SECTION 6.
HUMAN RIGHTS AND FUTURE LAW SCHOOL

YUDKIVSKA G. Y.

European Court of Human Rights,
Judge in respect of Ukraine

DOES RIGHT TO PRIVACY EXIST IN THE ERA OF TRANSPARENCY AND MASS SURVEILLANCE?

Key words*: right to be forgotten, fair balance, transparency.*

As technology develops, and the online world takes over the real world, our increasing online presence is becoming a defining feature of XXI century, with new challenges frequently emerging.

New informational space brought us new full transparency that is changing, first of all, an institute of reputation, which for a long time was outside human rights discourse.Quite paradoxically new informational technologies brought us back to traditional communities where everyone was in the public eye of the community, but now – on a new technological level. For example, they gave rise to a new right – the «right to be forgotten».

The «right to be forgotten» was prominently recognised by the Court of Justice of the European Union in the famous *Google Spain* in which the Court held that individuals had right to ask search engines to remove links containing personal data about them if the information about the individual is «inadequate, irrelevant or no longer relevant». The case was brought by a Spanish man Mr Gonzalez, who was involved in insolvency proceedings relating to social security debts in the late 1990s. These proceedings were reported in a regional newspaper in Spain in 1998 and the article was later made available online. Mr Gonzalez asked Google Spain to remove links to the newspaper in its search results when his name was entered as a search term in the Google search engine, arguing that the insolvency proceedings were concluded and it was no longer of relevance.

The CJEU accepted that a 'fair balance' must be struck between the rights to data protection and privacy on the one hand and the interest of the general public in having access to the information on the other [1], the Court also held that "as a rule" the privacy and data protection rights should prevail [2]. This judgment contains no reference to the Strasbourg Court's case-law and apparently provides for a different balancing exercise.

For the ECtHR, the right to freedom of expression applies not only to the content of information, but also to the means of transmission or reception, since any restriction imposed on the means necessarily interferes with the right to receive and impart information [3]. Thus, for example, if certain

online platforms are told not to show certain web pages on search results, this can amount to an interference with Article 10. Firstly, it can interfere with the publisher's ability to impart information and secondly it can interfere with the public's ability to receive information.The «right to be forgotten» might thus become a serious threat to free online speech in the coming years, unless a delicate balancing exercise is performed on a case by case basis to determine which right will be given greater weight.

The ECtHR's balancing exercise is well-known – in a number of cases, starting with the leading *Von Hannover* judgment, the Court has provided a list of factors to be taken into account:

(i) contribution to a debate of general interest;

(ii) how well-known is the person concerned and what is the subject of the report;

(iii) prior conduct of the person concerned;

(iv) method of obtaining the information and its veracity;

(v) content, form and consequences of the publication; and

(vi) severity of the sanction imposed [on the party claiming an interference with freedom of expression] [4], [5].

This balancing exercise is not easily reconcilable with the *Google Spain* judgment, according to which the rights to privacy and data protection «override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name». [1] It is also noteworthy that the CJEU referred to accessing information as an «interest» rather than as a fundamental right.

At the same time, according to the ECtHR's findings in its landmark judgment of *Magyar Helsinki Bizottság v. Hungary,*a right of access to information may arise in circumstances where access to the information is instrumental for the individual's exercise of his or her right to freedom of expression [6].

It is clear that the ECtHR does not prioritise the "right to be forgotten" without due consideration of the potential wider impact on freedom of expression – as was already proved by several recent cases where the Court engaged with the issues raised by the «right to be forgotten2 [7].

While it is true that the Internet poses new risks to data protection and privacy, this does not justify any downgrading of the fundamental right to freedom of expression.

Another challenge posed by new technologies is the fear of Big Brother who is watching you according to George Orwell, or omnipotent state.

The trigger for the case of *Big Brother Watch and others v. the United Kingdom* [8], pending now before the Grand chamber of the ECtHR, was the disclosure by Edward Snowden of electronic surveillance programs used by the United States and the United Kingdom for mass interception of communications, as well as the exchange of intercepted communications and communications between the two states.

More broadly, such cases concern both the rights to privacy and of freedom of speech for Internet users and mobile communication. Again,

internet has opened up the possibility of a dramatically shrinking sphere of personal privacy in which so many aspects of our lives become opened up to scrutiny and possible ongoing surveillance. When unrestricted, state observation can transform the achievements of civilization into a tool of unbelievable repression, and provide unprecedented opportunities to invade private life.

The concept of «reasonable expectation of privacy», widely used nowadays by the Strasbourg Court, is to be reconsidered. A person on the Internet might be said to have a more limited expectation of privacy, as was firstly recognised in the case of *Muscio v. Italy* [9] back in 2007. More recently, the concept was mentioned in the GC case of *Barbulescu v Romania* [10]. The case concerned the applicant's dismissal following the monitoring of his electronic communications, mainly through his Yahoo Messenger account, which the applicant was instructed to create for communicating with clients. It was found that he used the Internet for personal purposes during the working day, in violation of internal rules. The Court left open the question of whether the applicant had a reasonable expectation of privacy, notwithstanding the employer's clear instructions for abstaining from any personal activity in the workplace, because an «employer's instructions cannot reduce private social life in the workplace to zero».

In *Benedik v. Slovenia* [11], for the first time in order to address privacy issues the Court has gone into a study of the Internet Protocol and forms of IP addressing. In that case the applicant accessed the internet through a dynamic IP address (Unlike the static IP address, 'a dynamic IP address is assigned to a device by the Internet Service Provider temporarily, typically each time the device connects to the Internet, and therefore changes each time there is a new connection to the Internet). He had done so, as was established, for dissemination of child pornography, and police, without a court order, requested an Internet service provider to disclose data regarding a user to whom a dynamic (IP) address had been assigned at a particular time.The Court addressed the question of whether dynamic IP addresses fall within protection of Article 8 and gave a positive answer.

In *LópezRibalda and Others v. Spain* [12] the applicants complained of covert video surveillance of supermarket cashiers by employer who wanted to investigate economic losses. The employer installed surveillance cameras consisting of both visible, of which the applicants were given notice, and hidden cameras, of which they were not. The applicants were dismissed following video footage showing them stealing items.

The Court found that the covert video surveillance of an employee at his or her workplace must be considered, as such, as a considerable intrusion into his or her private life. It entails a recorded and reproducible documentation of a person's conduct at his or her workplace, which he or she, being obliged under the employment contract to perform the work in that place, cannot evade.

Since the legislation clearly established that every data collector had to inform the data subjects of the existence of a means of collecting and processing their personal data, aim and manner of covert video surveillance

was clearly regulated and protected by law, therefore the applicants had a reasonable expectation of privacy.

So, our privacy and its reasonable expectations should be sufficiently protected by law.

Any surveillance by itself is not a violation of human rights and the right to privacy in particular, it has to have a legal basis and be proportionate to the legitimate aim pursued in order to comply with the Convention. In particular, it must be the "least intrusive tool among those which can achieve the desired result." Yet while individual monitoring programs may seem necessary to achieve this legitimate purpose when taken separately, when they are analysed alongside other data sets which collect information for the same purpose, this analysis can reveal a great deal more and constitute a much greater interference with individual rights.

The nature of surveillance has changed. Previously, we were dealing with individual surveillance as seen in cases like *Khan v. UK*, *Bykov v. Russia*, *Allen v. UK* etc. – and exclusively within the context of criminal proceedings and admissibility of evidence against individuals. Today there is a shift from targeted to a mass surveillance. Previously we dealt with a deliberate decision to conduct surveillance in relation to a particular person; by contrast, metadata is typically collected automatically.

The case of *Roman Zakharov v. Russia* [13] is an excellent example of what safeguards the ECtHR could demand of Governments under such circumstances: the following minimum requirements should be set out in law in order to avoid abuses of power:

– the nature of offences which may give rise to an interception order;

– a definition of the categories of people liable to have their communications intercepted;

– a limit on the duration of interception;

– the procedure to be followed for examining, using and storing the data obtained;

– the precautions to be taken when communicating the data to other parties;

– the circumstances in which intercepted data may or must be erased or destroyed

– the arrangements for supervising the implementation of secret surveillance measures,

– any notification mechanisms and the remedies provided for by national law

The issues raised by the *Big Brother Watch and Others* case are novel ones. This case will give the Grand Chamber a fresh opportunity to conduct a comprehensive review of the Court's jurisprudence on the interception (both targeted and, of particular relevance, bulk interception) of communications and to refine the key principles for reconciling the use of surveillance measures and the protection of privacy.

Privacy protection is a crucial achievement in European political and legal culture, not least because it was formed against the backdrop of the horrors of the Nazi and communist regimes of the twentieth century. In the long run,

privacy will stand as a fundamental right so long as it is defended and valued by society, and it will disappear only if society permits it. Today, we have a reasonable expectation that our privacy is protected even when we go online. Our fundamental right to control how we present ourselves to the outside world and our ability to live our lives without constant scrutiny – these must be seen as vital for both the individual and also for a healthy society as a whole.

References:

1. *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* Case C-131/12 (13 May 2014) at [81].
2. Ibid at [99].
3. *Autronic AG v Switzerland* , no. 12726/87, § 47, 22 May 1990.
4. *Von Hannover v. Germany (no. 2)*[GC], nos. 40660/08 and 60641/08, § 108, ECHR 2012
5. *Satakunnan MarkkinapörssiOy and SatamediaOy v. Finland* [GC], no. 931/13, § 62, 27 June 2017.
6. *Magyar Helsinki Bizottság v. Hungary* [GC], no. 18030/11, § 156, ECHR 2016
7. See, for example, *Fuchsmann v. Germany*, no. 71233/13, 19 October 2017 and *M.L. and W.W. v. Germany,* nos. 60798/10 and 65599/10, 28 June 2018.
8. *Big Brother Watch and Others v. the United Kingdom* [GC], nos. 58170/13 and 2 others, 13 September 2018).
9. *Muscio v. Italy (dec.),* no. 31358/03, 13 November 2007.
10. *Bărbulescu v. Romania* [GC],, no. 61496/08, ECHR 2017
11. *Benedik v. Slovenia,* no.62357/14, 24 April 2018.
12. *LópezRibalda and Others v. Spain*, nos.1874/13 and 8567/13, 9 January 2018.
13. *Roman Zakharov v. Russia* [GC], no. 47143/06, ECHR 2015

ARAKELIAN M. R.

National University «Odesa Law Academy»,
Vice-Rector for Educational Work, Professor at the Department
of International and European Law, Doctor of Law, Professor

EU CHARTER OF FUNDAMENTAL RIGHTS: POLITICAL AND LEGAL ASSESSMENT

In the article the EU Charter of Fundamental Rights has been considered and received legal and political assessment in the framework of the European integration processes. Furthermore, it has been proved that the Charter played an important role in the process of the elaboration of standards of the human rights protection and represents a constitutional heritage for the whole European Union.

Key words: *EU Charter of fundamental rights, negative rights, positive rights, European Union, constitutional process.*