

Журнал
конституционализма
и прав человека



Journal of
Constitutionalism &
Human Rights

www.chr-centre.org

ISSN 2351-6283 online

2015 * 3-4(8)

Космополитическая демократия
и государство

«Роман Захаров против России»
большой брат под контролем?

Национальное измерение
Европейской Конвенции

Cosmopolitan Democracy
and the State

Roman Zakharov v. Russia:
Big Brother Under Control?

The National Dimension
of the European Convention



European Humanities University

Centre for Constitutionalism &
Human Rights



Journal of Constitutionalism & Human Rights

ISSN 2351-6283 online

2015 * 3-4(8)

Editorial Board

Published with the financial support
of the Council of Europe

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Maxim Timofeev * Editor-in-Chief

**Gleb Bogush, Oleg Bresky,
Anton Burkov, Sergey Golubok,
Neda Mullalli, Anita Soboleva,
Aleksander Vashkevich, Maria Voskobitova,
Liudmila Uliashina** * Editors
Oleg Malevich * Technical Editor

Editorial Council

Address of the Publisher:
European Humanities University
Tauro st. 12, LT-01114
Vilnius Lithuania

Editorial Address:
journaljchr@gmail.com

Published by the Center for
Constitutionalism & Human Rights,
European Humanities University

<http://www.chr-centre.org>

Anatoly Kovler * former Judge of the European Court of Human Rights

Ganna Yudkivska * Judge of the European Court of Human Rights

Toma Birmontiene * Judge of the Constitutional Court of Lithuania

Michael Krasnov * Prof., Head of Constitutional Law Department, Higher School of Economics, Russia

Gulnara Useinova * Prof., Head of Constitutional Law Department, Al-Farabi Kazakh National University, Kazakhstan

Bill Bowring * Barrister, Director of the LLM / MA in Human Rights School of Law, Birkbeck, University of London

Oleksiy Kresin * Cand. Legal Sci., Head of the Center of Law and Comparative Legal Studies, Institute of State and Law of the National Academy of Science of Ukraine

Karina Moskalenko * Founder of the International Protection Centre, Russia





Журнал конституционализма и прав человека

ISSN 2351-6283 online

2015 * 3-4(8)

Редакционная коллегия

Публикуется при финансовой
поддержке Совета Европы
COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Максим Тимофеев * главный редактор

**Глеб Богуш, Олег Бреский,
Антон Бурков, Александр Вашкевич,
Мария Воскобитова, Сергей Голубок,
Неада Муллалли, Анита Соболева,
Людмила Ульяшина** * редакторы
Олег Малевич * технический редактор

Редакционный совет

Адрес издателя:
Европейский гуманитарный
университет
Tauro st. 12, LT-01114
Vilnius Lithuania

Адрес редколлегии:
journaljchr@gmail.com

Публикуется Центром
конституционализма и прав
человека Европейского
гуманитарного университета

<http://www.chr-centre.org>

Анатолий Ковлер * судья Европейского Суда
по правам человека в отставке

Анна Юдковская * судья Европейского Суда
по правам человека

Тома Бирмонтиене * судья Конституционного суда Литвы

Михаил Краснов * проф., заведующий кафедрой
конституционного и муниципального права,
НИУ Высшая школа экономики, Россия

Гульнара Усейнова * проф., заведующая кафедрой
конституционного и административного права,
Казахский национальный университет, Казахстан

Билл Бауринг * проф., школа права колледжа Биркбек,
Лондонский университет

Алексей Кресин * к.ю.н., руководитель центра
сравнительного правоведения,

Институт государства и права НАН Украины

Каринна Москаленко * основатель Центра содействия
международной защите, Россия



<p>ОТ РЕДАКЦИИ • EDITORIAL NOTE</p>	<p>МАКСИМ ТИМОФЕЕВ • MAXIM TIMOFEEV</p> <p style="text-align: right;">6</p>
<p>ДОКТРИНА • DOCTRINE</p>	<p>ASGER SØRENSEN Cosmopolitan Democracy and the State: Reflections on the Need for Ideals and Imagination</p> <p>• АСГЕР СЁРЕНСЕН Космополитическая демократия и государство: размышления о необходимости идеалов и воображения</p> <p style="text-align: right;">8</p>
<p>ПЕРЕДОВАЯ • FRONTLINE</p>	<p>SERGEY GOLUBOK Roman Zakharov v. Russia: Big Brother Under Control?</p> <p>• СЕРГЕЙ ГОЛУБОК «Роман Захаров против России»: большой брат под контролем?</p> <p style="text-align: right;">20</p>
<p>НАЦИОНАЛЬНОЕ ИЗМЕРЕНИЕ ЕВРОПЕЙСКОЙ КОНВЕНЦИИ • NATIONAL DIMENSION OF THE EUROPEAN CONVENTION</p>	<p>АНТОН БУРКОВ От редактора рубрики</p> <p>• ANTON BURKOV Editorial Remarks</p> <p style="text-align: right;">27</p>
	<p>СИМОН ГАБОРЬЮ Конвенция о защите прав человека и основных свобод и серьезные изменения в сфере уголовной юстиции Франции</p> <p>• SIMONE GABORIAU European Convention on Human Rights and Major Changes in the Sphere of French Criminal Justice</p> <p style="text-align: right;">29</p>
	<p>ТИМОТИ ПАРИС Европейская Конвенция и французский административный суд: от международного права к национальному праву?</p> <p>• TIMOTHÉE PARIS French Administrative Court and the European Convention on Human Rights: From International Law to National Law?</p> <p style="text-align: right;">39</p>

<p>ПРАВА ЧЕЛОВЕКА И МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ</p> <ul style="list-style-type: none"> • HUMAN RIGHTS AND INTERNATIONAL RELATIONS 	<p>MOGENS CHROM JACOBSEN The Internationalisation of the Universal Declaration of Human Rights</p> <p>47</p> <ul style="list-style-type: none"> • МОГЕНС ХРОМ ЯКОБСЕН Интернационализация Всеобщей декларации прав человека
<p>КОНСТИТУЦИОНАЛИЗМ И СУДЕБНЫЙ КОНТРОЛЬ</p> <ul style="list-style-type: none"> • CONSTITUTIONALISM AND JUDICIAL REVIEW 	<p>DMITRY KURNOSOV Judicial Standard of Fair Representation in a Proportional Electoral System: The Case of Russia</p> <p>71</p> <ul style="list-style-type: none"> • ДМИТРИЙ КУРНОСОВ Правовой стандарт равного представительства в пропорциональной избирательной системе: пример России
	<p>DEBJYOTI GHOSH The Categorical Other: Going Beyond the Gender Binary in Law in India</p> <p>86</p> <ul style="list-style-type: none"> • ДЕБЖЙОТИ ГОШ Иная категория: преодоление гендерной бинарности в праве в Индии
<p>ПРАВА ЧЕЛОВЕКА И УГОЛОВНОЕ ПРАВОСУДИЕ</p> <ul style="list-style-type: none"> • HUMAN RIGHTS AND CRIMINAL JUSTICE 	<p>ДМИТРИЙ ДУБРОВСКИЙ The Internationalisation of the Universal Declaration of Human Rights</p> <p>104</p> <ul style="list-style-type: none"> • DMITRY DUBROVSKY Expert Witness's Opinion in Hate Speech Cases in Russia: A Dispute Over Methods

ПЕРЕДОВАЯ FRONTLINE



Sergey Golubok

LL.M. in International Human Rights Law, University of Essex (United Kingdom), Ph.D., St. Petersburg University (Russia), Attorney at Double Bridge Law¹

Email: sgolubok@gmail.com

Roman Zakharov v. Russia: Big Brother Under Control?

Abstract

On 4 December 2015 Grand Chamber of the European Court of Human Rights rendered its unanimous judgment in *Roman Zakharov v. Russia*. This is a new step in development of international human rights standards vis-à-vis massive surveillance techniques used by many States worldwide. The author draws our attention to the threats of mass surveillance in a digital era, deficiencies of the human rights mechanisms in this regard, and concludes that *Roman Zakharov* sets the agenda for a vast area of human rights litigation in the future. What visible today is only general contours of this area; digital frontier poses sets after sets of exciting questions that lawyers should start answering.

Keywords: European Court of Human Rights, right to respect for private life, secret surveillance.

«Роман Захаров против России»: большой брат под контролем?

Аннотация

4 декабря 2015 года Большая Палата Европейского Суда по правам человека вынесла единогласное постановление по делу «Роман Захаров против России». Это, безусловно, новый шаг в развитии стандартов международного права прав человека, касающихся технологий широкомасштабного надзора, используемых многими государствами во всем мире. Автор привлекает наше внимание к угрозам систем массового надзора в эпоху цифровых технологий, а также недостаткам механизмов защиты прав человека в этой области и приходит к выводу, что постановление по делу Романа Захарова открывает огромное поле возможностей для судебной деятельности в защиту прав человека. Сегодня видны только общие контуры этой области; цифровая действительность ставит захватывающие вопросы, на которые юристы должны начать давать ответы.

Ключевые слова: Европейский Суд по правам человека, право на уважение частной жизни, тайный надзор.

¹ Сергей Голубок, магистр международного права прав человека (Университет Эссекса, Великобритания), кандидат юридических наук (Санкт-Петербургский государственный университет), адвокат, «Double Bridge Law».

ROMAN ZAKHAROV V. RUSSIA: BIG BROTHER UNDER CONTROL?

On 4 December 2015 Grand Chamber of the European Court of Human Rights (hereinafter, also the Court) rendered its unanimous judgment in *Roman Zakharov v. Russia*.¹ This is a new step in development of international human rights standards vis-à-vis massive surveillance techniques used by many States worldwide.

Article 8 of the European Convention on Human Rights provides “everyone” with “the right to respect for his [or her] private and family life, his [or her] home and his [or her] correspondence”.²

Back in 1978 the Court accepted that “the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications [was], under exceptional circumstances, necessary in a democratic society”. However, “being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it” the Court was wise to affirm that States “may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate”.³ The Court “must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse”.⁴

The Court developed this approach in a line of cases concerning interception by the authorities of various communications, including phone conversations and letters. That case-law focused on the grounds and procedure for authorization to intercept communications, in particular, in the framework of criminal proceedings. The Court reiterated that “[i]n the context of covert measures of surveillance, the law must be sufficiently clear in its terms to give citizens an adequate indication of the con-

ditions and circumstances in which the authorities [were] empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence”.⁵

The Court’s approach was based on the assumption that authorities would identify certain individuals or groups of communications between them for surveillance. Therefore, it was necessary to ensure that authorization procedure provides “adequate and effective guarantees against abuse”. Normally, it is for independent courts to authorize surveillance.

However, the Court has always been aware that “the technology available for use is continually becoming more sophisticated”.⁶ In 2013 the Snowden revelations of the scope and magnitude of electronic surveillance programs run by the United States and their partners made headlines.⁷ In 2015 the Court affirmed that at least in Russia “legislation institute[d] a system of secret surveillance under which any person using mobile telephone services of Russian providers can have his or her mobile telephone conversations intercepted, without ever being notified of the surveillance”.⁸ It is now official. In Russia security services and police have direct access through backdoor under their exclusive control to all mobile telephone communications of each and every citizen.⁹

Such system is not incompatible with the Convention only if it provides for “adequate and effective guarantees against abuse”. However, in the

¹ *Roman Zakharov v. Russia* [GC], no. 47143/06, 4 December 2015.

² Convention for the Protection of Human Rights and Fundamental Freedoms. Article 8 § 1.

³ *Klass and Others v. Germany*, no. 5029/71, §§ 48-49, 6 September 1978.

⁴ *Ibid.*, § 50. Emphasis is added.

⁵ *Association for European Integration and Human Rights and Ekimidzhev v. Bulgaria*, no. 62540/00, § 75, 28 June 2007.

⁶ *Kruslin v. France*, no. 11801/85, § 33, 24 April 1990.

⁷ Marko Milanovic, Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age. 56 *Harvard International Law Journal* (2015). P. 81.

⁸ *Roman Zakharov*, cited above, § 175.

⁹ *Ibid.*, §§ 268 and 270. See also: Andrei Soldatov and Irina Borogan, The Red Web. The Struggle between Russia’s Digital Dictators and the New Online Revolutionaries. *Public Affairs* (2015).

reality of potentially total surveillance these guarantees should have more dimensions than in the situation of individualized interceptions. It is not prudent to focus only on the procedure for authorization of surveillance when in fact everyone is followed. This new generation of guarantees against abuse by secret services should aim principally at the process of surveillance and especially use of data thus obtained.

Russian legislation and practice scrutinized by the Court in *Roman Zakharov* provided a good example of what is *not* sufficient.

Supervision over secret surveillance by Russian prosecutors is illusory in practice.¹⁰ It is not conducted in transparent manner.¹¹ Moreover, this supervision is flawed due to the conflict of interests because the same prosecutors need the information obtained through secret surveillance for their criminal cases.¹²

Judicial remedies are *de facto* inaccessible given that the victim of surveillance is by design of the system (known in Russia as “SORM”) deprived of the information about who and to what extent managed to overhear his or her conversations. The only exception is when the criminal proceedings are brought against the person concerned, and relevant communications are disclosed to be used as evidence against him or her. The Court therefore concluded that Russian law did not “provide for an effective judicial remedy against secret surveillance measures in cases where no criminal proceedings were brought against the interception subject”.¹³

The systemic deficiency of Russian law revealed by the European Court of Human Rights in *Roman Zakharov* is exacerbated by the fact that it was consistently found to be compatible with Russian Constitution by the Constitutional Court of the Russian Federation.¹⁴

It led the Court to important conclusion “that Russian legal provisions governing interceptions of communications [did] not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which is inherent in any system of

secret surveillance, and which is particularly high in a system where the secret services and the police have direct access, by technical means, to all mobile telephone communications”.¹⁵

It is not the Court’s task to determine which general measures should be taken by the Russian Federation to ensure compliance with *Roman Zakharov* pursuant to Article 46 of the Convention. However, it is clear from what the Court said that such general measures should cover not only authorization to intercept, but also modalities of storage and destruction of information obtained through secret surveillance.¹⁶ Most importantly, “adequate and effective guarantees against abuse” must encompass independent, effective and continuous supervision of interceptions which is, moreover, subjected to public scrutiny.¹⁷

It is the Court’s position that the secrecy of surveillance measures should not result “in the measures being effectively unchallengeable and outside the supervision of the national judicial authorities” and ultimately the Court itself.¹⁸

For systems like SORM (and there are grounds to believe that they are run not only by the Russian Federation but also by other powerful States) to be compliant with Article 8 of the Convention, independent general overview of the secret services’ activities should be coupled with effective individual complaints procedure accessible for persons concerned.

As for general measures, independent (judicial, public, and / or parliamentary) oversight should include the possibility to routinely check how exactly the secret services utilize the surveillance system and how they dispose of the data collected. In practice, this external audit should be tantamount to at least backdoor to the backdoor. *Modus operandi* of the Interception of Communications Commissioner established by the Regulation of Investigatory Powers Act¹⁹ in the United Kingdom can perhaps be used as a model.

Apart from that, persons who have reasonable

¹⁰ *Roman Zakharov*, cited above, § 284.

¹¹ *Ibid.*, § 283.

¹² *Ibid.*, § 280.

¹³ *Ibid.*, § 298.

¹⁴ *Ibid.*, § 299.

¹⁵ *Ibid.*, § 302.

¹⁶ *Ibid.*, § 302.

¹⁷ *Ibid.*, § 302.

¹⁸ *Kennedy v. the United Kingdom*, no. 26839/05, § 124, 18 May 2010.

¹⁹ See *ibid.*, §§ 57-61.

grounds to believe that their communications were intercepted should have effective and accessible remedy at their disposal, resembling perhaps the Investigatory Powers Tribunal²⁰ in the United Kingdom.

These oversight structures, to be meaningful, should have competence to order the destruction of data if its storage is no longer justified.²¹ One of the important remedies for the persons under surveillance is to ensure *a posteriori* access by them to the dossier collected.²² This remedy represents an important dimension of the right to the truth: "For society in general, the desire to ascertain the truth plays a part in strengthening confidence in public institutions and hence the rule of law. For those concerned... establishing the true facts and securing an acknowledgement... constitute forms of redress that are just as important as compensation, and sometimes even more so".²³ In essence, quarry should be able to pursue the hunters after the chase in order to ensure the fairness of the chase itself.

Irrespective of the particular regulatory scheme in respect of secret surveillance accepted in a given jurisdiction it is clear that new technological realities revealed in *Roman Zakharov* make judicial authorization of interceptions *per se* simply not enough. The 2014 report of the Office of the United Nations High Commissioner for Human Rights noted that judicial involvement in oversight of secret surveillance should not be viewed as a panacea given that "in several countries, judicial warranting or review of the digital surveillance activities of intelligence and / or law enforcement agencies have amounted effectively to an exercise in rubber-stamping".²⁴ *Ro-*

man Zakharov names one of such "several countries".

General approach taken by the Court in *Roman Zakharov* is applicable not only to surveillance of communications transmitted through mobile phones (smartphones). It will most probably lead to case-law concerning backdoors to other digital means of communication such as on-line messengers and social networks, e-mails and new methods of human interaction in the future. However, so far one has to agree with the somber assessment made in 2013 by the Special Rapporteur of the United Nations Human Rights Council on the Promotion and Protection of the Right to Freedom of Opinion and Expression that "[h]uman rights mechanisms have been... slow to assess the human rights implications of the Internet and new technologies on communications surveillance".²⁵

Existence and effective functioning of the independent institutions ensuring both general oversight and examination of individual complaints vis-à-vis massive surveillance conducted by the secret services is indispensable for the exercise and enjoyment of human rights in societies where authorities have advanced surveillance systems like SORM at their disposal. It should not be overlooked that such systems interfere not only with Article 8 (privacy) rights but also with rights enshrined in Article 10 of the Convention (freedom of expression). The mere existence of such systems contributes to the chilling atmosphere of fear and self-censorship that undermines freedom of expression. People are afraid to talk to each other. They are prevented from expressing themselves. Very often not being able to rely on confidentiality of their communications by digital means they choose to stay silent. As infamous saying goes, the fact that one suffers from paranoia does not necessarily mean that he or she is *not* followed.

The United Nations General Assembly in its 2013 Resolution on the right to privacy in the digital age emphasized that unlawful or arbitrary surveillance

Office of the United Nations High Commissioner for Human Rights. A/HRC/27/37 (30 June 2014), § 38.

²⁵ Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. A/HRC/23/40 (17 April 2013), § 18.

²⁰ See *ibid.*, §§ 84-98.

²¹ *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, § 120, 6 June 2006.

²² Véronique Bruck, *Lever le voile sur la surveillance secrete – le droit au respect de la vie privée face à l'activité des services de renseignement. Liber amicorum* Dean Spielmann. *Wolf Legal Publishers* (2015). P. 56.

²³ *El-Masri v. The Former Yugoslav Republic of Macedonia*, no. 39630/09, 13 December 2012. Joint Concurring Opinion of Judges Tulkens, Spielmann, Sicilianos and Keller, § 6.

²⁴ The Right to Privacy in the Digital Age. Report of the

and / or interception of communications as highly intrusive acts violate both right to privacy and right to freedom of expression and may contradict the tenets of a democratic society.²⁶

Apart from that, total secret surveillance of all communications irrespective of their nature by definition threatens advanced confidentiality regime accorded under Article 8 of the Convention to certain types of communications such as those covered by legal professional privilege,²⁷ containing confidential health data,²⁸ and capable of disclosing the identity of the journalistic sources.²⁹

Mobile telephone conversations are frequently transboundary. Freedom of expression includes the right “to receive and impart information and ideas... regardless of frontiers”.³⁰ Cases that the Court will decide in the future building upon *Roman Zakharov* may have extraterritorial dimension. Take, for example, users of Russian mobile phone providers who are outside of Russia. It was convincingly shown that there was “much uncertainty as to how existing case law on the jurisdictional threshold issues might apply to foreign surveillance”.³¹ There are of course essential differences between cases concerning use of lethal force outside of territory of a given State and cases about wiretapping of foreign or transboundary phone conversations. However, there are also similarities, and the useful test is “the degree of control exercised by the state over the conduct alleged to constitute a violation of human rights law”.³² It should be added that in

cases of foreign or extraterritorial surveillance this control may be exercised by more than one State especially given the element of intelligence sharing.

Important and thrilling issue for the Court to deal with in the future is the use of encryption as counter-surveillance technique. Professor David Kaye, new Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, opined in his 2015 report that “[c]ourt-ordered decryption, subject to domestic and international law, may only be permissible when it results from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals (i.e., not to a mass of people) and subject to judicial warrant and the protection of due process rights of individuals”.³³ The Court will explore this myriad of questions in its future cases. Competition between surveillance / decryption and encryption is arms race of the digital age. It has legal dimension, not only technological one.

There is a cross-cutting public / private element of the problem raised by *Roman Zakharov*. The applicant initially brought domestic proceedings against three leading mobile network operators in St. Petersburg arguing that they had installed equipment which permitted the Russian secret services to intercept all telephone communications, the authorities including the Russian intelligence service were joined to the proceedings only as third parties.³⁴ In fact, surveillance conducted by public authorities is impossible without at least tacit approval or connivance by private telecommunications service providers who *de facto* act as undercover agents with, frankly, not much choice left.

But sometimes surveillance can be driven by private interests. Taking aside the cases of commercial espionage and dishonest spouses one can think about the relations between employer and employee. Indeed, as Professor Sheldon Leader has wisely pointed out “[a] good place to examine the protection afforded by basic liberties when vulnerable individuals meet powerful organizations is in

(2011). P. 182.

²⁶ United Nations General Assembly Resolution 68/167, Preamble.

²⁷ *Kopp v. Switzerland*, no. 23224/94, §§ 73-75, 25 March 1998. Note pending case *Versini-Campinchi and Crasnianski v. France*, no. 49176/11, communicated in 2013.

²⁸ *Avilkina and Others v. Russia*, no. 1585/09, § 45, 6 June 2013.

²⁹ *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, no. 39315/06, §§ 97-102, 22 November 2012.

³⁰ Convention. Article 10 § 1.

³¹ Milanovic, cited above. P. 87.

³² Françoise Hampson, *The Scope of the Extra-Territorial Applicability of International Human Rights Law. The Delivery of Human Rights. Essays in Honour of Professor Sir Nigel Rodley*. Edited by Geoff Gilbert, Françoise Hampson and Clara Sandoval, *Routledge*

³³ Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye. A/HRC/29/32 (22 May 2015), § 60.

³⁴ *Roman Zakharov*, cited above, § 10.

the law governing the workplace” given that “it is in the employment relation that balances and imbalances of power present some of their most subtle challenges”.³⁵ Intrusive and secretive big brother may turn out to be your boss, not even a real spy.

Many tired eyebrows of office workers worldwide were raised by the Court’s pronouncement in *Bărbulescu v. Romania*.³⁶ The applicant was fired by his employer for using his on-line messenger during the supposedly busy working hours for chatting with his fiancée and his brother. Employer monitored the applicant’s private communications. The Court found that “it [was] not unreasonable for an employer to want to verify that the employees [were] completing their professional tasks during working hours”.³⁷ In the situation *sub judice*, in the Court’s opinion, that aim justified the means used to achieve it. Will the conclusion of the Court be different if the employer had other objectives such as, for example, learning more about planning of strike by its staff?

It is also a matter of not so distant future that massive private surveillance schemes will be launched very much like private contractors who take active part in many armed conflicts now. Special Rapporteur of the United Nations Human Rights Council on the Promotion and Protection of the Right to Freedom of Opinion and Expression expressly encourages States to “take measures to prevent the commercialization of surveillance technologies, paying particular attention to research, development, trade, export and use of these technologies considering their ability to facilitate systematic human rights violations”.³⁸

Roman Zakharov sets the agenda for a vast area of human rights litigation in the future. Only general contours of this area are visible so far today. Digital frontier poses sets after sets of exciting questions that lawyers should start answering.

³⁵ Sheldon Leader, Human Rights, Power, and the Protection of Free Choice. Strategic Visions for Human Rights. Essays in Honour of Professor Kevin Boyle. Edited by Geoff Gilbert, Françoise Hampson and Clara Sandoval, *Routledge* (2011). P. 82.

³⁶ Application no. 61496/08, Chamber Judgment of 12 January 2016, not yet final at the moment of writing.

³⁷ *Ibid.*, § 59.

³⁸ A/HRC/23/40, cited above, § 97.

The Court has communicated at least two complaints that allege use of massive digital surveillance by British secret services.

In *Big Brother Watch and Others v. the United Kingdom*³⁹ the applicants complain about the program known as PRISM that allegedly allows United States National Security Agency to access a wide range of internet communication content (such as emails, chat, video, images, documents, links and other files) and metadata (information permitting the identification and location of internet users) collected and stored by the American corporations such as Microsoft, Google, Yahoo, Apple, Facebook, YouTube and Skype. In the applicants’ submission, the United Kingdom authorities may have been in receipt of foreign intercept material from the United States relating to their electronic communications. The applicants contend that the United Kingdom Government Communications Headquarters (GCHQ, British intelligence and security organisation “tasked by Government to protect the nation from threats”⁴⁰) conducts generic interception of transboundary communications transmitted by transatlantic fibre-optic cables.

In *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom*⁴¹ the applicants also complain about the system that enables GCHQ to access electronic traffic passing along transatlantic fibre-optic cables running between the United Kingdom and North America. Applicants allege violation of their rights under Article 8 of the Convention and also under Article 10 of the Convention given that, in their submission, the deficiencies and the unlawfulness of the conduct of the British security services and of the applicable regulatory framework has impacted upon their ability to undertake their work of investigative journalism without fear for the security of their communications.⁴²

³⁹ Application no. 58170/13, communicated in 2014.

⁴⁰ Message of Robert Hannigan published at the GCHQ website: http://www.gchq.gov.uk/who_we_are/Pages/welcome-to-GCHQ-from-Robert-Hannigan.aspx.

⁴¹ Application no. 62322/14, communicated in 2015.

⁴² For the summary of legal arguments that may be put forward by the Governments see: Peter Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, 82 *Ford-*

It is safe to predict that *Roman Zakharov* will be relied upon in judgments / decisions of the Court in both cases which “may provide further clarifications”⁴³ of applicable legal standards as well as in many other dossiers to be placed before the judges of the European Court of Human Rights in Strasbourg. Hopefully, they will continuously find right techniques to keep their judicial deliberations totally confidential.

Bibliography and list of authorities

Monographs

Françoise Hampson, *The Scope of the Extra-Territorial Applicability of International Human Rights Law. The Delivery of Human Rights. Essays in Honour of Professor Sir Nigel Rodley*. Edited by Geoff Gilbert, Françoise Hampson and Clara Sandoval, *Routledge* (2011).

Harris, O’Boyle & Warbrick: *Law of the European Convention on Human Rights*. 3rd edition. *Oxford University Press* (2014).

Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*. 56 *Harvard International Law Journal* (2015).

Peter Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, 82 *Fordham Law Review* (2014).

Sheldon Leader, *Human Rights, Power, and the Protection of Free Choice. Strategic Visions for Human Rights. Essays in Honour of Professor Kevin Boyle*. Edited by Geoff Gilbert, Françoise Hampson and Clara Sandoval, *Routledge* (2011).

Véronique Bruck, *Lever le voile sur la surveillance secrete – le droit au respect de la vie privée face à l’activité des services de renseignement. Liber amicorum Dean Spielmann*. *Wolf Legal Publishers* (2015).

European Court of Human Rights case law⁴⁴

Association for European Integration and Human Rights and Ekimidzhiev v. Bulgaria, no. 62540/00, judgment of 28 June 2007.

El-Masri v. The Former Yugoslav Republic of
ham Law Review (2014). P. 2137.

⁴³ Harris, O’Boyle & Warbrick: *Law of the European Convention on Human Rights*. 3rd edition. *Oxford University Press* (2014). P. 556 (author of the chapter – Michelle Lafferty).

⁴⁴ Including communicated cases.

Macedonia, no. 39630/09, judgment of 13 December 2012.

Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands, no. 39315/06, judgment of 22 November 2012.

Versini-Campinchi and Crasnianski v. France, no. 49176/11, communicated in 2013.

Big Brother Watch and Others v. the United Kingdom, no. 58170/13, communicated in 2014.

Bureau of Investigative Journalism and Alice Ross v. the United Kingdom, no. 62322/14, communicated in 2015.

Klass and Others v. Germany, no. 5029/71, judgment of 6 September 1978.

Kruslin v. France, no. 11801/85, judgment of 24 April 1990.

Kopp v. Switzerland, no. 23224/94, judgment of 25 March 1998.

Segerstedt-Wiberg and Others v. Sweden, judgment of no. 62332/00, 6 June 2006.

Kennedy v. the United Kingdom, no. 26839/05, judgment of 18 May 2010.

Avilkina and Others v. Russia, no. 1585/09, judgment of 6 June 2013.

Roman Zakharov v. Russia [GC], no. 47143/06, judgment of 4 December 2015.

Bărbulescu v. Romania, no. 61496/08, judgment of 12 January 2016.

Resolutions, reports and other materials

Message of Robert Hannigan published at the GCHQ website: http://www.gchq.gov.uk/who_we_are/Pages/welcome-to-GCHQ-from-Robert-Hannigan.aspx.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue. A/HRC/23/40 (17 April 2013).

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye. A/HRC/29/32 (22 May 2015), § 60.

The Right to Privacy in the Digital Age. Report of the Office of the United Nations High Commissioner for Human Rights. A/HRC/27/37 (30 June 2014).

United Nations General Assembly Resolution 68/167.