kind of development of the "Thlimmenos rule" to treat differently persons whose situations are significantly different.⁴⁶ It is interesting to note that the *M.M.* judgment led to the introduction of a filtering mechanism in Irish police data retention rules, so that old and minor cautions and convictions could no longer be automatically disclosed on a criminal record certificate. Since 2013, disclosure may only be made after taking into account the seriousness and age

⁴³ *Ibid.*

⁴⁴ *Ibid.*, para 204.

⁴⁵ *Ibid.*, para. 207.

⁴⁶ ECtHR, *Thlimmenos v. Greece* [GC] (No. 34369/97) 06/04/2000, para. 44. Similarly, ECtHR, *Pretty v. the United Kingdom* (2346/02) 29/04/2002, para. 88.

of the offence, the age of the offender and the number of offences committed by the person.⁴⁷

In *Radu v. Moldova*⁴⁸, which concerned a hospital's disclosure of medical information on request of the applicant's employer, the Police Academy, about the pregnancy of the applicant who was a lecturer, the ECtHR was not convinced that the State's reference to the domestic law on Access to Information justified the interference. It noted that this law had not been referred to by the Supreme Court of Justice, which had merely stated that the hospital was entitled to disclose the information to the applicant's employer, without citing any legal basis for such disclosure. The ECtHR emphasised that this law and all the relevant domestic and international laws expressly prohibited disclosure of such information and that in some jurisdictions, such disclosure even amounted to a *prima facie* criminal offence. Therefore the ECtHR concluded that the interference with the applicant's private life was not "in accordance with the law" and violated Article 8. Accordingly, there was no need for the ECtHR to go further and to examine whether the interference pursued a legitimate aim or was "necessary in a democratic society".

In certain cases, the ECtHR, having established the lack of relevant legislation in the respondent State's domestic legal systems, has been satisfied instead by existing employer's policies which themselves provide some privacy protection to its employees. For example, in cases of obligatory drug tests, such as in *Wretlung v. Sweden*⁴⁹, the ECtHR noted that the requirement of lawfulness in countries where labour issues were mainly regulated by the parties on the labour market can be satisfied by the establishment of relevant provisions in collective agreements or the employer's policy.⁵⁰ In this case, the applicant who worked as a cleaner at the nuclear plant claimed that the compulsory drug testing was in breach with Article 8 of the ECHR as an employee's refusal to undergo the tests could lead to his or her dismissal from the job. It is interesting to note that the central collective agreement in force did not provide for the conducting of any drug or alcohol tests on the employees by employers.

⁴⁷ Information about the execution of this judgment is available at official site of the CoE: http://www.coe.int/t/dghl/monitoring/execution/Reports/pendingCases_en.asp (accessed 20.05.2016).

⁴⁸ ECtHR, *Radu v. The Republic of Moldova* (50073/07) 15/04/2014.

⁴⁹ ECtHR, *Wretlung v. Sweden* (46210/99) inadmissible 09/03/2004.

⁵⁰ Similar conclusions can be found in ECtHR, *Madsen v. Denmark* (58341/00) inadmissible 07/11/2002.

On the other hand, the local collective agreement which introduced at the plant a drug policy programme, involving (*inter alia*) compulsory drug and alcohol tests, was not signed by the applicant's trade union. However, the employer subsequently issued a policy, containing the same obligations of all employees as did the local collective agreement which the applicant's trade union had not signed.⁵¹

The ECtHR did not, in this case, give weight to the refusal of applicant's trade union to sign the relevant provisions of collective agreement. It relied completely on the approach of the Swedish Labour Court which recognised the employer's right to manage and organise the work as a general legal principle. The right to carry out control measures was deduced from the right to manage and organise the work.

The ECtHR's broad approach to the perception of "lawfulness" in the context of interference with applicants' privacy provides countries with multiple possibilities in handling employee's privacy and facilitates the reconciliation of the employee's right to respect for private life and the management rights of the employer. The ECtHR's case law in this area demonstrates that the states, in order to comply with either positive or negative obligations under Article 8, have to do at least one of the following: introduce relevant legislation to protect employees' privacy; elaborate a particular approach of national courts to this issue; or to ensure the adoption of relevant policies or rules on the enterprise or local level.

4. EVALUATING THE NECESSITY OF THE INTERFERENCE IN DEMOCRATIC SOCIETY

Where the lawfulness of an interference has been established, the ECtHR will turn to an analysis of its necessity in a democratic society. This test enables the ECtHR to balance the rights concerned (usually the employee's privacy versus employer's right to manage the activities) taking into account the particular circumstances of the case.

Two similar cases discussed below concern data protection, in the context of the employer's ability to gather urine samples for drug and alcohol tests. The ECtHR's reasoning in these cases matters for Europe because, in the majority of European countries, there are no express provisions in relation to bodily privacy and approaches differ significantly between jurisdictions. In the

⁵¹ ECtHR, *Wretlund v. Sweden* (46210/99) inadmissible 09/03/2004.

United Kingdom, for example, work drug testing is increasing in importance:⁵² the Employment Practices Data Protection Code, issued by the Information Commissioner, states that testing for drugs and/or alcohol must be proportionate to the aim to be achieved and should only be carried out on workers whose drug or alcohol consumption would put at risk the safety of others.⁵³ In Italy, a Workplace Drug Testing (WDT) law took effect from 2008 and applied to workers involved in public/private transportation, oil/gas companies, and explosives/fireworks industry with the aim to ensure public safety for the community.⁵⁴ In Poland and the Czech Republic, workplace drug and alcohol testing is generally prohibited.⁵⁵

The ECtHR's approach to the necessity of conducting drug tests on employees could provide general guidelines for finding a balance between the employee's right to privacy and the employer's rights, and help members of the Council of Europe create a framework of protection based on the interpretation of the ECHR.

The fact scenarios in *Madsen v. Denmark*⁵⁶ and *Wretlund v. Sweden* (considered above) are quite similar. In both applications the employees argued that the obligatory testing system itself amounted to the violation of their right to respect for private life. In *Madsen* the applicant, a passenger assistant in a Danish shipping company, argued that employer's requirement for employees to pass random control measure (by means of providing a urine sample) violated Article 8.

In both cases, the ECtHR attached great weight to the legitimate aims of "public safety" and "the protection of the rights and freedoms of others". Both applicants argued that they were not directly responsible for the safety of the ship nor the nuclear plant respectively. The ECtHR pointed out in *Wretlund* that in cases of emergency the applicant could be required to perform tasks with importance for the safety of the plant. In *Madsen*, the ECtHR found that

⁵² Verstraete, A. G.; Pierce, A., *Workplace drug testing in Europe*, Forensic Science International, No. 121.1, 2001, pp. 2 – 6.

⁵³ Verstraete, A., *Workplace Drug Testing*, London, Pharmaceutical Press, 2011, p. 114.

⁵⁴ Kazanga, I., et al., *Prevalence of drug abuse among workers: Strengths and pitfalls of the recent Italian Workplace Drug Testing (WDT) legislation*, Forensic Science International, No. 215.1, 2012, pp. 46 – 50.

⁵⁵ Urban, D., *U.S. Drug-Testing Rules Do Not Translate Overseas*. Published 12.08.2014. Available at: www.shrm.org/hrdisciplines/global/articles/pages/us-drug-testing-rules.aspx (accessed 30.05.2016).

⁵⁶ ECtHR, *Madsen v. Denmark* (58341/00) inadmissible 07/11/2002.

all crew members on board were part of the safety crew and had to be able to perform functions related to the safety on board at any time. The Court also noted that domestic courts had found the use of drugs by other employees of the Shipping company. Therefore a legitimate aim had been established in each of the cases.

Examining the proportionality of interference, the ECtHR took into account the following circumstances, as established by the national courts:

- Employees were appropriately informed about the possibility of such tests being conducted;
- The frequency of tests (once a year in *Madsen* and once in three years in *Wredlund*);
- Advance notice (In *Wredlund* employees were notified about a week in advance of the test; employees were not notified in advance in *Madsen*);
- Coverage of all employees without any exception;
- The way of testing and any further use of obtained data (in both cases, testing had to be performed in private and the results were disclosed only to persons involved in the drug policy for the purpose of detecting the employees' possible consumption of alcohol and drugs).

An examination of the factors set out above led the ECtHR to conclude that the assumed interferences were, in these instances, justifiable on the basis that they were necessary in a democratic society, and declared each of the applications as being manifestly ill-founded. These decisions were criticised for the application of proportionality test in the same way as national courts do.⁵⁷ However, this point is an advantage of the ECtHR's review as it demonstrates to the countries, where the proportionality test is not applied, a valuable tool for adjudication of disputes on employee's privacy.

In *Leander v. Sweden*, the ECtHR touched upon an important facet of informational privacy – the right to access one's personal information. Mr Leander complained that he had been prevented from obtaining permanent employment and had been dismissed from provisional employment on account of certain secret information held by the terminating employer, which allegedly named him as a security risk. The information related to his security risk assessment had not been disclosed to him. Mr Leander complained that he

⁵⁷ Mouly, J.; Marguénaud, J.-P., *L'alcool et la drogue dans les éprouvettes de la CEDH: vie privée du salarié et principe de proportionnalité*, Recueil Dalloz Sirey: hebdomadaire, No. 1, 2005, p. 36.

should have been provided with the information in question. The application was lodged under Articles 8, 10 and 13 of the ECHR. The jurisprudence of the ECtHR demonstrates that applicants are more successful in seeking access to their data (as stored by the public sector)⁵⁸ when they combine their right to receive information, set out in Article 10, with a demonstrated connection that failure to receive the information about themselves allegedly interferes with their right to respect for private or family life as set out in Article 8.⁵⁹

In *Leander* the ECtHR established the necessity of collecting personal information and the fact that it was stored in registers not accessible to the public. In addition, the information was only used for the purpose of assessing the suitability of candidates for employment in posts important to national security. It stated that the lack of communication of the information in question could not by itself warrant the conclusion that the interference was not “necessary in a democratic society in the interests of national security”, as non-communication was aimed at the efficacy of the personnel control procedure. The ECtHR did not explain how the communication of information could influence the personnel control procedure and proceeded with answering the question of whether the Swedish personnel control system provided the applicant with necessary safeguards in order to meet the requirements of Article 8-2, concluding that the State did not violate Article 8. Considering the case in light of Article 10, the ECtHR observed that the right to freedom to receive information does not provide a right of access to a register containing information on the applicant’s personal position, nor does it embody an obligation on the State to impart such information to the individual.⁶⁰

⁵⁸ There are opinions that a positive obligation to provide information could be deduced from Article 10 only in theory, see Hins, W.; Voorhoof, D., *Access to state-held information as a fundamental right under the European Convention on Human Rights*, European Constitutional Law Review, Vol. 3, No 1, 2007, pp. 114 – 126. Available at: <http://www.coe.int/t/dghl/standardsetting/media/ConfAntiTerrorism/HinsVoorhoofBackground.pdf> (accessed 30.05.2016).

⁵⁹ See ECtHR, *Leander v. Sweden* (9248/81) 26/03/1987, *Gaskin v. the United Kingdom* (10454/83) 07/07/1989, *Guerra and others v. Italy* (14967/89) 19/02/1998.

⁶⁰ In later cases the ECtHR was less rigorous and clarified that if a secret service file was used to justify restrictive measures against an individual, it must contain information making it possible to verify whether the secret surveillance measures taken were lawfully ordered and executed or not. Cited from Boehm, F., *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Berlin-Heidelberg, Springer Science & Business Media, 2011, pp. 78 – 79. See, for example, ECtHR, *C.G. and others v. Bulgaria* (1365/07) 24/04/2008.

In such situations, when public security outweighs the applicant's right to respect for private life, the existence of an effective remedy in case of an interference occurring becomes particularly important. However, the ECtHR by 4 votes to 3 found that "the aggregate of the remedies" (the control procedure by the National Police Board, the control by the Chancellor of Justice and the Parliamentary Ombudsman and the possibility of making an appeal to the Government) satisfied "the conditions of Article 13 in the particular circumstances of the case" even in the absence of the impartial and independent court. Judges Pettiti and Russo noted in their Partially Dissenting Opinion that an independent authority should be able to determine the merits of an entry in the register and even whether there has been a straightforward clerical error or mistake of identity - in which case the national-security argument would fail. The dissenting judges in this case emphasised that the State could not be the sole judge in its own cause in this sensitive area of human-rights protection and held that there had been a breach of Article 13.

This case had a very interesting follow up which demonstrated that the dissenting judges were right. The applicant obtained access to the materials in question in 1997. He found out that his having been categorised as a security risk was based solely on the grounds of his belonging to the movement against the Vietnam War. Therefore, the State had, at the time of the case being adjudicated, completely misled the Commission and the ECtHR.⁶¹

On 27 November 1997, the Swedish Government made an official statement that there was not, in 1979 nor then, any grounds on which to label Mr Leander a security risk; that it was wrong that he was dismissed from his job as a carpenter at the museum; and, as compensation for the unjust infringement of his rights, awarded him compensation of 400,000 Swedish crowns.⁶²

Leander story demonstrates that the ECtHR has to be more cautious with concluding that the lack of communication of the information cannot by itself warrant the conclusion that an interference was necessary in a democratic society. This case emphasizes the importance of a more detailed analysis of the necessity of interference. It also highlights the need to have impartial reviews of similar applications by independent bodies, such as the Supreme Adminis-

⁶¹ *The Leander case: challenge to European court decision*, Statewatch: monitoring the state and civil liberties in the UK and Europe, Vol. 7, No. 6, 1997. Available at: <http://www.statewatch.org/subscriber/protected/sw7n6.pdf> (accessed 30.05.2016).

⁶² *Ibid.*

trative Courts in Belgium, France and Italy.⁶³ Control over the processing of personal data has in fact become “a precondition for the effective protection of other civil, social and political rights”⁶⁴, and labour rights in particular. The ECtHR’s approach to this subject is crucial because of its influence on national courts. For example, the Constitutional Court of Latvia viewed the denial of access to an investigation file, in the case of dismissal of a public servant, as a restriction on the right to respect for private life and justified such an interference with the reference to the Leander judgement.⁶⁵

5. POSITIVE OBLIGATIONS OF THE STATES

The majority of cases considered in this section concerned employees hired by the states. In these judgments and decisions the ECtHR outlines in some detail the acceptable scope of state interference with its employee’s privacy. The establishment of the state’s positive obligations in the sphere of privacy protection is especially valuable for the development of relevant national policies.

The ECtHR’s approach to the positive duties of the states can be summarised as imposing an obligation to adopt regulations (the duty to regulate) and to provide for their effective implementation (the duty to act).

5.1. The duty to regulate

The ECtHR’s requirements as to the quality of a state’s legal framework dealing with privacy protection can be understood as requiring the State to adopt regulations of employee’s privacy protection either by introducing relevant legislation or through case law, soft law or employer’s regulations. The choice of those methods is left to the states. However, the Court has implied that a more intrusive interference should be regulated by law.⁶⁶

⁶³ As pointed out by Dissenting Judges Pettiti and Russo in their Partially Dissenting Opinion in *Leander v. Sweden* (9248/81) 26/03/1987.

⁶⁴ Resta, R., *Dignità, persone, mercati*, Torino, Giappichelli Editore, 2014, p. 156.

⁶⁵ See ECtHR, *Ternovskis v. Latvia* (33637/02) 29/04/2014, para. 26. It is interesting to note that in this case the lack of access to secret files was one of the submissions which led the Court to conclude the violation of the right to fair trial (see para. 72, 74).

⁶⁶ See ECtHR, *Köpke v. Germany* (420/07) 05/10/2010, *M.M. v. the United Kingdom* (24029/07) 13/11/2012.

The State should ensure that in case of conflict between the rights of an employee and those of the employer, a proper balancing exercise taking all relevant circumstances into consideration should be undertaken.⁶⁷

The general quality requirement to these regulations was formulated in the *Malone* case⁶⁸ as precision, certainty, and foreseeability. In *M.M. v. UK* the ECtHR went further and said that States needed to ensure there were clear, detailed rules governing the scope and application of measures interfering with the right to respect for private life and providing minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrary use.⁶⁹ In respect of data protection the ECtHR emphasised that appropriate and adequate safeguards which reflect the principles elaborated in applicable data protection instruments and prevent arbitrary and disproportionate interference with Article 8 rights must be ensured at each stage of data processing.⁷⁰

5.2. Duty to act

As far as the informational privacy of public employees is concerned, the State has a positive duty under Article 8 to implement effective methods of data protection. This facet of privacy protection was developed by the ECtHR in *I. v. Finland*.⁷¹ The applicant worked on fixed-term contracts as a nurse in the polyclinic for eye diseases in a public hospital; being HIV-positive she herself attended the polyclinic for infectious diseases at the same hospital as a patient as well. At that time, hospital staff had unfettered access to the patient register which contained information on patients' diagnoses and their treating doctors. The applicant's colleagues thus became aware of her disease. Upon her request, the hospital's register was amended so that only the treating

⁶⁷ See, for instance, *Köpke v. Germany* (420/07) 05/10/2010, or *Madsen v. Denmark* (58341/00) 07/11/2002, *Wretlund v. Sweden* (46210/99) inadmissible 09/03/2004.

⁶⁸ ECtHR, *Malone v. the United Kingdom* (8691/79) 02/08/1984.

⁶⁹ ECtHR, *M.M. v. the United Kingdom* (24029/07) 13/11/2012, para. 195.

⁷⁰ ECtHR, *M.M. v. the United Kingdom* (24029/07) 13/11/2012.

⁷¹ ECtHR, *I. v. Finland* (20511/03) 17/07/2008, see also Jari, R., *European Court of Human Rights: Failure to take effective information security measures to protect sensitive personal data violates right to privacy – I v. Finland*, *Computer Law & Security Review*, Vol. 24, No. 6, 2008, pp. 562 – 564.

clinic's personnel had access to its patients' records. The applicant complained before the ECtHR that there had been a failure on the part of the hospital to guarantee the security of her data against unauthorised access, or, in ECHR terms, a breach of the State's positive obligation to secure respect for her private life by means of a system of data protection rules and safeguards.⁷² The ECtHR noted that the mere fact that the domestic legislation provided the applicant with an opportunity to claim compensation for damages caused by an alleged unlawful disclosure of personal data was not sufficient to protect her private life. The State had to provide the practical and effective protection to exclude any possibility of unauthorised access to her personal data stored by her employer.⁷³

The judgment was met by scholars with much enthusiasm. Certain scholars supposed that as a result of the *I. v. Finland* judgement, signatory states to the ECHR could be found liable for failing to ensure that private parties had taken positive steps to prevent privacy violations by other private parties.⁷⁴ This opinion seems too optimistic at first glance; however, it might become true once applications by private employees are lodged claiming shortcomings in the State's control over employee privacy protection.

To conclude this paragraph, it is necessary to note that the elaboration of the states' positive duties is particularly important for the countries of the former Soviet Union, in particular, for Russia, where the right to privacy was only recently introduced to the legislation. One leading Russian labour scholar noted that, as nothing could be "private" in the Soviet Union, the idea of privacy did not penetrate easily into the citizens' consciousness nor the State's legal system.⁷⁵ The Court's conclusions on the states' duties in the field of privacy protection might be referred to in a national proceeding in Russia, even though they were not formulated in cases against Russia, in order to demonstrate the

⁷² ECtHR, *I. v. Finland* (20511/03) 17/07/2008, para. 37.

⁷³ *Ibid.*, para. 47.

⁷⁴ Purtova, N., *Private law solutions in European data protection: Relationship to privacy, and waiver of data protection rights*, Netherlands Quarterly of Human Rights, No. 28, 2010, p. 179. Available at: https://pure.uvt.nl/portal/files/1247976/purtova_private_law_solutions_in_european_data_protection_100712.pdf (accessed 25.05.2016).

⁷⁵ Lushnikov, A., *Protection of employee's personal data: comparative and legal comments of chapter 14 of the Russian Labour Code* [Zashchita Personal'nykh Dannykh Rabotnika: Sravnitel'no-Pravovoy Kommentariy Gl.14 Trudovogo Kodeksa Rf], Upravlenie personalom, No. 17, 2009. Available at: <http://www.top-personal.ru/issue.html?2150> (accessed 20.05.2016).

courts that Article 8 of the ECHR is applicable in cases of employees' privacy protection and imposes certain obligations on the state and on courts.

6. CONCLUSIONS

The research of the ECtHR's jurisprudence under Article 8 demonstrates that the Court has created the basis for the protection of employees' privacy, and indisputably acknowledged a link between private life and employment. This acknowledgment "can shield an individual employee against employer domination".⁷⁶ It is also very beneficial for the countries of the former Soviet Union, which have intrinsic difficulties with privacy protection. The ECtHR's legal positions on protection of an employee's privacy (both in respect of data protection and protection from interference with his private life at the workplace) might serve as a kind of vector for the development of relevant national legislations and case law.

It is important to note that the judgments considered in this paper contributed not only to the protection of the rights of the applicants, but forced the States to adopt certain changes into their national labour law, enhancing the level of protection of the right to respect for private life at the workplace. The Court underlined the need to elaborate a clear legislative framework for the collection and storage of personal data, and for the protection of employees' privacy at the workplace. In addition, the ECtHR provided domestic courts with the framework to determine the violation of this right.

BIBLIOGRAPHY

ARTICLES

Arnaud, S., *Analyse économique du droit au respect de la vie personnelle: application à la relation de travail en France*, *Revue internationale de droit économique*, Vol. XXI, No. 2, 2007, pp. 129 – 156.

Hins, W.; Voorhoof, D., *Access to state-held information as a fundamental right under the European Convention on Human Rights*, *European Constitutional Law Review*, Vol. 3, No 1, 2007, pp. 114 – 126.

⁷⁶ Mantouvalou, V., *Human Rights and Unfair Dismissal: Private Acts in Public Spaces*, *The Modern Law Review*, Vol. 71, No. 6, 2008, p. 939.

- Jari, R., *European Court of Human Rights: Failure to take effective information security measures to protect sensitive personal data violates right to privacy – I v. Finland*, *Computer Law & Security Review*, Vol. 24, No. 6, 2008, pp. 562 – 564.
- Kazanga, I., et al., *Prevalence of drug abuse among workers: Strengths and pitfalls of the recent Italian Workplace Drug Testing (WDT) legislation*, *Forensic Science International*, No. 215.1, 2012, pp. 46 – 50.
- Lushnikov, A., *Protection of employee's personal data: comparative and legal comments of chapter 14 of the Russian Labour Code [Zashchita Personal'nykh Dan-nykh Rabotnika: Sravnitel'no-Pravovoy Kommentariy Gl.14 Trudovogo Kodeksa Rf]*, *Upravlenie personalom*, No. 17, 2009, pp. 12 – 17.
- Mantouvalou, V., *Human Rights and Unfair Dismissal: Private Acts in Public Spaces*, *The Modern Law Review*, Vol. 71, No. 6, 2008, pp. 912 – 939.
- Mouly, J.; Marguénaud, J.-P., *L'alcool et la drogue dans les éprouvettes de la CEDH: vie privée du salarié et principe de proportionnalité*, *Recueil Dalloz Sirey: hebdomadaire*, No. 1, 2005, p. 36.
- Purtova, N., *Private law solutions in European data protection: Relationship to privacy, and waiver of data protection rights*, *Netherlands Quarterly of Human Rights*, No. 28, 2010, pp. 179 – 198.
- Urban D., *U.S. Drug-Testing Rules Do Not Translate Overseas*. Published 12.08.2014. Available at: www.shrm.org/hrdisciplines/global/articles/pages/us-drug-testing-rules.aspx (accessed 30.05.2016).
- Van der Sloot, B., *Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"*, *Utrecht Journal of International and European Law*, Vol. 31, No. 80, 2005, pp. 25 – 50.
- Verstraete, A. G.; Pierce, A., *Workplace drug testing in Europe*, *Forensic Science International*, No. 121.1, 2001, pp. 2 – 6.
- Warren, S. D.; Brandeis, L. D., *The Right to Privacy*, *Harvard Law Review*, Vol. 4, No. 5, 1890, pp. 193 – 220.
- Zykina, T. A., *The right of employees to private life protection [Pravo rabotnika na neprikosnovennost' lichnoy (chastnoy) zhizni]*, *Pravovedeniye*, No. 1, 2007, pp. 81 – 87.

BOOKS AND CHAPTERS

- Boehm, F., *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-level*. Berlin-Heidelberg, Springer Science & Business Media, 2011.
- Hendrickx, F.; Van Bever, A., *Article 8 ECHR: judicial patterns of employment privacy protection*. In: Dorssemont F.; Lörcher, K.; Schömann, I. (eds.), *The European Convention on Human Rights and the Employment Relation*. Oxford, Hart Publishing, 2013, pp. 183 – 208.
- Lavrysen, L., *Protection by the Law: The Positive Obligation to Develop a Legal Framework to Adequately Protect ECHR Rights*. In: Haeck, Y.; Brems, E. (eds.), *Human Rights and Civil Liberties in the 21st Century*. Dordrecht, Springer Science & Business Media, 2013, pp. 69 – 129.
- Löhmus, K., *Caring Autonomy: European Human Rights Law and the Challenge of Individualism*. Cambridge, Cambridge University Press, 2015.
- Pagallo, U., *La tutela della privacy negli Stati Uniti d'America e in Europa: modelli giuridici a confronto*. Milano, Giuffrè Editore, 2008.
- Resta, R., *Dignità, persone, mercati*. Torino, Giappichelli Editore, 2014.
- Ryssdal, R., *Data Protection and the European Convention on Human Rights*. In: *Data Protection, Human Rights and Democratic Values, Proceedings of the 13th Conference of Data Protection Commissioners held 2–4 October 1991 in Strasbourg*. Strasbourg, CoE, 1992, pp. 42 – 49.
- Verstraete, A., *Workplace Drug Testing*. London, Pharmaceutical Press, 2011.

Sažetak

Izv. prof. dr. sc. Elena Sychenko *

**MEĐUNARODNOPRAVNA ZAŠTITA PRIVATNOSTI RADNIKA
PREMA EUROPSKOJ KONVENCIJI ZA ZAŠTITU LJUDSKIH
PRAVA I TEMELJNIH SLOBODA**

Među različitim nacionalnim pristupima problemu zaštite privatnosti radnika na radnom mjestu sudska praksa Europskog suda za ljudska prava (ESLJP) pruža neprocjenjiv okvir za razmatranje slučajeva koji se odnose na privatnost radnika. Iako ESLJP nije upotrebljavao pojam "privatnost", njegovo široko tumačenje prava na zaštitu privatnog života znatno je pridonijelo zaštiti osobnih podataka razrađujući pozitivne obveze država. U članku se analizira kako je prilagođenom primjenom odredaba Europske konvencije za zaštitu temeljnih ljudskih prava i sloboda ostvarena zaštita osobnih podataka radnika, ograničen neovlašteni videonadzor, prisluškivanje telefonskih razgovora na radnom mjestu te je posebno obrađen recentni slučaj Bărbulescu protiv Rumunjske. Naglasak u radu stavljen je na pristup ESLJP-a pitanjima zakonitosti i nužnosti prilikom narušavanja privatnosti radnika s obzirom na posebnu važnost koju judikatura ESLJP-a ima u članicama Vijeća Europe.

Ključne riječi: privatnost, zaposlenje, Europski sud za ljudska prava, zaštita podataka, razumno očekivanje privatnosti

* Dr. sc. Elena Sychenko, izvanredna profesorica Pravnog fakulteta Državnog sveučilišta u Sankt Petersburgu, ul. K. Marksa, d. 36a, kv. 21, Gatchina, Lenjingradska regija, Ruska Federacija; e.sychenko@mail.ru;
ORCID ID: orcid.org/0000-0002-7045-9218

