HELSIŃSKA FUNDACJA PRAW CZŁOWIEKA
HELSINKI FOUNDATION for HUMAN RIGHTS

BUREAU OF INVESTIGATIVE JOURNALISM AND ALICE ROSS V. UNITED KINGDOM

(Application No. 62322/14)

WRITTEN COMMENTS BY THE HELSINKI FOUNDATION FOR HUMAN RIGHTS

9 FEBRUARY 2016

I. INTRODUCTION

Pursuant to the letter by the Section Registrar from 15 December 2015, we would like to present written comments of the Helsinki Foundation for Human Rights (HFHR) with its seat in Warsaw, Poland on the *Bureau of Investigative Journalism and Alice Ross v. United Kingdom* case before the Court. From 2008 the HFHR runs a programme specifically focused on freedom of expression issues – the "Observatory of Media Freedom in Poland". The Observatory engages inter alia in strategic litigation and advocacy activities in this area. One of the most important themes in our activity is protection of journalistic secrecy. On the national level, we have been involved in many individual cases of journalists and advocated for improving legal safeguards in this respect. From 2010, when it was revealed that the mobile phones metadata of 10 journalists working for nationwide media were subject to surveillance by the Polish intelligence agencies[1], we have become particularly interested in the threats to the confidentiality of journalistic sources of information posed by the new surveillance technology.

While all citizens should be adequately safeguarded against arbitrary mass surveillance, journalists are one the professional groups which needs enhanced protection. The aim of this third-party intervention is to present the HFHR's experience and expertise with regard to the impact of the use of mass surveillance instruments on journalistic secrecy and – consequently - on the journalists' capacity to fulfill appropriately their "public watchdog" role. In this context we consider the mass surveillance not only to be one of the most serious and current dangers for the right to privacy, but at the same time – also for the freedom expression. That is why, in our brief, we would like focus on issues related to the violation of Article 10 of the ECHR. However, we would like to stress that, as far as the Article 8 is concerned, we consider all the arguments presented by the HFHR in the submission filed in another case pending before the ECtHR – *Big Brother Watch and others v. United Kingdom* (application no. 58170/13) – to be very relevant for the resolution of the *Bureau of Investigative Journalism and Alice Ross v. United Kingdom* case as well.

II. MASS SURVEILLANCE AND FREEDOM OF EXPRESSION

[1] W. Czuchnowski, "Dziennikarze na celowniku służb", Gazeta Wyborcza, 08 October 2010, http://wyborcza.pl/1,76842,8480752,Dziennikarze_na_celowniku_sluzb_specjalnych.html (access: 8 February 2016)

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

1. Legal context

The need to protect the confidentiality of journalistic sources is a well-established principle recognized both most national legislations, as well as international human rights standards. It is considered necessary to guarantee a free flow of information and to protect the public interest. The development of digital means of communications, followed by the development of new surveillance methods, has brought new challenges with regard to legal protection of journalistic sources. In the last decade we have witnessed the rise in anti-terrorist and national security legislations. Along with the technological advancement national security agencies gained an opportunity to quickly and easily obtain a great amount of information about citizens and States are now able to conduct a broad-scale surveillance. Unfortunately, this was not accompanied by the development of instruments allowing for the effective protection of journalistic secrecy in the digital age (see section III of the brief to see the example of Polish legislation in this respect). This worrying trend has been noticed *inter alia* in the UNESCO report *World Trends in Freedom of Expression and Media Development. Special Digital Focus*[2]. According to the report, "there has been significant change in the realm of legal protections for journalists' sources between 2007 and mid-2015. There has been a partial trend towards preliminary recognition of challenges in terms of international actors, but there is less recognition of the issue at national state level. The developments recorded in the past eight years in 69% of States (84 countries from 121) are generally in directions that run counter to robust source protection in the digital era. The legal frameworks that support protection of journalists' sources are under significant strain in the digital era, with this protection unnecessarily subjected to collateral damage in the face of broader security trends which could result in a loss to societies of the benefits of this particular dispensation"[3]. As a result, more and more journalistic communications is being collected by the enforcement and intelligence agencies which puts at risk both journalists and their sources. Furthermore, there is a real danger that the data collected are used not only for the sake of public security. According to the Report on the US NSA surveillance programme prepared by Committee on Civil Liberties, "data collection of such magnitude leaves considerable doubts as to whether these actions are guided only by the fight against terrorism, since it involves the collection of all possible data of all citizens; points, therefore, to the possible existence of other purposes including political and economic espionage, which need to be comprehensively dispelled"[4].

2. Mass surveillance as a threat to journalistic secrecy

The potential threat to the privacy of journalists' communication and data related to mass surveillance is of unprecedented scale and calls into question the ability to protect anonymous sources in the digital age. Undoubtedly, if journalistic sources are not provided with sufficient guarantees with regard to their confidentiality, there is a risk, that they will refrain from divulging significant information they possess. The ECtHR underlined on many occasions the significance of the protection of journalistic sources of information for the exercise of freedom of expression. In *Goodwin v. United Kingdom* case it stated, that "without such protection, sources may be deterred from assisting the press in informing the public in

---

[2] UNESCO, "World Trends in Freedom of Expression and Media Development. Special Digital Focus 2015", UNESCO Publishing, 2015 http://unesdoc.unesco.org/images/0023/002349/234933e.pdf (access: 4 February 2016)

[3] Ibid, p. 92.

[4] Committee on Civil Liberties, Justice and Home Affairs, "Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs", 2014, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//EN (access: 5 February 2016).

matters of public interest. As a result the vital public watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected"[5].

The protection of journalistic sources of information is undermined not only when the content of communication is a subject to surveillance, but it is sufficient to monitor the metadata related to such communication. Examination of metadata, such as telephone billings, location data or data concerning the activity on the Internet (for example the history of visited websites, web searches, e-mail addresses of people with whom the journalist corresponded) raises serious concerns because it allows *inter alia* for verification of the circle of the journalist's interlocutors and consequently allows for identification of journalistic informants. In this respect the journalistic secrecy is even more sensitive than lawyers' secrecy as the information revealing the sole fact of the communication, and not necessarily its content, is sufficient to disclose the source of information which constitutes a central element of any journalistic shield laws. That is why it has been already established in the Polish legal doctrine that, for example, a document containing the telephone billings obtained from a telecom operator, should be considered a document containing information protected by the journalistic secrecy[6].

Moreover, it should be underlined that the mass surveillance instruments lead to a situation in which the confidential information can be acquired without journalists' knowledge and control. The authorities do not have to approach the journalist to compel him to disclose information, but instead can refer directly to telecom operators or ICT companies. Thus the journalist, not being a "party" to this process, is not able to invoke his right to confidentiality. As consequence, the sources of information, who know that law enables the authorities to reach for confidential data without the journalists' control, cannot fully rely on the journalists' promise to guarantee them anonymity. Such situation undermines the trust between the journalist and his source and – understandably - may strongly discourage sources to disclose any important information to media which could expose them to the risk of harm. Therefore it is crucial that any action of the authorities which may hinder the protection of journalistic sources, regardless of whether they engage the journalists themselves or any other actors such as telecom operators and ICT companies, should be in principle inadmissible. As recommended by the Committee of Ministers of the Council of Europe, any interception, surveillance and other digital searches "should not be applied if their purpose is to circumvent" source protection[7]. The guarantees protecting the journalistic secrecy may be thus effective only if they are applied with regard to any entity that is *de facto* in possession of the confidential information.

Such approach is in line with the earlier ECtHR jurisprudence concerning protection of journalistic sources. The ECtHR has previously stressed that any efforts to establish the identity of journalistic sources without the journalists' knowledge should be considered as the most dangerous, depriving the journalists any control over the disclosure of confidential information (see *Roemen and Schmitt v. Luxembourg*[8], *Ernst and others v. Belgium*[9]). The case of *Bureau of Investigative Journalism and Alice Ross* provides

---

[5] Judgement of the European Court of Human Rights in the case of *Goodwin v. the United Kingdom* of 27 March 1996, application no. 17488/90 , § 39.

[6] A. Bojańczyk, „Billingi jednak na specjalnych prawach", Rzeczpospolita, 01 December 2005.
J. Kondracki, K. Stępiński, „Billingi pod osłoną tajemnicy dziennikarskiej", Rzeczpospolita, 10 October 2010.

[7] Committee of Ministers, Recommendation No. R (2000) 7 of the Committee of Ministers to member states on the right of journalists not to disclose their sources of information, appendix, principle 6 (a).

[8] Judgement of the European Court of Human Rights in the case of *Roemen and Schmit v. Luxembourg* of 25 February 2003, application no. 51772/99.

[9] Judgement of the European Court of Human Rights in the case of *Ernst and Others v. Belgium* of 15 July 2003, application no. 33400/96,

the ECtHR with an opportunity to further develop this standard, by addressing precisely the most current and pressing challenge in the area of journalistic source protection.
It should be also noted that surveillance of electronic communication has been already considered a leading contemporary threat to the confidentiality of the journalistic sources by numerous international human rights institutions, as well as journalistic organisations. The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression explicitly emphasized in one of his reports[10] that "the ubiquitous use of digital electronics, alongside government capacity to access the data and footprints that all such devices leave behind, has presented serious challenges to confidentiality and anonymity of sources and whistle-blowers[11]. The problem of unintended self-disclosure has been a recurrent feature in the leading cases involving journalistic sources in recent years, in which the Government of the United States of America discovered probable source identities through telephone and e-mail records[12]. Writers themselves report concern that their ability to protect sources is much diminished in the face of surveillance"[13]. Similarly in the already quoted UNESCO report it was stated that "transparency and accountability regarding both mass and targeted surveillance, and data retention, are critically important if confidential sources are to be able to continue to confidently make contact with journalists"[14]. The importance of protection of journalistic sources in the digital age was moreover recognized by bodies such as: UN Human Rights Council[15], UN General Assembly[16], High Commissioner for Human Rights[17], Committee on Civil Liberties, Justice and Home Affairs[18] Organization for Security and Cooperation in Europe[19] and Committee to Protect Journalists[20].

Finally, it should be stressed that media play one of the crucial roles in the system of general oversight of the use of mass surveillance in a democratic society. This role has been explicitly underlined in the recent report of the Fundamental Right Agency of the European Union *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Mapping Member States' legal frameworks*[21]. Media reports disclosing unlawful surveillance were considered one of the effective tools for enforcing the limits placed on surveillance. The report explains that in light of lack of independent control over the

---

[10] Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report no. A/70/361, 08 September 2015.
[11] J. Posetti, "Protecting journalism sources in the digital age", UNESCO Publishing 2015.
[12] See, for example, *United States of America v. Sterling*, 724 F.3d 482, 2013.
[13] See PEN America, "Chilling effects: NSA surveillance drives U.S. writers to self-censor", New York, 2013; and Human Rights Watch and American Civil Liberties Union, "With liberty to monitor all: how large-scale U.S. surveillance is harming journalism, law and American democracy", New York, 2014.
[14] Op. cit.
[15] Human Rights Council: Resolution on the safety of journalists no A/HRC/RES/21/12, 09 October 2012; Resolution on the promotion, protection and enjoyment of human rights on the Internet no. A/HRC/RES/20/8, 16 July 2012; Resolution on the Safety of Journalists no. A/HRC/RES/27/5, 02.10.2014.
[16] General Assembly: Resolution on the Safety of Journalists and Issue of Impunity no. A/RES/68/163, 18 December 2013; Resolution on the Right to Privacy in the Digital Age no. A/C.3/68/167, 2013.
[17] High Commissioner for Human Rights, Report on the right to privacy in the digital age no. A/HRC/27/37, 30 July 2014.
[18] Committee on Civil Liberties, Justice and Home Affairs, "Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs", 2014.
[19] OSCE, "OSCE Safety of Journalists Guidebook", 05 December 2011, http://www.osce.org/fom/85777%20?download=trues (access: 4 February 2016).
[20] Committee to Protect Journalists, "Balancing Act: Press freedom at risk as EU struggles to match action with values, A Special Report of Committee to Protect Journalists", 2015, https://www.cpj.org/reports/cpj_eu_special_report_2015.pdf (access: 5 February 2016).
[21] FRA, "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU", 2015, http://fra.europa.eu/sites/default/files/fra_uploads/fra-2016-surveillance-intelligence-services_en.pdf (access: 08 February 2016).

use of mass surveillance in many countries "independent journalists and whistle-blowers play an essential 'intermediary' role in facilitating access to remedies. The Snowden revelations provide a good example of this since they led to both national and international litigation.". Therefore the lack of effective safeguards protecting journalists against surveillance, not only puts at risk their ability to safely cooperate with their sources, but also undermines the whole mechanism of authorities' accountability for potential abuses.

3. Practical impact of the mass surveillance on the protection of journalistic sources

Due to the secret nature of surveillance it is hard to determine the actual scale of the problem specifically with regard to the representatives of media. However the negative impact of the mass surveillance on the journalistic work can be already observed on the basis of individual cases (see the example described in the section III) or in the studies conducted among media practitioners. They reveal that journalists feel vulnerable to surveillance which already led some of them to change their behaviour as regards storing sensitive information or communicating with their sources.

According to the study[22] prepared by the team from PEW Research Center in association with Columbia University's Tow Center for Digital Journalism carried out in 2014, among 671 members of Investigative Reporters and Editors, almost two-third of respondents (64%) believe that U.S. government has collected their communication data and eight-in-ten believe that being a journalist make it more probable that such data will be collected. The group that is particularly likely to believe that the government obtained these data already are journalists reporting on national security, foreign affairs and the federal government. Because of these concerns, many of them have altered their behaviour during 2014 (49% changed the way they store or share sensitive documents, 29% altered the way they communicate with other reporters, editors or producers). Additionally, among 454 journalists who identified themselves as reporters, 38% admitted that they changed the way they communicate with sources. Overall, fortunately not many journalists said that concerns about surveillance have eventually changed the stories or sources they pursued. Still those who identified themselves as reporters admitted they feel an impact of mass surveillance programmes when it comes to their sources' willingness to share information. A vast majority (71%) of respondents also said they do not have confidence to external protection from digital threats provided by their internet providers. At the same time about half of those who work for news organizations reported getting no formal training or instructions on electronic security issues from professional sources.[23]

III. Mass surveillance and protection of journalistic sources in Poland

As already mentioned earlier, in the course of the work of the "Observatory of Media Freedom in Poland" the HFHR monitors the instances of the use of surveillance tools with regard to journalists in Poland, case law of national courts in this respect, as well as any legal developments in this area. In this section of the brief we would like to present our observations to the Court, hoping they may be useful for the resolution of the case in question.

1. Legal context in Poland

[22] Pew Research Center in association with Columbia University's Tow Center for Digital Journalism, "Investigative Journalists and Digital Security. Perceptions of Vulnerability and Changes in Behavior", 05 February 2016, http://www.journalism.org/files/2015/02/PJ_InvestigativeJournalists_0205152.pdf (access: 5 February 2016).
[23] Ibid.

The legal provisions protecting journalistic sources of information are quite strong in the Polish law. First of all, the Polish Constitution grants the right to privacy, secrecy of communication and informational autonomy (Articles 47, 49, 51), as well as the freedom of expression (Article 54). Secondly, more specific provisions on source protection are provided in the Article 15 and 16 of the Press Law Act. There is also specific regulation on journalistic secrecy in the Criminal Procedure Code which applies within the criminal proceedings (Article 180). Pursuant to the Press Law Act, a journalist is obliged to keep confidential: (a) any data making it possible to identify the author of material appearing in the press, a letter to the editor or other material of a similar nature, published or released for publication, if such persons demanded that such data remained confidential and (b) any information the disclosure of which could prejudices the interests of third parties protected by law. According to the Press Law Act the journalist may only disclose the source if they allow for revealing their identity. Moreover the journalist shall be exempted from keeping professional secrecy in this respect only if the information concerns one of the most serious crimes enumerated explicitly in the Article 240§1 of the Criminal Code. As regards the Criminal Procedure Code, it provides a general prohibition to disclose data enabling identification of the author of press denunciation, letter to the editor or other material of the same nature, as well as identification of persons imparting information published or passed to be published, if these persons reserved the right to keep the data secret. The journalist may be exempted from keeping the journalistic source of information confidential only (1) if required to reveal it by the court order, (2) when it is necessary for the benefit of the administration of justice, (3) the facts cannot be established on the basis of other evidence and (4) the information is needed for the purposes of proceedings concerning one of the most serious crimes enumerated explicitly in the article 240§1 of the Criminal Code (all the four conditions have to be met simultaneously).

At the same time, the Polish legal order lacks adequate safeguards against abusing the competences of intelligence agencies with regard to the mass surveillance of communication, also with respect to journalists. The access to telecommunication data stored by telecom providers is possible on the grounds of the Telecommunications Law in connection with particular legislative acts concerning relevant intelligence services which provide detailed regulations in this respect (these regulations transposed the invalidated UE's Data Retention Directive to the domestic legal order). So far, as regards the use of data stored by telecom providers, the law has not provided for judicial or any other independent, external control (neither *ex post* nor *ex ante*) over the access and use of such data. The surveillance has been possible for a broad range of purposes of performing any statutory duties of particular intelligence services (there has been no legal threshold for seriousness of a crime). There has been no requirement of notification of the person whose data were acquired (even once the proceedings were completed). Data subject's right to access has been denied as well. As consequence, individuals have had very limited possibilities to use legal remedies in case of an abuse of powers of intelligence services with regard to the use of telecommunications data stored by telecom providers as most often they would never find out about the fact that their data were acquired by competent authorities. Only in case of some of the enforcement or intelligence agencies there has been a specific obligation to destroy data once they were no longer needed for the purpose for which they have been acquired. The enforcement and intelligence agencies have had accessed telecommunications data at no cost (all costs generated by data retention regime have been covered by telecom providers) and often directly through simple interfaces established on telecommunications networks. What is more, the legal provisions concerning data retention have not contained any specific provisions preventing from violation of the guarantees protecting professional secrecy rules (such as journalistic shield laws or professional privilege of lawyers). Therefore in practice, despite the existence of general provisions protecting the journalistic sources, they could be easily circumvented due to very broad surveillance competences of enforcement and intelligence agencies. This legal framework, as well as the practice of the intelligence services with regard to the use of telecommunication data, was criticized by many Polish human rights NGOs and other bodies such as

Human Rights Defender[24] (*Rzecznik Praw Obywatelskich*), Supreme Bar Council[25] (*Naczelna Rada Adwokacka*), Prosecutor General[26] (*Prokurator Generalny*) or Supreme Audit Office[27] (*Najwyższa Izba Kontroli*).

On 30 July 2014 the Polish Constitutional Tribunal found the data retention regulations incompatible with constitutional right to privacy, including the violation of the information autonomy rights and correspondence secrecy, in particular to extent that they did not foresee any independent supervision over the use of these data by the enforcement and intelligence agencies (case no. K 23/11). One of the significant spheres touched upon by the Constitutional Tribunal concerned the necessity to destroy materials, which contain professional secrets (including journalistic secrecy). According to the Tribunal, the law on surveillance was unconstitutional to extent that did not guarantee immediate removal of such materials with regard to which the court had not lifted the professional privilege. The deadline to adopt a new regulations established by the Constitutional Tribunal was 7 February 2016.

In response to this Constitutional Tribunal's judgment the new law was adopted by the Polish Parliament in January 2016 and entered into force on 7 February 2016. Unfortunately it does not address most of the problems highlighted above in the context of the previous regulations and still does not provide sufficient safeguards against arbitrary use of mass surveillance of telecommunication data. The oversight mechanism which the new law introduces is considered to be far from effective[28]. Moreover it extends the surveillance mechanisms to the "Internet data", broadening the current competences of enforcements and intelligence agencies to encompass metadata concerning the citizens' activity on the Internet related to the use of electronic services. The first draft of the new law proposal did not contain any guarantees safeguarding professional secrecy in the context of mass surveillance. In the course of the parliamentary works this problem was eventually acknowledged and certain amendments were introduced. Unfortunately, as underlined by the Polish Chamber of Press Publishers[29] in their statement concerning the new regulations, they do not provide effective protection for journalists. Pursuant to the new provisions, all the materials which will be regarded as containing professional secrets should be delivered to the prosecutor, who later should hand them to the court. The court will then decide on the matter of admissibility of those materials. There are two main concerns with respect to the adopted regulation. First of all it is not clear why the materials should be delivered to the prosecutor in the first place and not the court directly (while the prosecutor does not have any power to order to destroy materials and what he does is simply handing them to the court). The second, more serious concern regards the arbitrariness of the decision of the agency conducting surveillance on whether the materials include professional secrets

---

[24] Human Rights Defender (*Rzecznik Praw Obywatelskich*), Wniosek do Trybunału Konstytucyjnego, RPO-662587-II-II/ST, 1 August 2012.

[25] Supreme Bar Council, "*Konferencja pt. Retencja danych: troska o bezpieczeństwo czy inwigilacja obywateli? Polak najbardziej inwigilowanym obywatelem Europy?*", 6 May 2011, http://archiwum.adwokatura.pl/?p=3396 (access: 02 February 2016).

[26] Prosecutor General (*Prokurator Generalny*), PG VII TK 62/11, 28 October 2011.

[27] Supreme Audit Office (Naczelna Izba Kontroli), „Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne", Report, 8 October 2013.

[28] Every six month, the competent agencies are obliged to provide the court with the report on the obtained data. The report should contain the following information: number of cases in which the data were asked for, types of those data, types of criminal offences, which were grounds for the decision to obtain information. The control will however be only of a facultative nature and will not be mandatory. The court will have a right (and not obligation) to carry it out. Afterwards the court is supposed to inform the agencies, which were subject to supervision on the control results, but it will not have any power to enforce the deletion of data.

[29] Polish Chamber of Press Publishers (*Izba Wydawców Prasy*), "Stanowisko Izby Wydawców Prasy w sprawie projektu nowelizacji ustawy o Policji i niektórych innych ustaw", 13 January 2016.

of any kind (the authority will have a wide discretion in this respect) and therefore whether at all should be submitted to the prosecutor and then to the court. The official checking the data would have access to the data and would decide upon their destruction due to protection of journalistic sources. The information he or she would access, would not be erased from their memory. The new law still does not provide any *ex-ante* independent control on the acquisition of data containing journalistic secrets or the principle of subsidiarity (providing that data containing professional secrecy could be acquired only when it is necessary for the proper administration of justice and when all other methods which do not involve disclosure of journalistic secrecy have been exhausted). In general the new law again has been a subject to criticism by many NGOs[30], including HFHR[31], but also some public institutions such as the Polish Human Rights Defender[32], Data Protection Authority[33] or Ministry of Digitization[34].

2. Surveillance of journalists in Poland

The use of both targeted and mass surveillance instruments against journalists is not only a hypothetical situation. Several instances of such abuses were confirmed in recent years in Poland. Apart from a few cases in which media practitioners were wiretapped[35], there were at least 13 revealed cases of journalists whose telecommunication data (metadata) were secretly acquired and analyzed by enforcement and intelligence agencies without any judicial authorization[36].

One of such cases was disclosed in 2010 when the Polish newspaper "Gazeta Wyborcza" revealed that mobile phone billings of 10 high-profile journalists had been repeatedly accessed by intelligence agencies for no particular reason, in some cases over a period of many months[37]. The case was accidently discovered by one of the newspapers' journalists when investigating court files of another case. One of the journalists affected by the surveillance - B.W. - filed a civil suit concerning protection of personal rights with the national court against the Central Anti-Corruption Bureau (CBA), one of the intelligence agencies which accessed his telecommunication data. The journalist was known for writing about public security issues, including some scandalous operations of the CBA. He stated in his suit that CBA had unlawfully accessed his telecommunications data, including phone records and location data for 6 months between 2005-2007. The journalist claimed that CBA infringed his constitutional rights including the right to privacy, freedom of communication and, above all, the right to the freedom of expression because it posed a threat to the confidentiality of journalistic sources. In the course of the court proceedings the journalist claimed that as a result of surveillance he felt he had lost the trust of some of his sources and acquaintances. They would refuse to talk to him on the phone, worrying that it can be tapped or otherwise monitored. He believed that the surveillance of his telecommunication data clearly undermined his

---

[30] Panoptykon Foundation, „Stanowisko Fundacji Panoptykon w sprawie projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk sejmowy nr 154)", 27 December 2015.
[31] Helsinki Foundation for Human Rights, „Uwagi Helsińskiej Fundacji Praw Człowieka do poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk sejmowy nr 154)", 30 December 2015.
[32] Human Rights Defender (*Rzecznik Praw Obywatelskich*), „Wystąpienie w sprawie poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk sejmowy nr 154)", 29 December 2015.
[33] Data Protection Authority (*Generalny Inspektor Ochrony Danych Osobowych*), „Opinia do poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk sejmowy nr 154)", 30 December 2015.
[34] Ministry of Digitization (*Ministerstwo Cyfryzacji*), „Uchwała nr 10 Rady do Spraw Cyfryzacji w sprawie projektu nowelizacji ustawy o Policji", 07 January 2016.
[35] See for example M. Duda, "Inwigilacja dziennikarzy? Policja przekazuje materiały prokuraturze", 01 December 2016, http://www.tvn24.pl/wiadomosci-z-kraju,3/policja-przekazala-materialy-prokuraturze-ws-podsluchow-dziennikarzy,615457.html (access: 08 February 2016),
[36] Currently investigation is pending over the monitoring of phone conversation of dozen of journalists and their families. The surveillance was imposed after a political affair in 2014.
[37] W. Czuchnowski, „Dziennikarze na celowniku służb specjalnych", op. cit.

reputation as a reliable journalist. The HFHR participated in the proceedings before the courts as a third-party in the trial.

The Polish courts of the first and second instances stated that, by accessing the journalist's phone records, the intelligence service had clearly interfered with his constitutional rights, both the right to privacy and the freedom of expression[38]. The courts emphasized that such interference should be possible solely when it is clearly permissible under the law, appropriately justified and proportionate in comparison to the benefits expected to be obtained (ex.: in case of a serious crime). In this case the courts confirmed that the journalist was not put under surveillance as a person suspected of any crime or even in connection with any particular investigation. At the same time the measure used with regard to the journalist deeply interfered with his right to private life as the acquisition of his telecommunication data enabled the CBA to gain knowledge about the claimant's phone connections, including their duration, the numbers he connected with, as well as his locations and locations of his interlocutors. Since the surveillance lasted for certain period, it also allowed for identification of some of the journalist's life patterns. Finally, the courts confirmed that the journalists' phone billings should be protected under the regulations concerning the journalistic shield laws. The District Court in Warsaw emphasized that „by accessing the journalist's telecommunication data, CBA used a legal instrument, that was both convenient for the CBA, because it did not involve much effort and an instrument that did not provide many safeguards for the person concerned, because (…) the CBA did not have the obligation to notify the claimant about the surveillance, neither it had to ask for the court's warrant.(...) The CBA's conduct was not lawful and it constituted a circumvention of law with regard to the guarantees protecting journalists which is unacceptable". The CBA was obliged to publish an apology to the journalist in the press and was ordered destroy the illegally acquired telecommunication data concerning the plaintiff.

The presented case has precedential character and a great significance for the protection of journalistic sources of information in the context of secret mass surveillance of metadata. What should be underlined however, is that it is a rare example of a case in which the victim could effectively question the surveillance before the court. As mentioned above, the fact that B.W. was subject to surveillance was discovered accidently by another journalist who then disclosed the information in the press article. Otherwise B. W. would most probably never learned about the fact of surveillance, and thus would not be able to seek any remedy. That is because the Polish law did not provide at the time (and still does not under the new regulations) for even an *ex-post* obligation to notify the persons that they were subject to secret surveillance. Consequently it is difficult, under normal circumstances, to question the lawfulness of such surveillance before the court. The victims' access to effective remedy is therefore very limited, unless they manage to find out about the surveillance and provide sufficient evidence before the court thanks to some extraordinary circumstances. In this context a very important principle has been established recently by the ECtHR in the case of *Roman Zakharov v. Russia* (application no. 47143/06). The ECtHR stated that "the applicant is entitled to claim to be the victim of a violation of the Convention, even though he is unable to allege that he has been subject to a concrete measure of surveillance in support of his application. For the same reasons, the mere existence of the contested legislation amounts in itself to an interference with the exercise of his rights under Article 8"[39]. That is why if the domestic law does not provide sufficient safeguards against arbitrary use of surveillance tools, the potential victims, and in

[38] The judgment of the Regional Court in Warsaw, case no. II C 626/11 (first instance court), The judgment of the Appellate Court in Warsaw, case no. I ACa 1002/12 (second instance court, final judgement). Both judgements has been translated in English and are available online at:
http://www.obserwatorium.org/index.php?option=com_content&view=article&id=4497:-angielskie-tumaczenie-wyrokow-ws-red-wroblewskiego-p-cba-&catid=40:zkraju&Itemid=34

[39] Judgement of the European Cour of Human Rights in the case *Roman Zakharov v. Russia*, application no. 47143/06, § 179.

particular members of the vulnerable groups such as journalists, should be able to question the lawfulness of such surveillance without being required to provide the concrete evidence which is often impossible to obtain.

IV. Conclusions

In Europe one may observe the trend to empower enforcement and intelligence agencies with more and more surveillance competences. It is therefore very important that these changes be accompanied by the development of adequate safeguards for citizens aimed at preventing disproportionate interference with their fundamental rights. Journalists are one of the most vulnerable groups in the context of the arbitrary use of mass surveillance. In their case it is not only the right to private life that is at risk, but at the same the freedom of expression. Mass surveillance instruments pose the most serious contemporary threat to the confidentiality of journalistic sources of information which is crucial for the media's "public watchdog" role. It should be also noted in this respect that, as far as the journalistic secrecy is concerned, the protection of metadata is as important as the protection of the content of journalists' communication.

The ECtHR's judgement in the case of *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom* may therefore have an important impact on setting standards for journalistic source protection in the digital age. Such standards might help law makers and human rights advocates in shaping appropriate guarantees for journalistic secrecy in national laws, as well as provide useful guidelines for domestic courts which – as we presume - may be confronted with this kind of cases more and more often.

This third-party intervention has been prepared by Dorota Głowacka and Marcin Sczaniecki, lawyers of the HFHR's "Observatory of Media Freedom in Poland" programme.

On behalf of the Helsinki Foundation for Human Rights,

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

Helsińska Fundacja Praw Człowieka
SEKRETARZ ZARZĄDU
Piotr Kładoczny

Dr Piotr Kładoczny
Secretary of the Board
of the Helsinki Foundation for Human Rights