DOI: 10.20472/IAC.2016.021.016

VLADIMIR JILKINE

Riga Stradins University , Finland

THE FIGHT AGAINST CYBER-CRIME IN THE CONTEXT OF COMPLIANCE WITH THE RIGHT TO PROTECTION AGAINST ARBITRARY OR U

Abstract:

The right to privacy of correspondence is enshrined in Article 8 of the European Convention and the jurisprudence of the ECHR. Violation of privacy is one of the crimes against the constitutional rights and freedoms of man. Within the framework of the problems in combating international terrorism and the legitimate interests of law enforcement or national security, restriction on the right of a citizen to privacy of correspondence is permitted only in accordance with the law, including international human rights law. Paragraph 2 of article 17 of the International Covenant on Civil and Political Rights explicitly states that everyone has the right to the protection of the law against unlawful or arbitrary interference with their privacy. This implies that any communications surveillance programme must be conducted on the basis of a publicly accessible law, which in turn must comply with the State's own constitutional regime and international human rights law.

Keywords:

international law, national security and cyber-crime, ECHR case-law, coercive measures.

JEL Classification: K14, K33

Relevance of the issue.

Technology has been advancing at an incredible pace over the last few decades. At present a pocket size digital communication device is easily accessible to every individual and is considered to be an everyday commodity, providing a real time access to communication and data. Ability to share this data in form of photos and voice recordings, especially with the use of social media, has given public an ability to expose abuse of power and improper conduct that may occur and has become a useful tool in an arsenal of Human Rights defenders.

The considerable reduction in the costs of technology and data has but removed financial and physical constraints of surveillance, enabling the State to setup simultaneous, targeted surveillance networks, on a never seen before scale.

In the Report of the Office of the United Nations High Commissioner for Human Rights the governments reportedly have threatened to ban the services of telecommunication and wireless equipment companies unless given direct access to communication traffic, tapped fibre-optic cables for surveillance purposes, and required companies systematically to disclose bulk information on customers and employees. Furthermore, some have reportedly made use of surveillance of telecommunications networks to target political opposition members and/or political dissidents. There are reports that authorities in some States routinely record all phone calls and retain them for analysis, while the monitoring by host Governments of communications at global events has been reported. Authorities in one State reportedly require all personal computers sold in the country to be equipped with filtering software that may have other surveillance capabilities. Even non-State groups are now reportedly developing sophisticated digital surveillance capabilities. [1]

Concerns have been amplified following revelations in 2013 and 2014 that suggested that, together, the National Security Agency in the United States of America and General Communications Headquarters in the United Kingdom of Great Britain and Northern Ireland have developed technologies allowing access to much global internet traffic, calling records in the United States, individuals' electronic address books and huge volumes of other digital communications content. These technologies have reportedly been deployed through a transnational network comprising strategic intelligence relationships between Governments, regulatory control of private companies and commercial contracts.[2]

The progressive development of society is impossible without legitimate application of human rights and without ensuring its unhindered development. At this stage, almost all of the legal, democratic states consolidated within their national legislations the priority and protection of human rights. The Finnish Constitution guarantees the

[1] Human Rigths Council. A/HRC/23/40 . Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development . Report of the Office of the United Nations High Commissioner for Human Rights, para 3.
[2] A/HRC/23/40, para 4.
http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

inviolability of private life and home, honour and personal data. The law provides for actions, concerning the restrictions on privacy of information during a criminal investigation, the judicial investigation and monitoring of state safety. [3]

The right to privacy of communication is considered to be an integral part of human rights - natural and imprescriptible rights of individuals recognized at an international level. Restrictions to this right shall be permitted only on the basis of a court decision. This principle does not only guarantee privacy of personal and family secrets but also confidential information, circulated in official and other public relations.

Monitoring of electronic communications data traffic may be a necessary and effective measure taken in the interest of legitimate law enforcement or national security, where it is carried out in accordance with the law, including international human rights law. However, reports of massive scale digital data surveillance raises questions whether such measures are consistent with international legal standards and whether its needed to reinforce the guarantees of the rule of law in tracking and gathering of this information in order to protect against possible breaches of the human rights. In particular, the measures for tracking and gathering information should not lead to arbitrary or unlawful interference to private and family life of a person, to violate the sanctity of the home, or to disclose the secret of his correspondence; Governments must take concrete measures in providing the protection of the law aimed at preventing such interference.

As recalled by the General Assembly in its resolution 68/167, international human rights law provides the universal framework against which any interference in individual privacy rights must be assessed. Article 12 of the Universal Declaration of Human Rights provides that “no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.” The International Covenant on Civil and Political Rights, to date ratified by 167 States, provides in article 17 that “no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation”. It further states that “everyone has the right to the protection of the law against such interference or attacks.”[4]

Other international human rights instruments contain similar provisions. Laws at the regional and national levels also reflect the right of all people to respect for their private and family life, home and correspondence or the right to recognition and

[3] The Contitution of Finland. Section 10. Everyone's private life, honour and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by an Act. The secrecy of correspondence, telephony and other confidential communications is inviolable.
Measures encroaching on the sanctity of the home, and which are necessary for the purpose of guaranteeing basic rights and liberties or for the investigation of crime, may be laid down by an Act.
In addition, provisions concerning limitations of the secrecy of communications which are necessary in the investigation of crimes that jeopardise the security of the individual or society or the sanctity of the home, at trials and security checks, as well as during the deprivation of liberty may be laid down by an Act.
[4] A/HRC/23/40, para 12.

respect for their dignity, personal integrity or reputation. In other words, there is universal recognition of the fundamental importance, and enduring relevance, of the right to privacy and of the need to ensure that it is safeguarded, in law and in practice.

Paragraph 2 of article 17 of the International Covenant on Civil and Political Rights explicitly states that everyone has the right to the protection of the law against unlawful or arbitrary interference with their privacy. This implies that any communications surveillance programme must be conducted on the basis of a publicly accessible law, which in turn must comply with the State's own constitutional regime and international human rights law.[5]

In its general comment No. 16, the Human Rights Committee underlined that compliance with article 17 of the International Covenant on Civil and Political Rights required that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. [6]

On the other hand the problem of combating extremism, the threat of terrorism, international crime and the increase in trafficking of narcotic substances had a significant impact on the evolution of telecommunication surveillance.

The terms "transnational terrorism" and "cybercrime" are a consistent element in the language of the media and everyday vocabulary. There are cases of Internet resources being used to promote terrorism and setup the recruitment of new The Islamic State of Iraq and the Levant (ISIL) supporters, incitement to ethnic hatred and even fundraising in support of military action groups.

International cooperation in combating organized crime and terrorism is an integral part of the activities of many international organizations for a long time. A European Union summit was held in the city of Tampere, Finland, in 1999. The Heads of State and Government have confirmed that the existence of different national systems of justice hinders coordinated fight against international crime and terrorism. An idea implementation of a "European area of freedom, security and legal protection" was outlined to strengthen the cooperation of all Member States.

This cooperation has become more intense since the terrorist attacks of September 11, 2001. In Europe, this cooperation was further strengthened after the terrorist attacks inflicted on Europe. First it was the explosion of a passenger train in Madrid in April 2004, and the following year an explosion in the London Underground. The Council of Europe strongly opposed international crime and terrorism. Examples of this reinforcement are the European Conventions for the Prevention of terrorism and cybercrime, which came into force in Finland on the 1.9.2007 (L 59/2007).

[5] International Covenant on Civil and Political Rights. Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, Article 17.
[6] Official Records of the General Assembly, Forty-third Session, Supplement No. 40 (A/43/40), annex VI, para. 8.

Government appetite for information about individuals has intensified in the twenty-first century, largely fed by three developments. The first is the appearance of new and dangerous threats to national security, demonstrated by terrorist attacks in New York, Washington, Madrid, London, Mumbai, and elsewhere and compounded by the rise in militant Islamic fundamentalism and increased concerns about chemical and nuclear weapons and cybersecurity vulnerabilities. The second is the explosion in the volume of digital data routinely generated, collected, and stored about individuals' purchases, communications, relationships, movements, finances, tastes—in fact, about almost every aspect of people's lives in the industrialized world— and the ever growing power of technologies to collect, store, and mine such data.[7]

International terrorism and crime, in contrast, have given rise to diverse forms of national and cooperative security strategies led by the United States and by the UN Security Council limited to policing immediate threats. The famous Decision of the European Court of Justice in Joined Cases C-402/05 P and C-415/05 P – Kadi [8] can be seen as one important reaction, in favour of human rights, to the self-constructed new legislative powers of the UN Security Council.

Political leaders, lawyers, and scholars have long grappled with questions of how to protect fundamental freedoms in times of national crisis…This observation is highly relevant in today's national security context. In an environment shaped by the terrorist attacks of September 11, 2001, securing the U.S. homeland from further attacks and confronting terrorist networks abroad are central priorities of U.S. foreign and domestic policy. Yet the transformation of the U.S. security apparatus after 9/11 and a range of new national security programs have generated widespread concern over the protection of international human rights, democratic norms, and a number of rights enshrined in the U.S. Constitution that form, collectively, the civil liberties of the American people.[9]

2 June 2015 vote in the Senate is the most significant action Congress has taken to curtail the nation's intelligence apparatus since the attacks of September 11. In the rush to avoid a prolonged lapse of the nation's bulk metadata collection program, many have criticized the Freedom Act as a hurried attempt. But really it's the first step toward reforming the rushed action Congress took in its passage of the Patriot Act almost 14 years ago.[10]

Interference with an individual's right to privacy is only permissible under international human rights law if it is neither arbitrary nor unlawful. In its general comment No. 16, the Human Rights Committee explained that the term "unlawful" implied that no interference could take place "except in cases envisaged by the law. Interference

[7] Fred H. Cate, James X. Dempsey and Ira S. Rubinstein, "Systematic government access to private- sector data", International Data Privacy Law, vol. 2, No. 4, 2012, p. 195.
[8] Joined Cases C-402/05 P and C-415/05 P. Yassin Abdullah Kadi and Al Barakaat. 21 September 2005. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62005CJ0402
[9] Daniel B.Prieto. War About Terror. Civil Liberties and National Security After 9/11. 2009. P.15.
[10] Senate Votes 67-32 To Reform The NSA's Phone Record Program, June 2, 2015 http://techcrunch.com/2015/06/02/senate-votes-67-32-to-reform-the-nsas-phone-record-program/

authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant".[11]

In other words, interference that is permissible under national law may nonetheless be "unlawful" if that national law is in conflict with the provisions of the International Covenant on Civil and Political Rights. The expression "arbitrary interference" can also extend to interference provided for under the law. The introduction of this concept, the Committee explained, "is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances". [12] The Committee interpreted the concept of reasonableness to indicate that "any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case".

The European Convention of human rights and fundamental freedoms has defined the limits of this right clearer. Article 8 (2) states:

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Under the European Convention, all persons have the right to privacy of correspondence, but this right can be limited "in accordance with the law" and if "necessary in a democratic society."

Also, many international human rights agreements refer to confidentiality of correspondence as a right. The International Covenant on Civil and Political Rights and the UN Convention on the Rights of the Child operate by the same concepts. At national level, the right to private and family life is enshrined by the Constitution, an integral part of this right is to respect the secrecy of private correspondence contained in correspondence, telephone conversations, postal, telegraph and other messages. The trend of a broad interpretation of the term "correspondence" in relation to the rights in question by the Court has found its logical continuation in Article 7 Charter of Fundamental Rights of the European Union, which states that "Everyone has the right to respect for his or her private, family life, home and communications."

However, cyber-attacks continue, compromising national security and violating freedoms and rights of citizens to correspondence and telephone conversations.

July 16th saw a 30-year-old Lauri Love arrested yet again, a Finnish and British citizen has been charged with hacking into various agencies, including the US army, NASA, the Federal Reserve and the Environmental Protection Agency.

[11] Official Records of the General Assembly (see footnote 3), para. 4.
[12] Toonen v. Australia, Communication No. 488/1992, U.N. Doc CCPR/C/50/D/488/1992 (1994). http://www1.umn.edu/humanrts/undocs/html/vws488.htm

The extradition warrant on behalf of the US alleges offences under the Computer Misuse Act for which he has been indicted in the districts of Virginia, New Jersey and New York between various dates in 2012 and 2013.

Love was first arrested by officers from the UK's National Crime Agency under the act in October 2013 and released on bail. [13]

An evident link between cybercrime and organized crime, the professional level and decrease in the age of cyber criminals gaining access to personal data of users of the Internet for fraud with bank accounts should be noted.

On the basis of data provided by the operational department to combat cybercrime, in April 2015 the Helsinki district court ordered the prison sentence of 24-year-old Viljar Kivi for 11 serious crimes in the networks of the Internet, where he received the credit card codes to further money laundering through electronic payments. Earlier, in September 2014 the same court found Viljar Kivi guilty of 280 offenses of fraud and 51 instances of hacking information between the years 2011-2012.

July 7, 2015 City of Espoo District Court sentenced a 17-year-old Finnish teenager Julius Kivimäki to two years probation for 50,700 information burglaries on the Internet in more than a hundred countries, including the server at MIT and Harvard University, he also managed to hack and capture the emails of more than 15 000 University of Massachusetts users.[14]

While the offences were committed the cyber-criminal was 15-16 years old, however his activities have commenced at a tender age of 13 years old. The teenager was sentenced for computer crime, money laundering and fraud: felon has exchanged the credit card data with the third parties and used stolen data for online purchases, colluding with the persons who remain unknown.

As long as there is a risk of proliferation of weapons of mass destruction, terrorism, cyber crime, extremism, transnational crime, drug trafficking within the framework of the problems of combating international terrorism, there is an issue of basic human rights in the context of the fight against terrorism, including having a form of manifestation of human rights to personal integrity, violation of the right to read personal correspondence and recording of the phone conversations.

In this regard, the issue of wiretapping and reading people's private correspondence in social networks by security services remains open. Within the framework of the fight against terrorism and crime, human rights, in particular on the correspondence, are violated. It is often the only way to reduce the number of victims of terrorist acts or avoid them altogether. Yet against the backdrop of the rule of law and respect for

[13] The Guardian. British man accused of hacking into US government networks arrested. 16 July 2015. http://www.theguardian.com/technology/2015/jul/16/british-man-lauri-love-accused-hacking-us-government-computer-networks-arrested

[14] Decision of the district court of Espoo 03.27.1997, R15/268 from 7.7.2015

human rights in such cases it should go only to limit the rights of man, but not a directly violate them.

Violation of the individual's right to respect for private life, his home and his correspondence was repeatedly considered by the European Court of Human Rights. According to Article 8 of the European Convention, the Court has clarified the circumstances under which a state is permitted to violate this integrity and identified a number of requirements for the rules on wiretaps by the member countries of the Convention.

Case of Class and others v. Germany [15] was the first grievance, considered by the European Court of Human Rights on the question of a possible violation of human rights through wiretapping. In 1978, the Court noted that due to "the development of terrorism in Europe" and "very serious threat" faced by European democracies, "the state should have the right to defend themselves against such threats and install secret surveillance of subversive elements operating within its jurisdiction ". In light of these judgments and a detailed study of the legislation in question, the Court concluded that the German legislator justifiably considers that the interference resulting from the implementation of the right, guaranteed by paragraph 1 of Article 8 of the Convention, is necessary in a democratic society in the interests of national security and the prevention of disorder and crime. Accordingly, the Court did not consider the contested German law to be in violation of Article 8 of the Convention.

According to the European Court of Human Rights, the protection of privacy should be considered during both the telecommunication monitoring and the wiretapping.

It is not in dispute that the obtaining by the police of information relating to the numbers called on the telephone in B.'s flat interfered with the private lives or correspondence (in the sense of telephone communications) of the applicants who made use of the telephone in the flat or were telephoned from the flat. The Court notes, however, that metering, which does not per se offend against Article 8 if, for example, done by the telephone company for billing purposes, is by its very nature to be distinguished from the interception of communications, which may be undesirable and illegitimate in a democratic society unless justified [16]

Any capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association. The very existence of a mass surveillance programme thus creates an interference with privacy. The onus would be on the State to demonstrate that such interference is neither arbitrary nor unlawful. [17]

[15] Case of Klass and Others v. Germany, 6 September 1978, Series A no. 28 . Application 5029/71
[16] Case of P.G. and J.H. v. The United Kingdom, art. 42. 25 September 2001. (Application no. 44787/98)
[17] Case of Weber and Saravia v. Germany, para. 78; and Case of Malone v. UK, para. 64.

On the other hand European Court of Human Rights also takes into consideration the fact that the authorities investigating cybercrime should be able to obtain data about the sender of the message from the service provider when it is necessary for solving the crime, which violated the privacy of the victim.

Any data acquisition obtained from communications is a potential invasion of privacy and the collection and preservation of communication data is a breach of privacy, regardless of whether the data is taken into account or used in the future. Even a faint possibility that this information can be registered constitutes an intervention into privacy, potentially constraining the exercise of rights, including the right to freedom of expression and association. Thus, the privacy of life is compromised by the very existence of the program of mass surveillance, where it is a responsibility of a state to prove that such interference is neither arbitrary nor unlawful.

The Court also recognized a violation of Article 6 of the Convention in Zagaria v. Italy. In the applicant's case, an overseer of the jury trial listened in and recorded telephone conversation of the complainant and his lawyer, who was in the courtroom, while the applicant observed the proceedings of the case under detention in a remote location. The Court emphasized that the defendant ability to pass confidential instructions to his lawyer during the proceedings and present evidence to the court is an essential feature of a fair trial. [18]

Case of Popescu v. Romania saw the appeal in regard to wiretapping and transcripts of telephone conversations made by the Romanian intelligence service in absence of the prosecutor's sanction against the suspect and the lack of legal framework providing sufficient guarantees against arbitrariness. The Court noted an insufficient degree of independence of the authorities empowered to authorize the intervention. [19]

Examination of Copland v. United Kingdom case has led to the change of the English common law guarantees for the protection of private life in which employers could record or monitor messages of their employees without their consent. At the request of the head of the college a control scheme was setup that monitored the use of the phone, email and Internet by a member of an educational staff. Phone calls made from the premises are covered by the concept of "private life" and "correspondence" thus the aforementioned actions constituted an interference with her right to privacy of life and correspondence. [20]

The Constitution and the laws of Finland enshrine only one fundamental rule that the restriction of the right to respect for person’s private life and correspondence is possible only on the basis of a court decision. The provisions of the Constitution of Finland (§ 10) and agreements on human rights as a legal interest to be protected; cover the private or family life, reputation, shelter and information.

[18] Case Zagaria v. Italy, 27.11.2007. (Application 58295/00)
[19] Case of Popescu v. Romania (N2), 26.04.2007. (Application 71525/01)
[20] Case of Copland v. United Kingdom , 3.4.2007. (Application 62617/00)

Search, seizure of postal and telegraph correspondence, their recess from the service providers, monitoring and recording of telephone and other conversations may be carried out only if there is sufficient evidence to establish the grounds for the conduct of investigations and the necessity of the court's decision on enforcement of action.

Under Article 3 of Chapter 10 of the coercive measures (Pakkokeinolaki 806/2011) preliminary investigation bodies can grant permission for surveillance, if there is reason to suspect one of the 16 listed serious crimes or suspected in the business or professional activities related to the 9 listed serious crimes. Cp 5 section 1§ of the Police Act (Poliisilaki, 7.4.1995 / 493, entered into force on 01.01.2014) requires the interception of telecommunications, data collection, monitoring, data collection on the location transmitters, systematic and covert surveillance, technical supervision, receiving personal data from telecommunications addresses or service providers, covert action, controlled purchases and deliveries for information in order to prevent the preparation of crimes, detection or prevention of danger. These methods of obtaining information can be used in secrecy from the surveillance subject. During the investigation of criminal cases the investigating authorities can obtain information about the telecommunication monitoring and telephone conversations of suspects after receiving special permission from the court for a period of not more than 1 month.

According to the report, the police department of the Ministry of Internal Affairs of Finland for the collection of classified information and monitoring, in 2014 the police received 1,428 permits for wiretapping and 1631 permits for tracking of mobile phones. [21]

Infraction when considering the prerequisites of application for telecommunication control and wiretapping were established by the decision of the Court of Appeal of Helsinki 21.3.2014. The Court of Appeal stated that on the basis of § 5 (paragraph 2) (821/2011) and § 16 (paragraph 4) of the Act on the Transparency of proceedings in the courts of general jurisdiction in the case of basic information, documentation, and the court's decision shall be classified until the data regarding collection of the information, in accordance with the Law on the use of coercive means (Chapter 10, § 60, paragraph 1), is communicated to the suspect informing him of the crime.

Helsinki Court of Appeal overturned the decision handed down by the court permission for the surveillance and decided that under § 10 of the Constitution everyone has the right to privacy of correspondence, telephone conversations and other confidential communications, but the law can also be installed in compliance with the necessary restrictions to privacy of information in the investigation of crimes encroaching on security of the person or company, or to the inviolability of the home, at the trial, and safety control. This right is enshrined in Article 8 of the Convention for

[21] Police report for the department of Internal Affairs of Finland, the collection of classified information and monitoring in 2014. 02/27/2015. SM 1523217 pp. 4-5.

the Protection of Human Rights and Freedoms and the jurisprudence of the European Court of Human Rights. [22]

In conclusion, we must showcase an example of the result provided by law on wiretapping in the investigation of crimes and for the purpose of a judicial investigation against criminal activities in Finland. As a result of a court of Helsinki permission for wiretapping investigation was initiated on suspicion of having committed a series of criminal cases in Finland. On the basis of this operational data November 15, 2013 the former chief of drug enforcement at the Helsinki Police Department was arrested on suspicion of 29 crimes, including 8 serious drug offenses, organizing the supply of around 1,000 kilograms of hashish from the Netherlands and of involvement in drug sales in Finland.

As the defendants in the case are 12 suspects, among them Keijo Vilhunen, who is considered to be the leader of a large criminal group United Brotherhood, as well as the 4 drug police officers and a subordinate Jari Aarnio and former Estonian policeman accused of money laundering.

The result of monitoring conversations of the Jari Aarnio's associates and his family, followed by the search and seizure of 65,000 euros, buried in the garden of his own house, as well as cash in the garage of the suspect and his daughter.

In the period 2004-2012, Jari Aarnio has acquired 7 cars in his own name, 5 of which are of BMW brand. Furthermore he has purchased 3 BMW cars and an Audi A6 in his wife's name. The investigation has not received a trustworthy explanation for the origin of more than 500,000 euros of cash from Jari Aarnio.

Helsinki district court has sentenced Jari Aarnio on 2.6.2015 to 1 year 8 months in prison on charges of abuse of office and taking bribes under aggravating circumstances in the case of Trevoc. Hearing on drug-related crimes will continue until February 2016. Prosecutor demands punishment for Jari Aarnio by means of imprisonment for a term of 13 years.[23]

Summary

International human rights law provides a clear and universal framework for the promotion and protection of the right to privacy, including in the context of domestic and extraterritorial surveillance, the interception of digital communications and the collection of personal data.

Wiretapping is an interference with the right guaranteed by Article 8 of the European Convention on Human Rights and Fundamental Freedoms. Therefore, in the legal practice and control of the legality of the case review by courts for surveillance permission it is important to check whether the interference is performed in

[22] Decision by Helsinki Court of Appeal from 18.12.2012, HelHO:2012:21
[23] Decision of the district court of Helsinki from 2.6.2015 R14/8864

"accordance with law", whether it processes one or more legitimate goals and whether it is necessary in a democratic society to achieve these goals.

The national legislation of Finland corresponds to the Article 8 of the Convention and the principles established by the case law of the European Court of Human Rights. Nevertheless, national security, the fight against crime and international terrorism require the amendment of national legislation. National legislation should include clear rules to ensure the interests of citizens in an adequate definition of the circumstances and conditions under which public authorities are empowered to take such tacit coercive measures.

Significant place in the responsibility for the implementation of the control functions assigned to the Parliamentary Ombudsman, whose role in terms of legal protection becomes central.

The investigation into former chief of drug enforcement at the Helsinki Police Department Jari Aarnio affected change in the law. The Government of Finland in September 2014 introduced a Parliamentary bill that extends the powers of the police.

The article states that a system of legal protection which includes the permit issued by the court of first instance meet the requirements of the European Court of Human Rights and provides the legitimate right to persons, who are subject to coercive measures.

Nevertheless, the threat of terrorism requires improvements to the safety and control of personal data. The EU has drafted a law giving police the right to check passenger lists.

The Council of Europe has not sorted certain crimes into separate groups, some of which to date are scrutinised in terms of their criminalization and require harmonization of legislation at an international level. One of those is the so-called "cyber-terrorism" and the use of cyberspace for purposes of terrorism. The lack of a unified definition for terrorism at an international level creates difficulties with the debate on the subject of cyber-terrorism as a phenomenon while requiring a universal criminalization in the interests of an international community. Cooperation and intelligence sharing between law enforcement agencies in the investigation and prosecution of international cases for information technology is needed among all interested States.

References

Human Rigths Council. A/HRC/23/40 . Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development . Report of the Office of the United Nations High Commissioner for Human Rights, para 3.

A/HRC/23/40, para 4.

The Constitution of Finland. Section 10. Everyone's private life, honour and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by an Act. The secrecy of correspondence, telephony and other confidential communications is inviolable.

Measures encroaching on the sanctity of the home, and which are necessary for the purpose of guaranteeing basic rights and liberties or for the investigation of crime, may be laid down by an Act. In addition, provisions concerning limitations of the secrecy of communications which are necessary in the investigation of crimes that jeopardise the security of the individual or society or the sanctity of the home, at trials and security checks, as well as during the deprivation of liberty may be laid down by an Act.

A/HRC/23/40, para 12.

International Covenant on Civil and Political Rights. Adopted and opened for signature,

Official Records of the General Assembly, Forty-third Session, Supplement No. 40 (A/43/40), annex VI, para. 8.

FRED H. CATE, JAMES X. DEMPSEY AND IRA S.RUBINSTEIN, “Systematic government access to private- sector data”, International Data Privacy Law, vol. 2, No. 4, 2012, p. 195.

Joined Cases C-402/05 P and C-415/05 P. Yassin Abdullah Kadi and Al Barakaat. 21 September 2005.

DANIEL B.PRIETO. War About Terror. Civil Liverties and National Security After 9/11. 2009. P.15.

Senate Votes 67-32 To Reform The NSA’s Phone Record Program, June 2, 2015

http://techcrunch.com/2015/06/02/senate-votes-67-32-to-reform-the-nsas-phone-record-program/

Official Records of the General Assembly (see footnote 3), para. 4.

Toonen v. Australia, Communication No. 488/1992, U.N. Doc CCPR/C/50/D/488/1992 (1994).

The Guardian. British man accused of hacking into US government networks arrested. 16 July 2015.

Decision of the district court of Espoo R15/268 from 7.7.2015

Case of Klass and Others v. Germany, 6 September 1978, Series A no. 28 . Application 5029/71

Case of P.G. and J.H. v. The United Kingdom, art. 42. 25 September 2001. (Application no. 44787/98)

Case of Weber and Saravia v. Germany, para. 78; and Case of Malone v. UK, para. 64.

Case Zagaria v. Italy, 27.11.2007. (Application 58295/00)

Case of Popescu v. Romania (N2), 26.04.2007. (Application 71525/01)

Case of Copland v. United Kingdom , 3.4.2007. (Application 62617/00)

Police report for the department of Internal Affairs of Finland, the collection of classified information and monitoring in 2014. 02/27/2015. SM 1523217 pp. 4-5.

Decision by Helsinki Court of Appeal from 18.12.2012, HelHO:2012:21

Decision of the district court of Helsinki R14/8864 from 2.6.2015 R14/8864