HELSIŃSKA FUNDACJA PRAW CZŁOWIEKA
HELSINKI FOUNDATION for HUMAN RIGHTS

Warsaw, on the 9th of February 2016

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM

(Application No. 58170/13)

WRITTEN COMMENTS

BY

THE HELSINKI FOUNDATION FOR HUMAN RIGHTS

1. Introduction

Pursuant to the letter of Mr Søren Nielsen, the Section Registrar of the First Section of the European Court of Human Rights (hereinafter also referred to as "ECtHR"), dated 15th December 2015, granting leave to make written submissions to the High Court by the 9th of February 2015, and our letter of 27th March 2015, the Helsinki Foundation for Human Rights (hereinafter also referred to as "HFHR") with its seat in Warsaw, Poland, would like to respectfully present its written comments on the case of *Big Brother Watch and Others against the United Kingdom* (app. no. 58170/13).

Due to the nature of third-party intervention in the form of written comments, we do not include any comments on the facts or merits of the analysed case of *Big Brother Watch and Others v. the United Kingdom*. These comments are limited to general principles involved in the solution of the case. We discuss the domestic constitutional and legislative standards in the matter of operational control used by the secret services. Within these written comments we would also like to present the HFHR's experience concerning the judicial control over the surveillance of communication by public authorities in Poland. In addition to that we would like to elaborate on the judgment delivered by the Polish Constitutional Tribunal in case K 23/11 and briefly discuss how the judgment is now being realised by the Polish authorities.

00-018 Warszawa, ul. Zgoda 11; tel.: (48 22) 556-44-40, fax: (48 22) 556-44-50; e-mail: hfhr@hfhr.org.pl, www.hfhr.pl
NIP: 525-12-61-255, konto: PKO BP SA I O/Centrum 58 1020 1013 0000 0502 0002 9165, swift: BPKOPLPW

Finally, these written comments contain brief signalisation of the flaws which can be identified within the Polish standards concerning operational control from the perspective of Article 8 of the Convention.

It needs to be underlined that we fully support the written comments presented by the HFHR in another case that is currently pending before the ECtHR - the case of *Bureau of Investigative Journalism and Alice Ross v. United Kingdom* (appl. no. 58170/13). In the other case the HFHR presents the analysis of the issues related to mass surveillance in the context of Article 10 of the Convention. The HFHR elaborates on the need for enhanced standard of protection of the safeguards of Article 10 of the Convention for journalists and certain other professional groups.

2. Protection of privacy under the Polish constitution

In order to put the HFHR's experience that will be described in the next section of these written comments, we would like to respectfully present to the High Court certain standards on the right to privacy in the Polish legal system. Due to the nature of these written comments, these description will be limited to the analysis of the provisions of Polish constitution and the interpretation of these provisions made by the Polish Constitutional Tribunal.

The right to privacy is primarily defined in Article 47 of the Polish Constitution[1] which states that "Everyone shall have the right to legal protection of his private and family life, of his honour and good reputation and to make decisions about his personal life.". In addition to that Article 51 provides for the so-called information autonomy:

> *Article 51*
>
> *1. No one may be obliged, except on the basis of statute, to disclose information concerning his person.*
>
> *2. Public authorities shall not acquire, collect nor make accessible information on citizens other than that which is necessary in a democratic state ruled by law.*
>
> *3. Everyone shall have a right of access to official documents and data collections concerning himself. Limitations upon such rights may be established by statute.*
>
> *4. Everyone shall have the right to demand the correction or deletion of untrue or incomplete information, or information acquired by means contrary to statute.*
>
> *5. Principles and procedures for collection of and access to information shall be specified by statute.*

As is mentioned in the legal doctrine, the term "necessary" under Article 51(2) of the Constitution describes such information, which is indispensable for the public authorities to conduct the activities defined under its competence. This means that the scope and details of the information that is to be acquired must be assessed on a case to case basis[2].

The Constitutional Tribunal also pointed in its judgments that the information autonomy also corresponds with the protection of privacy of correspondence (Article 49 of the Constitution) and the freedom of communication[3]. It has been underlined by the Constitutional Tribunal that the

---

[1] Poland, Official Journal of 1997 no. 78 pos. 483. English translation of the Polish Constitution is available at: http://www.sejm.gov.pl/prawo/konst/angielski/kon1.htm. Date of access: 7th February 2016.

[2] B. Banaszak, *Commentary to Article 51, The Constitution of the Republic of Poland (Komentarz do art. 51, Konstytucja Rzeczpospolitej Polskiej)*, Warsaw 2009, p. 262.

[3] See e.g. the Constitutional Tribunal judgment of 20th June 2005 in case K 4/04.

retention of dignity by a human being requires that his strictly personal sphere is respected, i.e. the sphere where he is no exposed to the necessity of "being with others" or "sharing with others" of his experiences or sensations[4].

The general rule for establishing limitations to rights and freedoms of citizens and other persons is to be found in Article 31 (3) of the Constitution which states that should there be limitations upon the abovementioned, they may be imposed only by statute, and only when necessary in a democratic state for the protection of its security or public order, or to protect the natural environment, health or public morals, or the freedoms and rights of other persons. Such limitations shall not violate the essence of freedoms and rights. The rule of proportionality is thus established. The Constitutional Tribunal has in addition stipulated that the abovementioned Article 51 provides for a special means of protection of the values enshrined under Article 47 of the Constitution[5].

3. The HFHR experience connected with the involvement of Polish public bodies in the PRISM programme

Due to the Edward Snowden's publication of information concerning the activities of NSA, on 15th October 2013 the Helsinki Foundation for Human Rights (hence: "HFHR"), the Panoptykon Foundation and Amnesty International have brought before various public authorities in Poland motions on access to public information on the activities of the National Security Agency in Poland. The HFHR has brought the motions concerning various aspects of the case of E. Snowden to the heads of special services: the Internal Security Agency, the Central Anticorruption Bureau, the Military Counterintelligence Service and the Military Intelligence Service.

The motion on access to public information in Poland is a legal instrument prescribed in the Constitution and the Act from 6th September 2001 on access to public information[6]. As article 61 (1) provide a citizen shall have the right to obtain information on the activities of organs of public authority as well as persons discharging public functions. Such right shall also include receipt of information on the activities of self-governing economic or professional organs and other persons or organizational units relating to the field in which they perform the duties of public authorities and manage communal assets or property of the State Treasury. Article 61 (3) states that limitations upon the rights referred to in paras. 1 and 2 above, may be imposed by statute solely to protect freedoms and rights of other persons and economic subjects, public order, security or important economic interests of the State. As provided in article 10 of the aforementioned Act, public information that was not made available via the Public Information Bulletin or in the central repository, is made available upon motion. Article 5(1) of the Act on access to public information clarifies that the right to public information is subject to limitations to the extent and on the conditions defined in the regulations on the protection of confidential information and other secrets protected by law (pol. *"[...] w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych"*). This means that under Polish law the authorities can deny access to certain categories of information, *i.a.* under the regime that is defined in the Act of 5th August 2010 on the protection of classified information[7].

In addition to the abovementioned motions, the HFHR has in 2013 officially asked the Ministry of Administration and Digitalization, the Ministry of the Interior and the parliamentary Commission on Secret Services and the Commission on Justice and Human Rights whether the matters of the invigilation of Polish citizens under the PRISM programme were a subject of debate under the

[4] *Inter alia* the Constitutional Tribunal judgment of 23rd June 2009 in case K 54/07 (OTK ZU nr 6/A/2009).
[5] The Constitutional Tribunal judgment of 24th June 1997 in case K 21/96 (OTK ZU 2/1997).
[6] Poland, Official Journal from 2001 no. 112 pos. 1198.
[7] Poland, Official Journal from 2010 no. 182 pos. 1228.

works of these institutions[8]. By that time, the HFHR pointed out that the activities conducted under the Prism programme might be considered as a significant interference with the sphere of citizen's rights and freedoms, especially with the right to privacy as defined in Article 47 of the Polish Constitution ("Everyone shall have the right to legal protection of his private and family life, of his honour and good reputation and to make decisions about his personal life.").

The questions included in the motions for public information that were launched in 2013 concerned primarily whether the special services were offered the opportunity to use the XKeyscore Programme, which gives the possibility to analyze the data that is sent via Internet and the possibility to de facto use the aforementioned data by the special services. The questions concerned also whether the special services were capable of tracking the phone communications and communications made via Internet by the use of keywords. Taking into account the relevant for that day wording of: the Act of 24th May 2002 on the Internal Security Agency and the Intelligence Agency[9], the Act of 9th June 2006 on the Central Anticorruption Bureau[10] and the Act of 9th June 2006 on the Military Counterintelligence Service and Military Intelligence Service[11], the HFHR asked also whether the use of that type of surveillance measures was in accordance with Polish law. The question directed to the Internal Intelligence Agency also pertained to the matter whether the Agency cooperated with the American services in respect to conferring telecommunication data, and whether the American Party was the initiator of the cooperation.

The heads of the secret services refused to grant access to public information. The refusal was justified, firstly, by the fact that information on the possibility of the use of that measures by the secret services was protected as classified information. Secondly, the heads of the secret services pointed that the requested information could not be disclosed due to the obligation to protect the forms, methods and operational means that derived from the aforementioned Acts. The heads of secret services pointed out generally that the requested information was of classified character, even if it was no officially attributed with one of the four secrecy clauses (i.e. "top secret", "secret", "confidential" and "proprietary"). In their opinion it was necessary to protect the aforementioned information in order to avoid lowering of the public safety level. As for the matter of conformity of the use of such measures with the Polish legislation, the heads of the secret services pointed that pursuant to the Act on Access to Public Information one cannot request the public authorities to interpret binding legal regulations.

The HFHR Rights has challenged the refusal of granting access to information to the Voivodeship Administrative Court in Warsaw. In the cases against the heads of the Central Anticorruption Bureau, the Military Counterintelligence Service and the Military Intelligence Service the court has rejected the complaint made by the Foundation[12]. The Court generally agreed with the positions presented by the secret services and held that it was sufficient to rely on the protection of requested information on the basis its confidential character. The Court noted that the security of the State outweighed the citizen's right to access public information.

As for the complaint against the Head of the Internal Security Agency refusal of access to information, the Voivodeship Administrative Court in Warsaw took a different point of view and held that the potential detriment to the public security was only abstract and hypothetical[13]. The

[8] Further information is available at: http://www.hfhr.pl/hfpc-pyta-o-prism/. Date of access: 7th February 2016.
[9] Poland, Official Journal from 2002 no. 74 pos. 676 with further changes.
[10] Poland, Official Journal from 2006 no. 104 pos. 708 with further changes.
[11] Poland, Official Journal from 2006 no. 104 pos. 709 with further changes.
[12] The Voivodeship Administrative Court in Warsaw judgment of 28th march 2014 in case II SA/Wa 141/14; the The Voivodeship Administrative Court in Warsaw judgment of 11th September 2014 in case II SA/Wa 723/14; the Voivodeship Administrative Court in Warsaw judgment of 8th October 2014 in case II SA/Wa 616/14.
[13] The Voivodeship Administrative Court in Warsaw judgment of 25th June 2014 in case II SA/Wa 710/14.

Court pointed out that the questions about agreements between the special services were formulated in a very general character. The Court thus held that the citizens were entitled to be informed about the activities of the state in relation to the public security policy. The Court stated that it is justified considering especially the scope of engagement in such political activities of significant financial means and considering the growing terrorist threat, threat of hacker attacks and surveillance of the multimedia environment. Finally the Court pointed out that the transparency of public life cannot be overlooked in the process of assessment whether a specific information can be made public based on the constitutional right to public information. As far as the use of invigilation methods by the Agency is concerned, the Court pointed that not all of such methods are protected by secrecy. Considering that the questions did not pertain to application of such methods in individual cases, in the opinion of the Court there was no reason to deny access to public information.

Currently, the cassation complaint against the judgments of the Voivodeship Administrative Court are awaiting trial before the Supreme Administrative Court.

The Supreme Administrative Court, acting upon a cassation complaint brought by the HFHR, in its judgment of 18th August 2015[14] has partly set aside the judgment of the Voivodeship Administrative Court in Warsaw in which the Court upheld the decision of the Head of the Central Anticorruption Bureau that denied access to information concerning XKeyscore Programme and tracking the phone communications and communications made via Internet by the use of keywords. The Supreme Administrative Court held that the Head of the Central Anticorruption Bureau has lawfully denied access to information concerning the technical capabilities of tracking of communications made by phone and via Internet by the use of keywords:

> *In the opinion of the Supreme Administrative Court the unauthorized publication of information concerning the technical capabilities of tracking phone calls and communications made via Internet by the use of keywords would or at least could be detrimental for the Republic of Poland or would be adverse from the perspective of its interests – Article 1(1) of the Law on protection of confidential information, which allows to classify the information as falling under the regime of protection of classified information, regardless of whether it was granted any secrecy clauses (...) The aforementioned data enables to formulate conclusions not only about the points of interest of the CAB, but also about the actual capabilities of the secret service. Since the CAB is a secret service designed to fight against corruption in public and economic domain, especially in state and local government institutions, and also to fight against any activities undermining the economic interests of the state, the learning about the methods and technical means that are used by the service would with a significant degree of probability detriment the realization of its tasks defined by law*[15].

The reason why the Supreme Administrative Court partially set aside the judgment of the court of lower instance and relegated the case for anew examination is because the Voivodeship Administrative Court did not provide in its judgement significant argumentation concerning the question of Central Anticorruption Bureau access to XKeyscore Programme. The Supreme Administrative Court stated that it the Voivodeship Court did not provide sufficient argumentation why it agreed with the Head of the secret service that the knowledge on whether the CAB has access to XKeyscore Programme should be treated as confidential information.

In 2014 the HFHR also requested the Head of the Central Anticorruption Bureau to grant access to public information, whether this secret service was using the computer software ("spyware") called "Remote Control System". The Head of the Central Anticorruption Bureau denied access to

[14] The Supreme Administrative Court judgment of 18th August 2015 in case I OSK 1679/14. Judgment available at the Central Base of Administrative Court rulings: http://orzeczenia.nsa.gov.pl/doc/24669337CC. Date of access: 7th February 2016.
[15] *Ibidem.*

information due to the confidential nature of the requested information. Similarly as in the cases concerning XKeyscore Programme and tracking communications by the use of key words, the Central Anticorruption Bureau held that revealing the information would contravene against the obligation to protect the forms, methods and operational means of the secret service. The Voivodeship Administrative Court, to which the Foundation brought a complaint against this decision, supported the argumentation of the Head of the secret service[16]. A cassation complaint against this judgment is currently pending.

In the opinion of HFHR the presented above description of mostly ineffective motions for access to information concerning the usage of XKeyscore Programme and other controversial operational measures proves that within the Polish system it is nearly impossible to review whether factual interferences with privacy that take place in connection with the work of secret services are meeting the requirements set in the Polish constitution and standards set out by binding international law. Without knowledge on the extent of interference, it is not possible to say whether such interference is justifiable. If such is the case for social "watchdogs" like the HFHR, it will be even more so for ordinary citizens.

4. Judgment of the Polish Constitutional Tribunal

The Constitutional Tribunal gave judgment on 30th July 2014[17] in a case initiated by the Polish Ombudsman concerning the "police" laws (the laws governing the organization and functioning of the Police, the Border Guard, the fiscal control, the Military Police and the of the secret services mentioned in the previous part of these written comments). The part of the aforementioned judgment that is most relevant for the currently analyzed case *Big Brother Watch and Others v. the United Kingdom* is the part concerning the so-called "operational control" (pol. *kontrola operacyjna*) by the services and acquiring and processing of the telecommunications data. The operational control pertains to the contents of communication, whereas the telecommunication data describe the characteristics of communication itself.

The Polish Prosecutor General in a written submission before the Polish Constitutional Tribunal concurred with the Ombudsman view and pointed out that:

> *[...] the regulation questioned by the Applicant strikes upon the right to privacy, the freedom of communication, the information autonomy and the right to judicial review due to lack of precision, vagueness and non-completeness of the regulation, lack of subsidiarity of the invasion of constitutionally guaranteed rights and freedoms of an individual, lack of judicial control over the acquisition of telecommunication data by the services, a lack of regulation concerning informing individuals about the operational control conducted in relation to them, as well as lack of respecting of professional privilege and probational bans connected with such professional privilege*[18].

The HFHR in the course of the proceedings before the Constitutional Tribunal in case 23/11 has presented an *amicus curiae* brief[19]. In our opinion we have underlined that it was eventually up to the discretion of the services to make the decision on what technical means will be used in a specified proceedings. The only limitations upon the applied means of confidential surveillance by

[16] The Voivodeship Administrative Court in Warsaw judgment of 13th July 2015 in case II SA/Wa 1670/14.

[17] The Constitutional Tribunal judgment of 30th July 2014 in case K 23/11 (Official Journal from 2014 pos. 1055).

[18] Poland, The written position made by the Prosecutor General, p. 92. Available at: http://ipo.trybunal.gov.pl/ipo/Sprawa?&pokaz=dokumenty&sygnatura=K%2023/11. Date of access: 8th February 2016.

[19] The Helsinki Foundation for Human Rights *amicus curiae* opinion from 13th June 2012 in case 23/11. The opinion is available at: http://www.hfhrpol.waw.pl/precedens/images/stories/opinia_srodki_techn_13_06_12.pdf. Date of access: 8th February 2016.

the services are the financial and organizational capabilities of the services[20]. The HFHR has also underlined that only clearly and precisely formulated regulatory framework legitimizes the state to limit the rights and freedoms of individuals by the means of application of surveillance methods[21]. The HFHR postulated the creation of a limited list of operational means that could be used by the services, especially considering the scope of the application of operational control in Poland[22].

The operational control is conducted in secrecy and can consist of: 1) the examination of the contents of correspondence; 2) the examination of the contents of packages; 3) the application of technical measures which allow to acquire information and evidence in a secret manner and preserve it, especially the contents of phone calls and other information distributed through telecommunication networks. The Constitutional Tribunal adjudicated on the constitutionality of an open-ended catalogue of measures that could be used within the operational control. The complainants before the Constitutional Tribunal argued that the term "technical measure" was very vague and imprecise. The Constitutional Tribunal did not agree with this argumentation. It held that the contested regulation complies with the Constitution provided that in the order on application of operational control the relevant authorities point to a defined in law technical measure of acquiring information and evidence and preserving it.

The judgment of the Constitutional Tribunal in respect to the conduction of operational control also covered the question, in what situations is the ordering of operational control possible. The Constitutional Tribunal adjudicated in relation to the Internal Security Agency that it is unconstitutional to grant the service with the right to order operational control on the basis of prevention, detection and prosecution of crimes "detrimental to the economical fundaments of the State". The Constitutional Tribunal pointed out, *i.a.* that the Polish regulations did not contain a catalogue of that kind of crimes.

The Constitutional Tribunal adjudicated that the regulations on applying operational control were incompatible with the Polish Constitution also in extent in which they did not provide for guarantees of prompt, official and protocolar destruction of materials containing information protected under professional privilege (i.a. for attorneys, physicians and journalists) if a court did not repeal the professional privilege or the repealing was impermissible. The existing regulations did not provide for a procedure of destruction of materials containing information protected under professional privilege which was acquired in the process of operational control. As a result, the data could have been used in the course of criminal proceedings.

As far as the telecommunication data (*i.a.* cell phone location, billing data) is concerned, the Constitutional Tribunal found that it is contrary to the Constitution that there is no independent control over sharing that data with the services. Under the contested regulations the acquiring of such data was allowed for the purposes of "prosecution of offences" and "fulfilling the tasks defined by laws" and was not subject to obtaining a permission from the court, or the prosecutor. The Constitutional Tribunal also declared unconstitutionality of the lack of obligation to promptly destroy collected telecommunication data which was of no use for the purposes of a pending criminal procedure.

Within the *obiter dicta* section of the judgment, the Constitutional Tribunal stated that the constitutional protection of privacy, as resulting from Articles 47, 49 and 51 of the Polish Constitution, covers all means of transferring of information, in whatever form of communication and regardless of the existence of physical carrier of the information. The constitutional protection:

---

[20] *Ibidem*, p. 3.
[21] *Ibidem*, p. 5.
[22] *Ibidem*, p. 12.

[...] covers not only the contents of the message, but also all circumstances of the process of communication, to which one can include the personal data of the participants of this process, information on dialed phone numbers, searched web pages, the data that presents time and frequency of calls or enabling the geographical localization of the participants of the conversation, finally the data on IP number and IMEI number[23].

The Constitutional Tribunal ordered that the provisions which were declared unconstitutional were to lose their binding force after the elapse of eighteen months since the publication of the judgment in Polish Official Journal.

5. Current standards of "operational control" under Polish legislation

In order to realize the judgment of the Constitutional Tribunal in case 23/11 the Polish Parliament has enacted the Act of 15th January 2016 on the amendment of the Act on the Police and several other acts[24] (pol. *Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw*). This Act has been enacted by the parliamentary majority elected in the fall of 2015, but to a significant extent, as has been noted by non-governmental organizations, it is a reiteration of the propositions that were being prepared by the previous parliament[25].

To illustrate the scope of the competence of the Police and other services, it is fruitful to analyze current wording of the Article 20c of the Act on the Police, which is the result of the abovementioned amendment. Under Article 20c of the current wording of the Act of the Police:

1. In order to prevent or detect crimes, or in order to save life or health of humans, or in order to support search and rescue missions, the Police can acquire the data which do not constitute the content of respectively, telecommunications, postal consignments or a communication made within the framework of electronical service, as specified in:

...

3) Article 18 (1-5) of the Act of 18th July 2002 on the provision of services by the use of electronic means (Official journal from 2013 pos. 1422 and from 2015 pos. 1844), hereinafter reffered to as "internet data".

- and can process them without knowledge and consent of the person, to whom they apply.

2. The telecommunication undertaking, postal operator and the provider of services by the use of electronic means makes the data mentioned in (1) available free of charge (...)

Similar competence is now vested due another provisions of the Act of 15th January 2016 on the amendment of the Act on the Police and several other acts to the also with other services, such as the Border Guard, the fiscal control organs, the Military Police and the Customs Office.

The Polish non-governmental organizations have presented concerns, whether the proposed regulations comply with the standard, *inter alia* set out in Article 8 of the Convention[26]. The

[23] *Ibidem*, para. 1.4.
[24] Poland, Official Journal from 2016 pos. 147.
[25] See, i.a. the opinion of Panoptykon Foundation available at: https://panoptykon.org/wiadomosc/sluzby-wciaz-poza-kontrola-zmarnowana-szansa-na-dobra-zmiane
[26] Poland, A letter of 10 non-governmental organisations directed to the Members of Parliament (signed by the Amnesty Internation, the Digital Centre, E-Państwo Foundation, the Frank Bold Foundation, the Modern Poland Foundation, the Panoptykon Foundation, the Helsinki Foundation for Human Rights, the Public Matters Institute, the Association of Legal Intervention, the Klon/Jawor Association). Available at:

organizations stated that the term "internet data" is not precise and there are genuine doubts whether such data would not include the contents of electronic correspondence. The NGO's underlined that the scope of this term beyond any doubts includes a broad category of meta-data. The new regulation has also been a subject of criticism of the Polish Ombudsman[27].

The NGO's have also pointed out that under the Act (by then it was a parliamentary project), there were no guarantees of genuine and preventive judicial control over the access by the services to the telecommunication and internet data.

There are genuine doubts whether the Act of 15th January 2016 on the amendment of the Act on the Police and several other acts does not contradict the requirements set out in the previous jurisprudence of the ECtHR concerning Article 8 of the Convention. In case of *Liberty and Others v. the United Kingdom*[28], the High Court reiterated that the expression "in accordance with the law" under Article 8 § 2 of the Convention also "[...] refers to the quality of the law in question, requiring that it should be compatible with the rule of law and accessible to the person concerned, who must, moreover, be able to foresee its consequences for him"[29]. The Court also repeated its case-law on the requirement of legal "foreseeability" in the field of secret measures of surveillance" as followed from the *Weber and Saravia*[30] admissibility decision. The Court indicated once more that "[T]he domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures"[31]. The ECtHR also set minimum protective standards that should be included in the statute law to prevent abuses of power[32] by, e.g. the secret services or the Police.

Additionally, the High Court stressed in the *Liberty and Others v. the United Kingdom* case that it does not "consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other"[33].

6. Conclusions

Considering the argumentation presented in these written submissions, we believe that the subject of analysis in the case *Big Brother Watch v. the United Kingdom* will present an opportunity for the European Court of Human Rights to confirm that it is of paramount importance to safeguard the right to private and family life, as defined in Article 8 of the Convention, in the context of mass surveillance and sharing information by secret services across Europe.

---

http://programy.hfhr.pl/monitoringprocesulegislacyjnego/apel-10-organizacji-pozarzadowych-ws-zmian-w-uprawnieniach-sluzb/. Date of access: 8th February 2016.

[27] Poland, Ombudsman (pol. *Rzecznik Praw Obywatelskich*), Position concerning the parliamentary project of the Act on amendment of the Act on the Police and several other acts; Sejm document no. 154 (pol. *Wystąpienie w sprawie poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw - druk sejmowy nr 154*).

[28] European Court of Human Rights (Fourth Section) judgment of 1st July 2008 in case of Liberty and Others v. the United Kingdom (appl. no. 58243/00).

[29] *Ibidem*, para. 59.

[30] Third Section Decision as to the admissibility of Gabriele Weber and Cesar Richard Saravia v. Germany (app. no. 54934/00), paras. 93-95.

[31] *Ibidem*, para. 93.

[32] *Ibidem*, para. 95: „[...]the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; 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; and the circumstances in which recordings may or must be erased or the tapes destroyed".

[33] *Liberty and Others v. the United Kingdom...*, para. 63.

The Helsinki Foundation for Human Rights believes that our written comments will provide the High Court will valuable information concerning the matters of operational control and methods used by the secret services in the Republic of Poland. In the Foundation's opinion, the future judgment of the High Court in the analyzed case will serve as a model for the formulation of statutes regulating the methods and means used by secret services, and will thus enhance the protection of human rights standards in Poland and other Council of Europe Members.

These written comments have been prepared by advocate Artur Pietryka and Michał Kopczyński from the Strategic Litigation Programme of the Helsinki Foundation for Human Rights.

On behalf of the Helsinki Foundation for Human Rights,

FUNDACJA PRAW CZŁOWIEKA HELSIŃSKA 00-018 Warszawa ul. Zgoda 11

Piotr Kładoczny, Ph.D.

The Secretary of Board

Helsinki Foundation for Human Rights