# “IT’S ENOUGH FOR PEOPLE TO FEEL IT EXISTS”

CIVIL SOCIETY, SECRECY AND SURVEILLANCE IN BELARUS

AMNESTY INTERNATIONAL

**Amnesty International is a global movement of more than 7 million people who campaign for a world where human rights are enjoyed by all.**

**Our vision is for every person to enjoy all the rights enshrined in the Universal Declaration of Human Rights and other international human rights standards.**

**We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and public donations.**

© Amnesty International 2016
Except where otherwise noted, content in this document is licensed under a Creative Commons (attribution, non-commercial, no derivatives, international 4.0) licence.
https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode
For more information please visit the permissions page on our website: www.amnesty.org
Where material is attributed to a copyright owner other than Amnesty International this material is not subject to the Creative Commons licence.
First published in 2016
by Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, UK

**Index: EUR 49/4306/2016**
**Original language: English**

amnesty.org

***Cover photo:*** *Minsk, Belarus*
*© Maxim Sarychau*

AMNESTY INTERNATIONAL

# CONTENTS


**1. EXECUTIVE SUMMARY** 6

**2. METHODOLOGY** 10

**3. BACKGROUND** 11

3.1 Restrictive Legal Framework for Civil Society 11

3.2 Online Media and Human Rights Online 11

**4. A CHILLING EFFECT: LIVING WITH SURVEILLANCE** 13

4.1 A Widespread Suspicion of Surveillance 14

Use of Surveillance in the Crackdown Following the 2010 Elections 15

4.2 How to communicate 18

4.3 How to meet 19

4.4 Importance of encryption 19

4.5 Phone location/Listening 20

4.6 Bugging/Physical Surveillance 22

4.7 Hacking 23

4.8 Confiscation 28

4.9 Chilling Effect: Conclusion 29

**5. INTERNATIONAL HUMAN RIGHTS LAW AND SURVEILLANCE** 32

**6. COMMUNICATIONS SURVEILLANCE IN BELARUS: LAW AND PRACTICE** 34

6.1 Direct Access to Communications Data 34

6.2 Data Retention 36

6.3 Scope of Application of Secret Surveillance measures 37

6.4 Accessibility of Domestic Law 38

6.5 Authorization of Surveillance Measures 38

6.6 Supervision of Surveillance Measures 39

6.7 Duration of secret surveillance 40

6.8 Treatment of Data 41

6.9 Notification of Surveillance 41

6.10 Remedies 42

**7. ROLE OF PRIVATE COMPANIES** **45**

**8. CONCLUSION** **48**

**9. RECOMMENDATIONS** **49**

9.1 To the Executive and Legislative Branches of Government of Belarus: 49

9.2 To Prosecutors: 50

9.3 To Authorities Carrying out Operational Search: 50

9.4 To Telecommunications Companies: 51

# GLOSSARY

| | |
|---|---|
| IP ADDRESS | UNIQUE ADDRESS THAT IDENTIFIES AN ADDRESS ON THE INTERNET OR A LOCAL NETWORK |
| IMEI NUMBER | International Mobile Equipment Identity: a number used to identify a mobile phone |
| IMSI NUMBER | International Mobile Subscriber Identity: a number used to identify a mobile subscriber |
| MAC ADDRESS | A unique hardware identifier permanently assigned to a computer's network adapter at the time of manufacture |
| METADATA | Data that accompanies digital communication that is not the content of the communication. Examples include, but are not limited to: the sender and recipient of communications, time of communications, or location of sender or recipient |
| PROXY SERVER | A server that acts as an intermediary for requests from clients towards other servers (typically web servers). A proxy server may be used to record or modify the content of websites requested through it. |
| VPN | Virtual Private Network: A technology used to create a secure, encrypted, network connection between computers over an untrusted public network (such as the internet). |

| | |
|---|---|
| KGB | Abbreviation for the State Security Committee of Belarus, the national intelligence agency. |
| OMON | Abbreviation for the Special Purpose Police Unit |
| OAC | Abbreviation for the Operations and Analysis Centre, the agency under the President in charge of protection of information and state secrets who play a large role in regulating internet-related issues in Belarus, including surveillance |

# 1. EXECUTIVE SUMMARY

The legal framework governing secret surveillance in Belarus is characterized by inadequate safeguards, and allows the authorities to undertake wide-ranging surveillance with little or no justification. While it is possible that almost anyone could be subject to surveillance, it is nearly impossible for anyone to know whether they are or have been. This uncertainty exerts a chilling effect on human rights defenders, opposition politicians, lawyers and activists, and limits their ability to exercise their human rights, including the rights to privacy, freedom of association, peaceful assembly and expression.

While secret surveillance can be a legitimate tool for law enforcement, where it lacks adequate safeguards or supervision, or otherwise fails to adhere to international law and standards, it violates human rights. This report examines the ways in which unlawful secret surveillance affects human rights, and the effect this has on civil society in Belarus. The report is based on interviews with more than fifty civil society activists, the majority in Belarus, but also in exile. It is also based on a detailed examination of the Belarusian and international legal framework governing surveillance.

The system of surveillance in Belarus has many problematic aspects. Prominent among them is the SORM system, a set of standardised technical means for interception of communications which allows the authorities direct, remote-control access to all user communications and associated data without notifying the providers. Under Belarusian law, all telecommunications providers in the country must make their hardware compatible with the SORM system. The system facilitates real-time monitoring of communications as well as access to data which telecoms are required by law to retain for up to five years. It provides access both to the content of communications and the associated metadata (data such as the time, manner or location of communication).

This problematic surveillance system is facilitated by corporate actors, such as mobile telephone or internet providers, who – according to Belarusian law – are required to allow the authorities direct access to their customers' data. These Belarusian companies, and the international companies that are their owners or major shareholders, are failing (in violation of their obligations) to identify, prevent, and address human rights abuses resulting from their operations, or arising from their business relationships. As such, they are in violation of international standards on business and human rights. Companies must take positive steps to fulfil their human rights responsibilities, regardless of where they choose to operate. These steps must be commensurate to the threat of harm that people face as a result of their operations.

Surveillance of telecommunications is not the only surveillance risk Belarusians face. The right to privacy is also at risk because the law allows broad powers of physical surveillance, including audio monitoring of people or premises, and because personal data may be compromised when computers, mobile phones, or other devices are confiscated by the authorities. The lack of transparency regarding the state's surveillance capabilities means ultimately no one knows the full range of tools and techniques available to the authorities.

Secret surveillance is carried out by a wide array of state agencies and authorized on the basis of a number of broad and vague legal grounds. It can be used, as a matter of domestic law, to subject to surveillance people who are not suspected of any wrongdoing. Authorization and supervision safeguards are inadequate, and usually carried out by prosecutors, rather than an independent judicial body.

Where surveillance leads to violations of human rights, it is extremely difficult to seek remedies in practice. This is especially true since the authorities are not required to notify individuals that they have been subjects of surveillance once the surveillance has ended - even when such notification could be given without jeopardising the purpose of investigations. Consequently individuals rarely have access to evidence with which to sustain a complaint. Almost none of the activists who believed they had been subject to unlawful surveillance had been able to bring a complaint. Of those who had, almost none believed their complaints would be successful, and often sought to obtain them only as a protection against being prosecuted themselves.

While Belarus' legal framework makes it nearly impossible for anyone to know with certainty whether they may be or have been subject to surveillance, Belarus' recent history gives many activists reason to think they are.

The crackdown by authorities that followed the 2010 presidential elections was characterized by arrests and imprisonments of political opposition members for exercising their human rights. Many of these well-publicized prosecutions were characterized by the prominent use of personal communications and associated data, and the media widely reported that mobile phone location data was used by the authorities to determine the identities of people who had attended the unregistered – but largely peaceful – demonstrations that followed the elections.

In part because of this, activists who spoke to Amnesty International uniformly expressed the belief that they were subject to at least some form of secret surveillance as a result of their activism. This fear of surveillance is exacerbated by the restrictive legal environment for civil society in Belarus, with activists regularly facing punishment merely for exercising their human rights - such as by attending a peaceful protest - and the increasingly harsh limits on human rights exercised online. All of this creates a chilling effect that has led many to self-censor and to refrain from exercising their rights in many cases.

The activists interviewed by Amnesty International said that generally they do not discuss sensitive topics on the phone – topics such as financing an unregistered organization or organizing a peaceful protest, both of which can lead to criminal charges. Even normally mundane organizational tasks such as arranging meetings involve elaborate systems of coded language and generally require people to meet in person, often outdoors, without mobile phones that could record their conversations or track their locations. The fear of surveillance of digital communications also makes the use of encryption tools, including PGP (a system for encrypting e-mail), encrypted chat programmes and disk encryption, essential to the work of activists.

Activists reported experiences – such as being stopped by police who seemed to know where to find them – that they attributed to surveillance of their mobile phone location data. Given the problematic legal framework in Belarus however, they are not able to confirm such suspicions, leaving most people no option but to presume their locations are being tracked.

Some activists feared their offices or even their homes may be subject to audio or video monitoring, which prevents them from carrying out sensitive work in their own offices, significantly hindering their ability to work.

Amnesty International spoke to three activists who said they believed their e-mail or social media accounts had been hacked. They suspected the authorities may have been behind the attacks, suspicions they said were increased when their personal data used to threaten or prosecute them. More commonly, activists had had computers or other equipment confiscated by the authorities, with the result that they were unable to continue working with their equipment, even after it was returned, for fear it may have been infected with software to monitor their use.

Internet use in Belarus has increased rapidly in recent years. In 2014, internet penetration stood at 59%, up from 39.6% in 2011.[1] Despite this, the risk and uncertainty of communications surveillance makes the work of Belarusian activists more difficult. Activists are not able to take advantage of increased connectivity. Instead, because of the chilling effect that the fear of surveillance creates, communications are slowed, flow of information is restricted, organizing is stymied and trust is impaired.

[1] http://data.worldbank.org/indicator/IT.NET.USER.P2

Because of the problematic legal framework governing surveillance in Belarus, everyone is forced to live as if they under surveillance, with a detrimental impact on rights. While the current scale of surveillance cannot be known, the impact of its past misuse is clear: well-publicized cases of the authorities using communications data to prosecute opposition politicians and human rights defenders following the 2010 elections continue to be cited as a reason people fear surveillance. The cases described by activists who spoke to Amnesty International indicate that they continue to be subject to secret surveillance.

The Belarusian authorities must urgently revise laws governing secret surveillance to bring them in line with international standards. For instance, they must ensure that surveillance can only be undertaken when authorized (and overseen) by independent judges on the basis of sufficiently narrow grounds, taking into account the need for individualised reasonable suspicion of wrongdoing and the requirements of necessity and proportionality. The SORM system must be replaced with one that does not allow direct access to communications data. Prosecutors must not seek to subject people to surveillance for the exercise of their human rights, such as organizing peaceful protests. Prosecutors and authorities conducting surveillance must be more transparent about the number of instances in which surveillance is authorized and undertaken. People who have been subject to surveillance must be provided with notification, and with effective access to remedies for human rights violations linked to this surveillance. Private companies facilitating surveillance in Belarus must challenge unlawful government surveillance practices, push for their reform and be more transparent about the law and practice governing access to customer data in Belarus.

Additional recommendations are included at the end of this report.

# 2. METHODOLOGY

This report is based on interviews with more than 50 activists, human rights defenders, journalists, lawyers, political opposition members, technology experts and others, many of them in exile. The majority of interviews were conducted in Minsk (Belarus), with others conducted in Vilnius (Lithuania) and Warsaw (Poland), between August and December 2015. Additional interviews were conducted, both remotely and in person, in London during 2016. In many cases, names of interview subjects, and some other identifying information, has been omitted or altered to protect the anonymity of sources.

Amnesty sent summaries of our findings and concerns, and sought information and comment from many government agencies, including both houses of the Parliament, the Office of the Prosecutor General, the Ministry of Internal Affairs, the Operations and Analysis Centre, the State Security Committee (KGB), the Border Service, the Financial Investigations Department of the State Control Committee, and the State Customs Committee. We received replies from the Financial Investigations Department of the State Control Committee and the State Customs Committee.

We also sent similar correspondence and sought information from mobile providers Life, MTS (Belarus) and Velcom, as well as their parent companies Telekom Austria Group, América Móvil, Teliasonera and Turkcell. We also wrote to Beltelecom and to the social network VK. We received replies from Teliasonera and Telekom Austria Group, and met by phone with representatives from Telekom Austria Group.

The responses we received are reflected in the report where relevant.

# 3. BACKGROUND

## 3.1 RESTRICTIVE LEGAL FRAMEWORK FOR CIVIL SOCIETY

As Amnesty International documented in its 2013 report *What is Not Permitted is Prohibited: Silencing Civil Society in Belarus*, civil society in Belarus generally operate in a restrictive legal environment that violates numerous internationally protected human rights.[2] Activists regularly face arrest, detention or imprisonment merely for exercising their human rights.

Non-governmental organizations (NGOs) in Belarus face numerous bureaucratic requirements which the authorities often use to refuse them registration, or to close them down for failure to comply with the requirements. For example, the Belarusian authorities have used these requirements to deny registration to NGOs on the basis of minor faults in documentation which could be easily remedied.[3] The Criminal Code prohibits activities by unregistered organizations, including political parties, religious groups and NGOs.[4]

The media is tightly controlled. Journalists who work with foreign media organizations are required to obtain government accreditation, which is often refused or delayed, and freelance journalists contributing to foreign media are subject to fines.[5]

Any public demonstrations or other protests must receive permission from local authorities, which they rarely granted. Participation in peaceful, but unauthorized, demonstrations can lead to fines or administrative detention.[6]

Other laws of general application also make the work of activists more difficult. 'Insult' or 'defamation' of the President or other authorities are criminal offenses.[7] Indeed, slander and insult in general are punishable by imprisonment, in contravention of international standards.[8]

## 3.2 ONLINE MEDIA AND HUMAN RIGHTS ONLINE

The climate for human rights online in Belarus is restrictive, even apart from the issue of surveillance.[9]

2 Amnesty International, What is Not Permitted is Prohibited: Silencing Civil Society in Belarus, EUR 49/002/2103, April 2013.
3 Amnesty International, What is Not Permitted is Prohibited: Silencing Civil Society in Belarus, EUR 49/002/2103, April 2013.
4 Amnesty International Report 2015/2016, Belarus, https://www.amnesty.org/en/latest/research/2016/02/annual-report-201516/
5 Amnesty International Report 2015/2016, Belarus, https://www.amnesty.org/en/latest/research/2016/02/annual-report-201516/; See also, Belarusian Association of Journalists, Fines to Journalists for Violating Article 22.9 of the Administrative Code (Chart) (Updated), https://baj.by/en/analytics/fines-journalists-violating-article-229-administrative-code-chart-updated
6 Amnesty International, What is Not Permitted is Prohibited: Silencing Civil Society in Belarus, EUR 49/002/2103, April 2013.
7 Criminal Code, Articles 367 - 369.
8 Criminal Code, Articles 188-9.
9 See, Index on Censorship, Belarus: Pulling the Plug (2013), https://www.indexoncensorship.org/2013/03/belarus-pulling-the-plug/

A new Law on Mass Media, passed in December 2014, grants the Ministry of Information the power to block access to web content without a court order. The law also creates liability for website owners for illegal user-generated content. As a result, some websites have shut down user comments sections, or have moved them to separate sites.[10]

During 2015, several popular websites of human rights groups or independent news sources – including Charter 97, Belarusian Partisan and Viasna - were blocked temporarily. The list of blocked sites is not public.[11]

A decision of the Operations and Analysis Center of the President (OAC) in February 2015 expanded the powers of the Ministry of Information to block websites, creating the legal framework to block not only prohibited content, but also anonymity tools that could be used to access blocked content, such as TOR or proxy servers or VPNs.[12] While such tools do not appear to have been blocked yet, the government does seem to have awarded a tender to company for a tool to search for and identify such anonymization tools.[13]

10 Interview with internet experts, Vilnius, August 2015; Interview with website owner, Minsk, December 2015.
11 http://www.belgie.by/ru/lists_access
12 See Box: Encryption and Anonymity Online, below.
13 https://baj.by/en/content/belarus-authorities-switch-automatic-blocking-anonymizers

# 4. A CHILLING EFFECT: LIVING WITH SURVEILLANCE

Fear of surveillance[14] is pervasive amongst civil society activists in Belarus, and even among many of those in exile. Inadequate regulation and oversight, and a lack of opportunity to challenge surveillance mean that activists have little choice but to assume they are under surveillance at any time. Because many legitimate activities - including working as a journalist without government accreditation, working for an unregistered organization or participating in peaceful demonstration without authorization – are subject to administrative or even criminal penalties in Belarus, activists often fear that surveillance of their daily activities could expose them to legal jeopardy. This fear is exacerbated by the memory of the crackdown that followed the 2010 elections, where private communications and location data – whether obtained through surveillance or otherwise – played a prominent and public role in several politically-motivated prosecutions of opposition politicians and other activists.

> **"EVEN THE MERE POSSIBILITY OF COMMUNICATIONS BEING CAPTURED CREATES AN INTERFERENCE WITH PRIVACY, WITH A POTENTIAL CHILLING EFFECT ON RIGHTS, INCLUDING THOSE TO FREE EXPRESSION AND ASSOCIATION."**
>
> United Nations High Commissioner for Human Rights[15]

The chilling effect caused by the fear of surveillance manifests in several ways. Activists generally feared communicating about anything of substance by telephone or e-mail, or even in their own offices or homes. This makes it often necessary to meet in person to have serious discussions. However, this too is complicated by surveillance fears and activists often fear their mobile phones could be used to track their locations or eavesdrop on their conversations, or that they may be under physical surveillance or recorded by listening devices. Additionally, activists fear their e-mail or other digital communications could be exposed due to hacking or confiscation of their devices by the authorities. These factors make the use of encryption

14 The term "surveillance" or "secret surveillance" in this document refers to all types of searches or monitoring of telephone, mobile phone, internet, or other communications data, either in real-time or by access to retained data, including either the content of communications or location or other metadata related to communications. It also includes the audio or video monitoring of people or premises.
15 UN High Commissioner for Human Rights, The Right to Privacy in the Digital Age, A/HRC/27/37, 30 June 2014 (hereinafter UNHCHR Privacy in the Digital Age), para. 20.

and other privacy tools essential for activists, but nonetheless, nearly every aspect of the day-to-day work of activists is impeded by surveillance and the chilling effect it creates.

## 4.1 A WIDESPREAD SUSPICION OF SURVEILLANCE

> **"Most people are afraid to speak openly on the phone. It's like part of your mindset. You assume from the beginning that you live in fear, that everything is bad, that you cannot control or influence it."**
>
> Independent journalist, Minsk, December 2015

Activists, journalists, opposition party members, and others who spoke with Amnesty International - both in Belarus and abroad - nearly uniformly expressed suspicion that their communications were monitored.[16] One journalist noted that the fear of secret surveillance affects the lives and work of activists and "creates a paranoid attitude," but added that this attitude "is quite justified in this situation."[17] Another independent journalist said that because of his profession, "of course they are listening to us."[18] An activist who said that he was certain the authorities listened to the phone calls of activists related that mobile phones were often jokingly referred to amongst activists as a "police officer in your pocket."[19] Another activist told Amnesty International, "In principle if I am talking indoors, or on the phone, or writing emails, I assume it all gets to the KGB[20]. So I don't worry about it, I talk openly and say only what I would say if there were a KGB agent sitting next to me."[21]

[16] Interviews in Minsk, December 2015 ; Interview in Vilnius, August 2015, Interviews in Warsaw, August 2015.
[17] Interview with independent journalist, Minsk, December 2015.
[18] Interview with independent journalist, Minsk, December 2015.
[19] Interview with human rights defenders, Minsk, December 2015.
[20] State Security Committee
[21] Interview with youth activist, Minsk, December 2015.

# USE OF SURVEILLANCE IN THE CRACKDOWN FOLLOWING THE 2010 ELECTIONS

The crackdown that followed the widely-disputed 2010 elections saw numerous people arrested for the exercise of their human rights, including for participation in peaceful protests against the outcome of the elections. The use of surveillance of mobile phone and internet data to track the identities of protestors and to prosecute opposition political leaders and others was a significant feature of this crackdown. Though Belarus has not seen a crackdown on this scale in the intervening years, these events, including several well-publicized prosecutions, were cited by many people who spoke to Amnesty International as a key reason why they believed they were not safe from state surveillance.

Following the post-election protests, numerous media outlets reported that the authorities used mobile phone data to determine who was present at the locations of protests, and to summon people who were detected there for interrogation.[22]

In addition, several opposition candidates expressed their fears of surveillance in the run-up to the election, and several opposition candidates prosecuted following the elections had private communications used against them as evidence at trial.[23] Former opposition presidential candidate Mikalai Statkevich was imprisoned for his role in peacefully protesting the 2010 elections, and was considered by Amnesty International to be a prisoner of conscience, until his release in August 2015. He told Amnesty International that during his interrogation, transcripts of his phone calls and Skype chats, as well as those of his friends and associates, were shown to him by his interrogators. He believes that these transcripts were obtained without a legal basis.[24]

Andrei Sannikau, another former presidential candidate, says that during his criminal interrogation following the election, he was read direct quotations from private phone conversations. He says that although the authorities justified this surveillance by reference to the criminal investigation against him, he learned that the surveillance in fact started many months prior to the start of the investigation. At the time, he protested that this earlier surveillance lacked any legal basis.[25] Sannikau was imprisoned following the elections for his role in the protests, and Amnesty International considered him a prisoner of conscience.[26] Prior to this, in September 2010, during the campaign period, he was also investigated regarding the death of his friend and campaign press secretary, Aleh Babenin. During those interrogations, he was told about the tracking of his location: "They asked me specific questions about what we talked about with Aleh at precise times. And when I asked 'how do you know this', they showed me how they checked our location, and they explained to me how they can track telephones […] very accurately, within one to three meters. And they have proven this to me because I do remember when we met and I do remember where we met, and they have proven to me that they were following us, not [just] following us, they said that the company, the mobile phone provider can provide the exact location if they are asked by the prosecutor's office or the police […] It was the eve of the campaign, so I had to take it into account of course."[27]

Ales Bialiatski, the chairperson of the Human Rights Centre Viasna, was arrested in 2011 on tax evasion charges. Viasna had been providing assistance to victims of the post-election crackdown. Amnesty considered the charges against Bialiatski to have been politically motivated, arguing that he was a prisoner of conscience who should be released.[28] He told Amnesty International: "Parts of my Skype conversation with our Polish NGO partners were actually published in the state newspaper – "Sovetskaya Belarussia" (Soviet Belarus) [currently called "Belarus Segodnia", (Belarus today)] – the leading one. So they were trying to compromise me as if I was looking for funding to overthrow the regime or something but I was actually discussing assistance to victims of political repression. The conversation took place in spring of 2011 and they published it in the newspaper in fall of 2011, right after they arrested me. I don't know how they managed to read it, most probably it was my mistake. Most likely I forgot to log out, or perhaps they learned the password somehow. It was not attached to the charge, it was not in the case materials, but it was published in the newspaper because they were trying to create this climate of distrust for human rights defenders…Anyway, it seems to me they were able to access my Skype account back then, when the conversations in question happened, in spring, in real time. The disk was encrypted. That's why most

likely they intercepted it somehow. During the trial there was testimony by experts that they were not able to read the disks."[29]

Recent years have not seen a recurrence of the type of crackdown that followed the 2010 elections and subsequent protests. The 2015 elections were not accompanied by mass protests or arrests, as in 2010. Also, the period preceding the 2015 elections saw the early release of several opposition figures who had been jailed following the 2010 elections.[30] However, the elections of 2015 were criticized by Organization for Security and Cooperation in Europe (OSCE) election observers, who said that they "indicated that Belarus still has a considerable way to go in meeting its OSCE commitments for democratic elections".[31] Additionally, following the elections, the UN Special Rapporteur on the situation of human rights in Belarus noted that "the dismal state of human rights has remained unchanged in the country."[32]

The events of 2010 and 2011, including the well-publicized uses of personal data to track or prosecute people were cited by many people who spoke to Amnesty as a reason they continued to fear they were under surveillance. Many people expressed concern that the current, relatively free, environment as regards human rights would not last, and that changes in political circumstances could again lead to the sort of crackdown on human rights seen in the recent past. As one activist put it: "We have kind of vegetarian times now. We don't know how long it will last."[33]

As the European Court of Human Rights noted in *Roman Zakharov v. Russia*, secret surveillance can harm the human rights even of people who have not been subject to surveillance. The ECtHR stated that where a secret surveillance system may affect anyone and where there are inadequate remedies to challenge suspected secret surveillance:

> **"widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified […]. In such circumstances the menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right [to private and family life]."**

[22] See: Belarus Opposition Trapped in Mobile Network, 5 Jan 2011, https://www.rt.com/politics/minsk-mobile-phones-protesters/; How Teliasonera Sells to Dictatorships, Uppdrag Granskning: The Black Boxes, Mission: Investigation, https://vimeo.com/41248885; Human Rights Watch, Shattering Hopes: Post-Election Crackdown in Belarus, footnote 31 (March 2011), https://www.hrw.org/report/2011/03/14/shattering-hopes/post-election-crackdown-belarus; Charter 97, О событиях 19 декабря КГБ допрашивает несовершеннолетних, January 17, 2011, https://charter97.org/ru/news/2011/1/17/35277/ and Warsaw 7.
[23] Тайны президентской кампании. Как шпионят за кандидатами: http://naviny.by/rubrics/elections/2010/12/19/ic_articles_623_171727/?_sm_au_=iVVLpMFqWVFfsQ58
[24] Interview with Mikalai Statkevich, Minsk, December 2015.
[25] Андрей Санников: Лукашенко должен уйти в отставку уже только за прослушку моих телефонов, https://charter97.org/be/news/2011/7/5/40243/?_sm_au_=iVVk6775DJ0jQ5j7
[26] Belarus: Further Information: Prisoner of Conscience Freed: Andrei Sannikau, https://www.amnesty.org/en/documents/eur49/004/2012/en/
[27] Interview with Andrei Sannikau, Warsaw, August 2015.
[28] Amnesty International, Belarus: Ales Bialiatski is Freed under Prisoner Amnesty, https://www.amnesty.org/en/documents/eur49/008/2014/en/
[29] Interview with Ales Bialiatski, Minsk, December 2015; see also: http://www.sb.by/peredovitsa/article/za-kulisami-odnogo-zagovora.html
[30] Amnesty International USA, Belarus: Political Prisoners Released, but Authorities Need to Do More for Human Rights, http://blog.amnestyusa.org/europe/belarus-political-prisoners-released-but-authorities-need-to-do-more-for-human-rights/
[31] Republic of Belarus Presidential Election, 11 OCTOBER 2015, OSCE/ODIHR Election Observation Mission Final Report, http://www.osce.org/odihr/elections/belarus/218981?download=true
[32] http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17027&LangID=E#sthash.o5jDbz0w.dpuf
[33] Interview with independent journalist, Minsk, December 2015.

*Roman Zakharov v. Russia*, European Court of Human Rights, paragraph 171.

Several Activists emphasized that the ongoing uncertainty regarding whether they were subject to secret surveillance took a toll on their psychological state and the way in which they lived. Many activists told Amnesty International that maintaining confidentiality around sensitive information such as that related to their funding or public activities, was a key preoccupation. One activist said that such security precautions made it difficult to organize and to reach new audiences. He said "I am pretty sure we are listened to by the KGB," but that nonetheless "we try not to be so scared of this."[34]

**"This way of life has already become a habit. [The fear of surveillance] makes you obliged to lead a moral life. You realise you cannot afford drinking too much and so on. You realise you can be under surveillance any moment. I am wary of meeting new people. I do not communicate with people who approach me. I only communicate with those who have references from people whom I know really well."**

Independent journalist, Warsaw, August 2015

Another activist emphasized that it was difficult to know how to be careful under surveillance since it is hard to know what information might be used against you or how: "All people feel they have something to hide. Even if it's not a thing to hide, it could be used against you…I have nothing to hide, but sometimes you don't know you have to hide."[35] Several people emphasized that this sense of uncertainty was exacerbated in part due to suspicion that personal information obtained via secret surveillance might be used not for criminal prosecution, but in order to compromise people based on their personal lives.[36]

In the absence of publicly available information on the true nature of secret surveillance, rumours, anecdotes, and incidents which may not in fact have to do with secret surveillance, are sometimes perceived by activists as indicators of surveillance, increasing fear. As one Belarusian internet expert noted, regarding secret surveillance, "it's enough for people to feel it exists."[37] Even people who had had their own digital evidence (such as personal Skype chats) used against them by the authorities, or published, could not say for certain whether that information was intercepted by surveillance or had been obtained in some other manner.[38] Several people cited instances in which their social media accounts appeared to be online while they were in detention as events which increased the fear of surveillance among them and their friends, despite the lack of evidence regarding how this happened.[39] Another opposition activist noted that people tended to see any strange behaviour of electronic devices as evidence of surveillance, even when it may in fact be totally unrelated. For instance, he noted that if a mobile phone battery drained more quickly than usual, it was often seen as evidence of surveillance.[40] Others also noted unexplained events that fuelled fears of surveillance. One activist claimed to have seen transcripts of what he believed had been private meetings

[34] Interview with youth activist, Minsk, December 2015.
[35] Interview with environmental activist, Minsk, December 2015.
[36] Interview with human rights defender, Minsk, December 2015; Interview with opposition political activist, Vilnius, August 2015; Interview with opposition political activist, Minsk, December 2015.
[37] Interview with internet expert, Minsk, December 2015.
[38] Interviews with youth activist and human rights defender, Minsk, December 2015.
[39] Interview with independent journalist, Minsk, December 2015; Interview with youth activist, Minsk, December 2015.
[40] Interview with opposition political activist, Warsaw, August 2015.

he had attended posted on websites considered pro-government, which led him to believe that the authorities were behind the online stories.[41]

## 4.2 HOW TO COMMUNICATE

Living with a constant fear of surveillance, many simple daily activities become significant challenges, especially for activists. For instance, most people who spoke to Amnesty International emphasized that they did not trust most means of communication, and preferred to meet face-to-face to discuss their work, especially on sensitive subjects.[42]

Different people had different opinions as to what types of information is sensitive, but among the most commonly mentioned were financial information and information on public activities or protests.[43] Activists also had their own methods for communicating on the phone when it was necessary. An opposition activist related that she used pre-arranged code in order to talk with colleagues by phone.[44] Other groups had rules for secure communications, which included items like never discussing meeting locations over the phone.[45] Another stressed that he discussed only public information or spoke in generalities over the phone.[46]

A youth activist noted, "We don't discuss important things on the phone or on the Internet. We try to discuss the most important things in person during meetings face to face. We currently use Internet to arrange meetings but do not discuss anything that can be dangerous for us that way. We never discuss particular details of our events and don't name people or organizations."[47]

> **"Our telephones…our mobile phone providers, all of them communicate with the government[48]…So we prefer not to talk about money, or places of our meetings where we talk about different serious things and all of that. We even have special codes how we can talk about money."**
>
> LGBTI Rights Activist, remote interview from London, April 2016

An opposition activist, discussing the lengths he went to when speaking on the phone, including using fake names and coded locations, complained: "it's annoying really, because you have to live in this mode. You know, it's really annoying that you cannot speak openly, cannot talk over the phone without taking precautions."[49]

A human rights activist told Amnesty International: "I don't use the landline at all. As for my personal mobile phone, I use it only to arrange meetings. I am sure my mobile phone is subject to surveillance. I know there is a technical opportunity for them to identify my location using my mobile phone. That's why when I need to be not recognized, incognito, I leave the phone at the office."[50]

---

[41] Interview with youth activist, Minsk, December 2015.
[42] Interviews in Minsk, December 2015 and Vilnius, August 2015.
[43] Interview with activists in Minsk, December 2015, Vilnius, August 2015 and London, April 2016.
[44] Interview with opposition political activist, Minsk, December 2015.
[45] Interview with human rights defenders, Minsk, December 2015.
[46] Interview with human rights defenders, Minsk, December 2015.
[47] Remote interview with youth activist, London, March 2016.
[48] Mobile providers in Belarus provide direct, automated access to customer data to the authorities. See Box: What is SORM?
[49] Interview with opposition political activist, Warsaw, August 2015.
[50] Remote interview with human rights defender, London, May 2016.

## 4.3 HOW TO MEET

While the pronounced fear of surveillance amongst civil society activists makes meeting in person necessary, it also makes it more difficult and onerous. Most activists who spoke to Amnesty International were concerned that their mobile phones could be used to record their meetings remotely, or could reveal their locations, and thus who they meet with. Many additionally feared that their offices were bugged, making it necessary to find public spaces in which to meet for face-to-face discussions.

Several activists noted that they do not bring mobile phones to meetings due to fear of surveillance.[51]

> **"For some kinds of activities - not very open topics - of course we are going without phones and we are trying to have mediators to arrange meetings, and well, this is the price we are paying."**
>
> Interview with Independent Journalist, Minsk, December 2015

A youth activist with an unregistered organization recounted how he and his colleagues used designated abandoned buildings to hold meetings in order to avoid surveillance.[52]

An activist noted the time constraints that these types of meeting arrangements created. Essentially, he noted, he had to arrange in-person meetings just to arrange to meet in-person, rather than using simpler methods like placing phone calls.[53] Another activist lamented that without surveillance, "many things would be simpler. It's quite difficult, if you need to discuss some issue you need to meet with the person. So it's the 21st century but we still have to meet face-to-face as in the 90s."[54]

## 4.4 IMPORTANCE OF ENCRYPTION

Secret surveillance, and the fear thereof, makes the use of encryption especially important for journalists, activists and others in Belarus. Nearly everyone who spoke to Amnesty International highlighted the importance of encrypted communication or devices to their work.[55] As one activist noted, such tools are "absolutely necessary."[56] A student activist told Amnesty International: "everything work-related had always been encrypted by PGP,[57] and I never discussed any work-related issues on Skype."[58]

[51] Interviews in Minsk, December 2015, Vilnius, August 2015, and remotely from London, May 2016.
[52] Interview with youth activist, Minsk, December 2015.
[53] Interview with opposition political activists, Vilnius, August 2015.
[54] Interview with youth activist, Minsk, December 2015.
[55] Interviews in Minsk, 2015 and Vilnius, August 2015.
[56] Interview with independent journalist, Minsk, December 2015.
[57] A system of end-to-end encryption for e-mail, https://ssd.eff.org/en/glossary/pgp
[58] Remote interview with student activist, London, April 2016.

**ENCRYPTION AND ANONYMITY ONLINE**

Encryption refers to a mathematical process of converting messages, information, or data into a form unreadable by anyone except the intended recipient (and depending on the type of encryption, the service provider).

Encryption of the content of communications does not provide anonymity: whereas encryption tools ensure that the content of a communication is decipherable only to those holding a decryption key, they provide neither the recipient nor the sender with anonymity. The identity of the parties to a communication remains ascertainable when parties use encryption, because the metadata associated with a communication are not encrypted. Should an individual wish to remain anonymous, they need to employ anonymization tools and methods, such as using pseudonyms or anonymization tools such as the special web browser "Tor".[59]

While encryption and anonymity tools are helpful in many instances in protecting the privacy of communications, they cannot guarantee privacy in all circumstances, and remain vulnerable to hacking, user error or other factors.

In the digital age, access to and use of encryption is an enabler of the rights to privacy and freedom of expression, information and opinion, and also has an impact on the rights to freedom of peaceful assembly, association and other human rights. Encryption is a particularly critical tool for human rights defenders, activists and journalists, all of whom rely on it with increasing frequency to protect their security and that of others. Amnesty International believes that states should facilitate the use of encryption and must not interfere, or permit interferences by others, in an unjustified manner.[60]

For more information about tools that can be used to protect communications privacy, you may wish to consult the Surveillance Self-Defense page of the Electronic Frontier Foundation[61] or the Security in a Box project of the Tactical Technology Collective and Frontline Defenders.[62]

An LGBTI rights activist said, "It is not very secure to use all that Beltelecom stuff without any shields. So that's why we understood from the very beginning that we need to use a VPN[63] connection… Financial issues is one of the main points for the authorities to have a mechanism how to put pressure on us. That's why that's […]a taboo topic sometimes to talk, when you feel yourself not to be secure. You will never talk about it in a café. You will not use names, and all that. And not all of our donors really understand how harmful this could be, and though sometimes that's not really comfortable to them. Because you cannot really just write a letter and hit send and everything would be alright. We ask them to use secure mailbox and PGP communication and all that. So for now, that's the way we communicate with them, and they understand how important that could be."[64]

One youth activist complained that while encryption tools are necessary for activists, especially regarding financial information, they can be cumbersome and be a drain on work: "If you protect all your information, you can't reach anybody." He lamented that the time it takes to encrypt and decrypt information, the inability to keep paper files, or to print documents was a barrier to work: "It's not easy. It doesn't help our work at all. It makes our work much more ineffective. I hate all this security…[our organization] will disappear, become just like a secret group."[65]

# 4.5 PHONE LOCATION/LISTENING

[59] For more information about Tor, see https://www.torproject.org/about/overview.html.en

[60] See Amnesty International, Encryption: A Matter of Human Rights, https://www.amnesty.org/en/documents/pol40/3682/2016/en/
[61] https://ssd.eff.org/
[62] https://securityinabox.org/
[63] Virtual Private Network
[64] Remote interview with LGBTI rights activist, London, April 2016.
[65] Interview with youth activist, Minsk, December 2015.

A large proportion of the people interviewed by Amnesty International had experienced, or heard of, events that led them to suspect that phones were being listened to or tracked, though such suspicions cannot usually be verified.

A common complaint was that police sometimes appeared to be informed of the times and locations of events before they happen. One journalist related that she frequently had the experience of travelling to a town to meet activists with whom she had spoken on the phone, only to find that the police were waiting upon her arrival.[66] An activist noted that police seemed to frequently be aware of the locations of secretly-organized protests beforehand.[67] A human rights lawyer reported seeing a suspicious vehicle decked with antennae near protest events which she suspected was tracking protestors' phones.[68]

In other situations, information revealed in exchanges with authorities, or their behaviour, can lead people to suspect their phone conversations have been monitored. One opposition activist told Amnesty International how he had once been called by a police officer asking to meet. Since the activist was under a form of preventive supervision because of his role in protests at the time, he spoke often to this officer and knew him by name. After being called, he called his wife and told her about the call from the police, referring to the officer by a nickname they used for him privately. Two hours later he was picked up by the police on the street. He said he suspected the police knew his location by tracking his phone. When he was taken to the station, the officer who had called him asked him why he used a nickname to refer to him. The activist said he interpreted this as an attempt to demonstrate that the police could monitor his calls.[69]

The same activist related another incident, which occurred in 2012, where he believes his location was disclosed to the police through the monitoring of his phone conversations: "One day I was on the street talking on the phone with a person. We arranged to meet at 2.10pm at a train station, as I can remember. I came at 2:00pm and at 2:05 I saw two policemen wearing civilian clothes who were obviously looking for someone in the square in front of the train station. I was quite unexperienced then. That's why I thought (I remember thinking this clearly): 'They can't possibly be looking for me'. But no, obviously. They continued their search for some time, running back and forth for about three minutes, and finally approached me and put the handcuffs on me. That's it. And, as usual, they took me to the building that is situated nearby. Which is the Moscow District Office of Internal Affairs (The Main Moscow Police Department). I often reside there."[70]

Another activist told a similar story about being arrested by police he believes knew of his location from monitoring his phone: "For instance, there was a case in 2013. This wasn't the first time. I was in Minsk and had some meetings arranged in the city. I was going to a meeting and was approached by two policemen in a public subway. They showed their official IDs to me. It was not the first time, I knew what could happen next. That's why I started yelling and called out for help. Then other policemen approached from the underground station (these were wearing uniforms). The first two showed their documents to them. Then they handed me into a minibus and drove to a police department. We had a conversation there with those two guys. They were from a special operations force, I even thought it might be OMON, some kind of special police. I don't know exactly, but I think they were not from KGB. I was talking to them in Russian and they laughed at me and said: 'You don't use Russian language when talking on the phone'. I mean they made it clear they listened to my conversations. I think they meant the ones that happened that day, they listened to them in real time, live. And they were even not from KGB, just from some kind of special forces. And they knew I had a meeting, they waited for me where it was arranged."[71]

One human rights activist related how a KGB officer she spoke to on the phone claimed to know her location. She said: "When I was summoned to meet the KGB, their officer called and said 'we'll pick you up.' I answered: 'How do you know where I am?' He said I was at work and they would pick me up from there. My movements are controlled by the authorities."[72]

---

[66] Interview with independent journalist, Minsk, December 2015.
[67] Interview with internet expert, Vilnius, August, 2015.
[68] Interview with human rights defender, Minsk, December 2015.
[69] Interview with youth activist, Minsk, December 2015.
[70] Interview with youth activist, Minsk, December 2015.
[71] Interview with opposition political activist, Warsaw, August 2015.
[72] Interview with human rights defender, Minsk, December 2015.

# 4.6 BUGGING/PHYSICAL SURVEILLANCE

Physical surveillance, as well as bugging of offices and homes, continues to be a widespread fear among civil society actors in Belarus, complicating the work of activists by making them reticent to conduct sensitive conversations in their own offices.

One human rights defender said that they could not be sure whether their office was bugged. She recalled an incident from the time when they worked out of their previous office:

"One day we found out [our downstairs neighbours] were moving out and I asked them why. They answered they had been unable to work there because the secret services agents had been coming round every now and then to kick them out (together with their clients) in order to listen to what happened in our office. It was so devastating for their business that they had to relocate.

Any kind of checks for surveillance cannot be called really effective, as they show you only what happens at this particular moment. It can result in a sense of false security. Now we have such an attitude that the office can be surveilled any moment and it is not a place for serious conversations."[73]

Political opposition members also expressed the same belief that their office was likely monitored. However, they also said they felt it was futile to try to search for bugs in the office since even finding and removing such bugs would provide only a false sense of security, as they could be reinstalled at any point.[74]

The suspicion that offices or homes may be monitored leads activists to be wary of unexplained or unusual events that could possibly relate to surveillance. The above human rights activist related how she had brought in her car for service last year due to a fault with the alarm and the technician had discovered an unexplained device that appeared to be a microphone but was not part of the alarm system. She was concerned that it could be a listening device, but had no way to verify this.[75]

Because there are no meaningful avenues for remedy for secret surveillance, activists are left to speculate as to the causes of events that appear linked to surveillance. One activist related that she had been summoned to a discussion with the KGB, and during the conversation the KGB officer asked detailed questions indicating that he was familiar with the content of discussions she had recently had with an international donor. The information the KGB officer knew had only been discussed in a private meeting with the donor in Vilnius, in a car with fellow activists, and in a meeting in her office with members of her board. The activists speculated that the information could have come from bugging of her office, or from informants in her organization, but had no way to verify which of these, if any, were true.[76]

Many people expressed their suspicion that they were subject to physical surveillance or that their organizations were watched by government informers, but were rarely able to get any concrete information about this.

One journalist who works for an unaccredited news organization, and thus has to work out of unofficial offices based in apartments related this story, "We once [in 2008] hired a man who was a specialist at looking for hidden devices, and he found this bug in one of our flats. And the next day the KGB went to him, to his house, and they told him not, 'why did you find this bug for them,' but they told him 'somebody has signed a paper for this bug, please give it back to us. We are financially responsible for this device, and you should give it back to us.' And after this case, we stopped looking for bugs in our flats but I am almost 100% sure they are still there."[77]

Activists also worry about their own homes. Andrei Sannikau, the former opposition presidential candidate who was imprisoned following the 2010 election protests, and whom Amnesty International considered a prisoner of conscience,[78] related that he had learned that his apartment was bugged in the course of his

[73] Interview with human rights defender, Minsk, December 2015.
[74] Interview with opposition political activist, Minsk, December 2015.
[75] Interview with human rights defender, Minsk, December 2015.
[76] Interview with environmental activist, Minsk, December 2015.
[77] Interview with independent journalist, Minsk, December 2015.
[78] Amnesty International, Belarus: Further Information: Prisoner of Conscience Freed: Andrei Sannikau, https://www.amnesty.org/en/documents/eur49/004/2012/en/

prosecution, and conversations recorded there. He said he believes the apartment, where his family continues to live, is still bugged.[79]

Another activist, who had been arrested numerous times for his protest activities said that he no longer trusted the privacy of his flat. He recounted a time when he and his wife returned from a wedding and found the computer in their flat had been moved. Both he and his wife initially assumed the other had moved it, but after they each discovered the other had not, they became very nervous that someone had been in the flat or that the computer had been tampered with.[80]

*A listening device found in a café during a meeting of opposition politicians.*

In one rare case where there was physical evidence that indicated that individuals may have been targeted for surveillance, in October 2015, at a meeting of opposition politicians at a café in central Minsk, Anatol Liabedzka became suspicious after a waiter arrived and replaced the napkin holder on their table. Upon examining it, he found that the napkin holder opened and that it contained in its base what appeared to be some form of a listening device. They were unsure exactly what the device was, so decided to take it away with them to have it examined. They feared that immediately alerting the press or the police would result in the device being confiscated. After they had it examined and determined that it was a listening device, they filed a complaint with the Office of the Prosecutor General, demanding an investigation into the incident [see below].[81]

# 4.7 HACKING

Documented cases of hacking – the use of software or other technology to monitor or otherwise access the communications or other personal information or accounts of a user – are still a relatively rare, or at least unreported, occurrence in Belarus. Activists do not know what powers or tools the Belarusian government has at its disposal to hack computers or phones. In July 2015, as a result of a leak from the commercial spyware vendor Hacking Team, documents were revealed that appear to show that the OAC and Ministry of Internal Affairs had shown interest in purchasing Hacking Team spyware tools, including one that would allow access to and retrieval of data from a target computer via a USB drive. The documents do not provide evidence that the sale was completed.[82]

Where cases of hacking do appear to have occurred, it is generally not possible to determine by which means such hacking took place, or by whom it was perpetrated. Often these incidents are susceptible to

[79] Interview with Andrei Sannikau, Warsaw, August, 2015.
[80] Interview with youth activist, Minsk, December 2015.
[81] Interviews with United Civic Party, Minsk, December 2015; Статкевич, Лебедько и Некляев в ходе встречи в «Салодкім фальварку» обнаружили «жучок» в салфетнице
http://nn.by/?c=ar&i=158217&lang=ru.
[82] https://www.occrp.org/en/daily/4161-belarus-wanted-to-use-usb-sticks-to-infect-devices-and-collect-data;
https://charter97.org/en/news/2015/7/16/160052/

multiple technical explanations. However, the following examples demonstrate that it may nonetheless affect the rights of civil society activists when private e-mail or social media accounts become compromised.

### LEANID SUDALENKA

One case cited by many people who spoke to Amnesty International involved Leanid Sudalenka.[83] In January 2015, Sudalenka, a human rights activist from Homel, in southeastern Belarus, found himself locked out of his mail.ru email account:

> "The [mail.ru e-mail] account was actually hacked two times. It happened for the first time the 6th of January but I managed to restore it via their technical support and continued to use it. This account was important to me: I created it in 1999 when there was no Gmail yet, and this email address was public, and a significant number of people got to know it over the years. That's why I didn't want to delete this account, it was precious.
>
> When it was hacked for the first time I restored it and used it for two more weeks. But when it got hacked again on the 20th, I lost my interest in using this account. Also, by that time I decided I needed to stop using an account based in Russia. Those accounts don't provide confidentiality. There is even no need to hack them: my passwords could be easily disclosed to the Belarusian secret service by the Russian secret service."[84]

He was able to obtain documentation from Mail.ru about his efforts to restore his e-mail account.[85] Several months later, in April, his office, which is shared by numerous other civil society organizations, was raided by the police, who seized eight computers (four from the office, and four from his home, some of which belonged to his wife and children) in connection with a criminal investigation:

> "I was in Stockholm that day. Swedish human rights defenders invited me to an annual international human rights conference. When I was there my wife called and told me there was a search conducted in our flat and that they were looking not only for pornographic materials but also for drugs. She said so because the officers that came were from the Department against drug abuse. Of course, I was frightened. I have two teenage sons, 14 and 18 years old. It was likely that they as teenagers might be suspected of having something to do with drugs. The human rights activists from Sweden offered me to stay in Stockholm for a while but I refused and went to Belarus to prove I was innocent. I returned and tried to figure out what had happened. Today it is clear to me that it was a planned provocation aimed at defamation. I am sure that I would have been in prison now, had it not been for the presidential elections 2015. The articles I was supposed to be charged under do not provide any alternative forms of punishment; it is only imprisonment, for 2 to 4 years…
>
> The situation was the following. Pornography was sent from my account (by the way, they sent it not only to the tax authorities but to the district investigators office, as well). Then they initiated a criminal case on the basis of this fact. They needed to investigate this matter. As the pornography

[83] See for instance, World Report 2016: Belarus, Human Rights Watch, https://www.hrw.org/world-report/2016/country-chapters/belarus
[84] Remote interview with Leanid Sudalenka, London, May 2016.
[85] Remote interview with Leanid Sudalenka, London, May 2016.

was sent from my account, they came to my house and to my office in order to conduct searches there. They took the office equipment. I claimed it was a provocation aimed at defamation…

When they took away the computers, I was interrogated in the investigation department. Then I showed the investigator the screenshots that proved the administration of mail.ru and I were messaging to each other about that hacking [of his mail.ru account]. Then, after June 2015, an expertise was performed. And the expert said that the pornographic materials were sent not from our computers. Then they returned the computers and that was it. The investigators have not disturbed me since then.

By that time, a number of national and international organizations had stood up for me. They wrote to the president, the chief of the KGB and the Internal Affairs Ministry. Swedish human rights defenders, Front Line Defenders and Amnesty International had supported me. Also, more than 25 of the famous Belarusian human rights activists wrote an open letter to the Internal Affairs Minister stating that they knew me as a law-abiding citizen and asking to stop this provocation. The Special Rapporteur on the Situation of Human Rights Defenders also was informed about this situation. I think the conclusion of the expert would have been different had I not been supported so much. What does an expertise mean in Belarus? They always get what they order. That's why the expertise results could be completely different. And if the expert had said he had found that pornography had been sent from my computer, it would have been hard for me to prove my case in court."[86]

### ALIAKSANDR

Aliaksandr is a member of a political opposition group and an LGBTI rights activist. In 2015, his social media account was compromised, leading to problems with is employer. He believes the authorities were involved in the attack on his social media account, and feared he might be prosecuted. Despite this, he sought a criminal investigation into the hacking attack, in order to protect himself against such prosecution, but his request was refused, without even a cursory investigation being undertaken:

"It all started at the beginning of 2015. For instance… I was seen being "online" when I was unable to log in while being with my friends somewhere where I had no access to the computer.

There were several situations like this and once whoever was using my account even changed the password. But I always managed to get the access to my account back sending the messages to the social network administration from the telephone number that was connected to the account…

When all of these happened I contacted VK administration [to seek access to my login data in order to look for suspicious activity] and they replied they would disclose this information only in response to an official request from the investigative authorities."[87]

[86] Remote interview with Leanid Sudalenka, London, May 2016.
[87] Interview with Aliaksandr, Minsk, December 2015, and remotely from London, April 2016; Amnesty International wrote to VK to seek clarification, but did not receive a response.

A few months later, in May 2015, Aliaksandr began to have problems with a manager at an HIV/AIDS services organization where he worked. The problems were related to his membership in an opposition party. He said that he was careful to conceal his membership in the party and that he believes this information came to his manager's attention because the manager was shown his private chats from the social network VK – a suspicion he says his manager confirmed:

> "When I was talking to my supervisor (trying to persuade him not to fire me) he said that he met the officers from the department against drug abuse and human trafficking on the 29th of May 2015 and they gave him printed out screenshots of my VK conversations. And he showed those screenshots to me in the presence of witnesses. I saw it with my own eyes…
>
> This department also deals with non-registered organisations[88] (registered ones are dealt with by the KGB). Moreover, many LGBT activists are subject to a lot of pressure and are pursued by this department…
>
> The 'curator' [officer] said to my supervisor that the authorities hacked my VK account and from reading my messages they figured out that I was a member of a political party and connected to a human rights group, which meant I was involved in social activism. That 'curator' also defined me as 'an unreliable member of staff' and demanded that I be immediately dismissed."[89]

Also around this time, Aliaksandr said he started receiving threatening phone calls. Though he could not identify the callers, they threatened to prosecute him for his activities with an unregistered organization (the Young Social Democrats) under article 193 of the Criminal Code, leading him to believe they were from the authorities. Aliaksandr went to the police and demanded an investigation into the hacking of his accounts:

> "I had no hope [that the investigation would yield results]. Even if they investigated properly, the police would find the police. But I still thought it was important to file that request with them because there were several similar cases in Belarus: for example, they hacked the email account of the human rights activist [Leanid] Sudalenka [see above], sent some discrediting materials from his account and later initiated a criminal case against him. The same thing happened to my colleague: they sent pornography on his behalf and then prosecuted him for that. That's why I needed to file that complaint: to be able to prove the fact that my account was hacked, if required.
>
> I needed that refusal to place myself into a safer position. I didn't know what to expect from the authorities. They could initiate a criminal case against me in the same way as they did with Sudalenka."[90]

In response to his request for an investigation, Aliaksandr received a letter from the police[91] that states that the police had sent a request to the department of the Belarus Ministry of Internal Affairs in charge of investigating hi tech crime, but had not received a response. The letter said because of the lack of response, it was impossible for them to determine who had accessed Aliaksandr's account or indeed to

[88] Article 193.1 of the Criminal Code, prohibits activities by unregistered organizations (political parties and religious groups, as well as NGOs), Amnesty International Report 2015/2016, https://www.amnesty.org/en/latest/research/2016/02/annual-report-201516/
[89] Interview with Aliaksandr, Minsk, December 2015, and remotely from London, April 2016.
[90] Interview with Aliaksandr, Minsk, December 2015, and remotely from London, April 2016.
[91] On file with Amnesty International

determine whether a third party had in fact caused the harm, rather than a virus. The letter said that the police therefore refused to open an investigation. It appears therefore that the police took no steps to investigate Aliaksandr's claim beyond sending a request, which was not answered. Aliaksandr appealed this refusal to investigate, but never received a written response. He says that after insisting, he was granted an in-person meeting with prosecutors, who made it clear there would be no investigation.[92]

### IVAN

Ivan[93] is a student activist, who has helped organize unauthorized, but peaceful, demonstrations at university campuses. He explained how he came under pressure, and was eventually expelled from university, in part through his personal online communications being compromised:

> "The deputy of my university department chief showed me a screenshot of a conversation between a personal account and the account of the community [group of student activists on VK] of which I was an administrator. It was visible on this screenshot who of the administrators replied. Even though there was no important information in those messages, just jokes, the screenshot turned out to be useful for them. They used it for showing that I was connected to the community and was actually one of the administrators.
>
> After a while the following has happened. Previously I had installed two-step authentication for my VK account: first you enter a password and then they drop a message [SMS] to your mobile phone with the code you need to access your account. On the 18th of December I got 5 messages with the codes which I had not requested. My password is quite complicated: it consists of 18 random symbols. I'm sure it is impossible to guess what it is and I never write it down or store it anywhere, it is just in my own head… As for the second part of the authentication, I reckon they got the codes that VK sent to my mobile phone from Velcom.
>
> I think it was not the administration of the university but the KGB itself. [At a subsequent meeting university officials] printed off the screenshots of my conversations and tried to blackmail me. All the conversations were personal. I am gay and do not conceal this fact. They tried to use this information by humiliating me and exercising moral pressure on me in order to make me support them and provide them with information. They openly said: if you support us, you will graduate; if you refuse, you'll be expelled. They didn't threaten to publish it though, as I told them I was not concealing the fact that I was gay at all.
>
> And how they use it – not directly against me but against my family. My brother lives in a small city (regional centre) and works at a state-operated factory. He was a deputy of the chief engineer and when the chief engineer left my brother was supposed to take his position. The KGB had a long discussion with him on that occasion (even using a polygraph) and the main topic of the conversation was my life and what they knew about me. They asked him about what I was doing, for example about the international funds, to find out whether he had any understanding of those issues.
>
> I'd like to emphasise that I'm far from being the most dangerous person for these authorities. I was a student activist who was engaged in student projects only and I organised a meeting just once. I didn't pose a threat to security. I communicated with certain European institutions and represented Belarus on European platforms and I was considered dangerous because of that. And

[92] Interview with Aliaksandr, Minsk, December 2015, and remotely from London, April 2016.
[93] Not his real name.

it is not at all the level of the opposition leaders, such as Statkevich[94]. In comparison to those people, I'm nobody. And they use such strong means against me."[95]

## 4.8 CONFISCATION

While documented cases of hacking user data may be relatively rare, confiscation of computers, phones and other equipment remains a much more common threat for activists, and can equally lead to government access to personal data. Digital security experts who spoke to Amnesty International consider confiscation of devices to be the biggest information security threat for activists in Belarus, and noted that arrests that do not lead to prosecution may nonetheless lead to confiscation.[96]

One result of confiscation of devices is that even where the devices are returned, people generally no longer feel safe using them, worrying that they may have been tampered with and could be used to spy on them.[97]

> **"Obviously, we might be unsafe [following the confiscation and return of our computers by the authorities]…We don't have enough money to hire an expert to check our devices or to buy new equipment. There might be spyware on there…After we got our computers back we still have been using them but we have been trying not to use them as extensively as before. We replaced many of them but not all, it's the money issue again."**
>
> Youth Activist, interviewed remotely from London, March 2016.

One opposition politician recounted how following the 2010 elections, "[Government authorities] did confiscate two computers. But then they returned them, but you cannot use them, because definitely they did something with them." He said that they also confiscated memory sticks and other storage devices, "and they returned it as if inviting us to use them, but I tried using them on a friend's computer who used it only for checking for viruses and they were so badly contaminated."[98]

A student activist noted: "We had our laptops confiscated [in 2010] and we had no money to buy new equipment. Together with the Human Rights Centre "Viasna" we started to bombard the local KGB branches with requests such as "Return our laptops", "We have no technical equipment and therefore are unable to work", "We have a lot of important information on those laptops", "I am unable to finish my university coursework: how can I continue my studies?" etc… We included this part deliberately, as I was still a student

[94] Opposition politician Mikalau Statkevich, see Use of Surveillance in the Crackdown Following the 2010 Elections, above.
[95] Remote interview with "Ivan," London, April 2016.
[96] Interview with internet experts, Vilnius, August 2015.
[97] Interview with internet experts, Vilnius, August 2015.
[98] Interview with Andrei Sannikau, Warsaw, August 2015.

then. They returned my laptop and computer only after three months' time. And I had absolutely no desire to use them anymore."[99]

Another activist noted regarding confiscation that "when we work with donors, it's a huge problem." He said that this often involved the necessity of transporting sensitive financial and other documents related to funding applications across borders, which put them at risk of being discovered when or if their devices were confiscated, and thus put them at legal risk since funding an unregistered organization can lead to criminal sanctions.[100]

**LEANID SUDALENKA**
**CONFISCATIONS OF COMPUTERS**

Human rights activist Leanid Sudalenka said that the authorities had confiscated computers and other devices from his home and office numerous times:[101]

> "The searches and confiscations in question [see Hacking, above] were not the first. This was the second search exercised in my house and the fifth that happened in my office. And they always took the computers away, they always found some excuses to come and confiscate our office equipment. They usually took our computers, examined them for about six months and then return them. Some computers were returned broken. It always disturbs the working process…
>
> [After seized computers are returned] we don't use them.
>
> Also, the same thing happens when I cross the state border. For example, last time it happened last year when I was returning to Minsk from Vilnius. My name is in their database. After they scan my passport they immediately take me to another room, search me and usually take my laptop away to return it in about six months' time. But I won't use the laptop after that because I will have got a new one by that time via a sponsor programme. I mean absolutely new, from a store, packed in a box, which means it is safe to use it.
>
> This happened several times, for example, last year it happened twice, on the 24th of May and on the 25 of August. Both times I was carefully searched, even had to take off my socks. And both times they initiated the search after my passport was scanned."[102]

# 4.9 CHILLING EFFECT: CONCLUSION

Because many forms of legitimate activism are criminalized or otherwise punished in Belarus, civil society activists live with a constant risk that surveillance of their private communications could put them in danger. The pervasive secrecy around surveillance practices, and the inadequate regulation and oversight of these practices (see below) mean that the human rights of civil society activists may be violated by surveillance, even if they themselves are not subject to surveillance.

Activists fear their offices are bugged, their phone calls listened in on, their locations tracked and their online communications at risk of hacking. The psychological stress of the fear of surveillance and the self-censorship this fear causes, undermine the ability of activists to do their work. The most basic and crucial daily activities of activists – meeting, making phone calls, arranging public protests, raising funds – are made

[99] Interview with student activist, Minsk, December 2015.
[100] Interview with youth activist, Minsk, December 2015.
[101] Regarding one search and confiscation of computers in 2001, Sudalenka's organization successfully brought a claim before the UN Human Rights Committee, who found that the search and subsequent use of information from seized computers violated human rights, http://www2.ohchr.org/english/bodies/hrc/docs/CaseLaw/CCPR-C-105-D-1226-2003_en.doc.
[102] Remote interview with Leanid Sudalenka, London, May 2016.

more difficult, undermining their ability to function. Civil society itself is weaker in Belarus because of surveillance, and the chilling effect that comes with the fear of surveillance.

# 5. INTERNATIONAL HUMAN RIGHTS LAW AND SURVEILLANCE

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) provides that, "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence," and that "Everyone has the right to the protection of the law against such interference or attacks." As the United Nations High Commissioner on Human Rights has emphasized, "other rights may be affected by … the interception of digital communications and the collection of personal data."[103] These include the right to freedom of opinion and expression, the right to freedom of peaceful assembly and of association. These rights are also guaranteed by the ICCPR, to which Belarus is a state party. These rights are also guaranteed under the Belarusian Constitution.

Surveillance may violate human rights even where the content of communications is not intercepted, but also when only associated data having to do with – for example - the time, manner or location of communication (so-called "metadata") are intercepted. As the UN High Commissioner for Human Rights has noted, "the aggregation of information commonly referred to as 'metadata' may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication."[104]

In some circumstances, secret surveillance can be compatible with human rights obligations, and may in fact serve as an important and useful tool for law enforcement. However, where the domestic legal frameworks *per se* fails to be sufficiently detailed or publicly accessible, or otherwise fails to provide adequate safeguards against abuse, or where surveillance is carried out for purposes or in a manner contrary to the state's international human rights obligations, surveillance will amount to an "arbitrary or unlawful" attack on privacy or otherwise violate other human rights.

The requirements that an interference with the right to privacy through communications surveillance must meet in order to accord with international legal standards are summarized by the UN High Commissioner for Human Rights as follows:

> "To begin with, any limitation to privacy rights reflected in article 17 [ICCPR] must be provided for by law, and the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances. The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available. Moreover, the limitation placed on the right (an interference

[103] UN High Commissioner for Human Rights, The Right to Privacy in the Digital Age, A/HRC/27/37, 30 June 2014 (hereinafter UNHCHR Privacy in the Digital Age), para. 14.
[104] UNHCHR Privacy in the Digital Age, para. 19.

with privacy, for example, for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary."[105]

105 UNHCHR Privacy in the Digital Age, para. 23.

# 6. COMMUNICATIONS SURVEILLANCE IN BELARUS: LAW AND PRACTICE

On 4 December 2015, the Grand Chamber of the European Court of Human Rights (ECtHR) issued a ruling in the case of *Roman Zakharov v. Russia*, wherein it held that the Russian system of secret surveillance was in violation of Article 8 of the European Convention on Human Rights, which protects the right to respect for private and family life. While Belarus is not a party to the European Convention on Human Rights, because of the numerous and strong similarities between the Belarusian system of surveillance and the Russian systems at issue in *Zakharov*, the *Zakharov* decision provides a useful guide for analysing the human rights implications of the Belarusian system, especially since the rights at issue in *Zakharov* are also protected by treaties to which Belarus is a party, such as the International Covenant on Civil and Political Rights. Additionally, many other international experts and bodies have also criticized aspects of the regime governing surveillance in Belarus.

## 6.1 DIRECT ACCESS TO COMMUNICATIONS DATA

The ECtHR in *Zakharov* was critical of the system in Russia, which allows the authorities the technical ability to have direct access to communications and data[106] without the necessity to present a judicial authorization to the communications provider. It noted that, "the Court considers that a system such as the Russian one, which enables the secret services and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorisation to the communications service provider, or to anyone else, is particularly prone to abuse."[107]

106 The data at issue in the Zakharov judgment related to mobile phone communications.
107 ECtHR, Roman Zakharov v. Russia, Application No. 47143/06 (Grand Chamber), 4 December 2015, para. 270 (hereinafter Zakharov); See also, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/23/40, para. 61 (2013), (hereinafter A/HRC/23/40)
http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

## WHAT IS SORM?

"SORM" is the English abbreviation for the система технических средств для обеспечения оперативно-розыскных мероприятий (or СОРМ) - a set of standardized technical means for interception of communications and associated data. SORM first appeared in Russia and versions now exists in many countries of former USSR, including Belarus, where it provides state authorities with direct, automated access to communications and associated data from communications providers, including landline telephones, mobile networks and internet service providers (ISPs).

The requirements and capabilities for SORM in Belarus are laid out mainly in Presidential Edict no. 129 of 2010 and in technical documents developed and approved by the Ministry of Communication and Information, in consultation with the State Security Committee (KGB) and Operations and Analysis Centre under the President (OAC), under Art. 6 of that edict.[108]

By law, operators must ensure that when building communications networks or upgrading facilities or equipment, they are compatible with SORM.[109] Operators are responsible for funding the acquisition, maintenance and repair of SORM equipment.[110]

Providers must provide free non-stop remote access to customer data to the authorities. They must create and maintain databases, which the authorities can access remotely, that include identifying information about customers and their devices, as well as an overview of the internet communications services used.[111] By law, this information should be retained for five years, and the technical documents related to SORM indicate that data on customers' identities and the services they use may be in fact retained for as long as ten years.[112] SORM-linked devices in public access spots (internet cafes, etc…) must also store statistical information for 14 days.

Operators are responsible for limiting access to SORM equipment by staff and protecting data related to search operations.[113] The SORM equipment does not to allow unauthorized access to databases, and must be designed not to leave traces of remote searches in the operators' logbooks.[114]

The requirements of SORM differ slightly depending on the type of network (landline, mobile data, internet, etc…), but share several general characteristics. SORM can generally engage in two types of surveillance: "full monitoring" and "statistical monitoring." "Statistical" monitoring typically concerns communications metadata (types of data transmitted, times of use, etc…) while full monitoring generally involves remote access to all of a user's information in real time. Monitoring can be initiated on the basis of a search for any among a large range of identifying information, such as IP address, e-mail address, user log-in, phone number, time of connection, IMEI,[115] IMSI,[116] MAC address,[117] or other information which can be used to identify communications equipment. For mobile devices, remote control systems can also monitor device location at set intervals, or upon request. In general, the standards demand that the authorities should be able to initiate surveillance within 30 seconds of sending the initiation command.[118]

108 Edict of the President of the Republic of Belarus, March 3, 2010 No. 129, "On the Interaction of Telecommunication Operators with the Authorities Conducting Operational Search," http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.
109 Edict of the President of the Republic of Belarus, March 3, 2010 No. 129, "On the Interaction of Telecommunication Operators with the Authorities Conducting Operational Search," Art. 5 and 13, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.
110 Edict of the President of the Republic of Belarus, March 3, 2010 No. 129, "On the Interaction of Telecommunication Operators with the Authorities Conducting Operational Search," Art. 10, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.
111 Edict of the President of the Republic of Belarus, March 3, 2010 No. 129, "On the Interaction of Telecommunication Operators with the Authorities Conducting Operational Search," Art. 15 and 17, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.
112 Сети электросвязи СИСТЕМА ТЕХНИЧЕСКИХ СРЕДСТВ ДЛЯ ОБЕСПЕЧЕНИЯ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ Технические требования (Telecommunication Networks Technical Investigative Equipment Systems Technical Requirements), (on file with Amnesty International). It is not certain that these technical requirements represent the most current version. Amnesty International sought confirmation of this from several agencies of the Belarusian government, but did not receive a response.
113 Edict of the President of the Republic of Belarus, March 3, 2010 No. 129, "On the Interaction of Telecommunication Operators with the Authorities Conducting Operational Search," Art. 10, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.
114 Сети электросвязи СИСТЕМА ТЕХНИЧЕСКИХ СРЕДСТВ ДЛЯ ОБЕСПЕЧЕНИЯ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ Технические требования (Telecommunication Networks Technical Investigative Equipment Systems Technical Requirements), (on file with Amnesty International).
115 International Mobile Equipment Identity: a number used to identify a mobile phone.

In Belarus, direct access to communications and associated data is provided by a very similar system to that used in Russia, the SORM.[119] SORM provides 24-hour direct automated access to communications data stored by internet and mobile service providers.[120] New service providers who are granted licenses to operate must, within one month of being granted a license, notify the KGB and the Operational Analysis Center (OAC), which sits under the President, who will decide whether the operator is required to implement SORM.[121] Operators are required by law to build networks that allow the operation of SORM.[122] Operators are also required to pay for the acquisition, installation and maintenance of SORM equipment, to protect information regarding the tactics of searches, and to limit the range of persons involved in working with SORM equipment.[123] Where direct remote access to data is not technically feasible, operators are required, upon written notice, to provide a physical copy of customer information to the KGB, Ministry of Interior or OAC.[124]

There is no requirement in Belarusian law that communications service providers be shown any authorization to providers before communication data is accessed.

There is no publicly available information about how often authorities access communications or associated data. In response to a request for this statistical information from Amnesty International, the Department of Financial Investigations of the State Control Committee stated that it was impossible to provide, as it did not exist, and because "certain information according to the legislation of the Republic of Belarus is defined as state secrets."[125]

## 6.2 DATA RETENTION

The ECtHR, in *Zakharov*, noted that the Court of Justice of the European Union (the CJEU) had recently criticized blanket data retention directives, on 8 April 2014 in the joint cases of *Digital Rights Ireland and Seitinger and Others*. The CJEU declared invalid the EU Data Retention Directive (2006/24/EC), which required providers of publicly available electronic communication services or of public communications networks to retain all traffic and location data – but not the content of communications - for periods from six months to two years. The CJEU found that the retention of data constituted a serious and wide-ranging interference with fundamental rights, especially the right to privacy, and noted that "the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."[126]

---

116 International Mobile Subscriber Identity: a number used to identify a mobile subscriber.
117 A unique hardware identifier permanently assigned to a computer's network adapter at the time of manufacture.
118 Сети электросвязи СИСТЕМА ТЕХНИЧЕСКИХ СРЕДСТВ ДЛЯ ОБЕСПЕЧЕНИЯ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ Технические требования (Telecommunication Networks Technical Investigative Equipment Systems Technical Requirements), (on file with Amnesty International).
119 системами технических средств для обеспечения оперативно-розыскных мероприятий (Known by its acronym: СОРМ, or English acronym: SORM), see Edict of the President of the Republic of Belarus, March 3, 2010 No. 129, "On the Interaction of Telecommunication Operators with the Authorities Conducting Operational Search," Art. 2, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.
120 Edict of the President of the Republic of Belarus, March 3, 2010 No. 129, "On the Interaction of Telecommunication Operators with the Authorities Conducting Operational Search," Art. 15, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.
121 Edict of the President of the Republic of Belarus, March 3, 2010 No. 129, "On the Interaction of Telecommunication Operators with the Authorities Conducting Operational Search," Art. 7, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.
122 Edict of the President of the Republic of Belarus, March 3, 2010 No. 129, "On the Interaction of Telecommunication Operators with the Authorities Conducting Operational Search," Art. 5, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.
123 Edict of the President of the Republic of Belarus, March 3, 2010 No. 129, "On the Interaction of Telecommunication Operators with the Authorities Conducting Operational Search," Art. 10, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.
124 Under Art. 17 of the Law on Operational Search, Customer information includes: 1) subscriber number, full name, address, any other data allowing identification of a subscriber. Additionally for mobile service subscribers: requirements of subscriber's ID; 2) general information on telecom services activated by a subscriber. Edict of the President of the Republic of Belarus, March 3, 2010 No. 129, "On the Interaction of Telecommunication Operators with the Authorities Conducting Operational Search," Art. 16 and 17, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.
125 Letter from The Department of Financial Investigations of the State Control Committee, 3 June 2016 (on file with Amnesty International).
126 Digital Rights Ireland and Seitinger and Others (C-293/12 and C-594/12), Court of Justice of the EU, 8 April 2014, Para. 37; See also UNHCHR Privacy in the Digital Age, para. 26 ("Mandatory third party data retention – a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate."); See also, A/HRC/23/40 at para. 67.

In Belarus, communications service providers are obliged to retain many categories of user data. For example, Presidential Decree No. 60 of 2010 requires that ISPs shall identify and record information about subscribers and internet services used. Similarly, Resolution of the Council of Ministers no. 1055 of 2006 requires that service providers retain for one year information to identify subscribers (including MAC address, IP address,[127] time of connection and the domains and IP addresses of resources accessed by users).[128] Information on services rendered and bills paid must be retained for five years.[129] As of 1 January 2016, internet service providers are also required by Resolution No. 6 of the Ministry of Communications of 18 February 2015 to retain similar categories of data to identify users and their online activities for one year.[130]

Similarly, owners of internet service outlets (such as internet cafés) must identify users and keep records on personal data of users, as well as on the Internet services rendered. This information must be retained for one year and disclosed "at any request of the police investigation/operation organs, or by Public Prosecutor organs or by the preliminary investigation organs, or by the State Control Committee organs, or by fiscal organs or by the courts within their respective legislative procedures."[131] However, requirements in Resolution of the Council of Ministers No. 1055 of 2006 that owners record details of customers' IDs were relaxed by Resolution 1191 of 2012, which allows other means, such as photo or video recording of the premises or registration of customers by SMS.

Technical requirements for SORM databases require operators to retain many categories of user data[132] for as long as ten years. These data can be accessed remotely by the authorities.

## 6.3 SCOPE OF APPLICATION OF SECRET SURVEILLANCE MEASURES

In the *Zakharov* decision, the ECtHR emphasized that national law must give adequate indication of the circumstances in which surveillance powers might be used. The ECtHR expressed concern that surveillance could be ordered not only against a suspect under Russian law, but also "a person who may have information about a criminal offence" or "a person who may have information relevant to the criminal case," neither of which are defined in law.[133]

The court was also concerned that surveillance may be justified by vague grounds, including the need to protect national, economic or ecological security, but that these threats are nowhere defined in Russian law, thus creating possibilities for abuse.[134]

In Belarus, surveillance may be authorized under either the Criminal Procedure Code (hereinafter CPC) or the Law On Operational Search Activity (hereinafter OSA Law).[135] Under Article 214 of the CPC, interception and recording of conversations is limited to cases of grave or especially grave offenses. However, such

127 A unique address that identifies an address on the internet or a local network.
128 Resolution of the Council of Ministers of the Republic of Belarus of 17.08.2006 no. 1055, para. 181, http://naviny.org/2006/08/17/by38581.htm. Failure to store this information is considered a "typical violation" of licensing requirements by the Ministry of Communications, http://www.mpt.gov.by/ru/new_page_5_6_15100/
129 Resolution of the Council of Ministers of the Republic of Belarus of 17.08.2006 no. 1055, para. 146, http://naviny.org/2006/08/17/by38581.htm.
130 Resolution No. 6 of the Ministry of Communications of 18 February 2015, para. 3, http://www.belgie.by/_files/npa/p_min_sv_i_inf_n_6.doc; See also, http://www.mpt.gov.by/ru/content/3632. While Resolution No. 6 was introduced following Presidential Decree of 28.12.2014 No. 6 "On urgent measures of counteraction against illegal turnover of drugs" (На основании пункта 9 Декрета Президента Республики Беларусь от 28 декабря 2014 г. № 6 «О неотложных мерах по противодействию незаконному обороту наркотиков»), there is no explicit requirement that the use of retained data be restricted to the purpose of combatting illegal drugs.
131 Presidential Decree No. 60 of 2010, "On the issues to improve making use of the national segment of Internet," art. 6 [Unofficial Translation] http://www.e-belarus.org/docs/decree60.html
132 See "What is SORM?"
133 Zakharov at paras. 243-249.
134 See also A/HRC/23/40 at para. 83 ("Legal frameworks must ensure that communications surveillance measures: (a) Are prescribed by law, meeting a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee their application.")
135 Act of July 15, 2015, No. 307-Z "On operational search activity," http://kgb.by/ru/zakon289-3/

surveillance may take place not only against suspects, but "any other individual" if there are sufficient grounds to believe that a monitored conversation may contain information relevant to a criminal case.[136]

Under the OSA Law, surveillance may be undertaken on the basis of a large number of grounds, several of which are quite broad or vague, including, "if there is:

- information about events or actions that threaten the national security of the Republic of Belarus;
- information about signs of preparing and committing of the offense or persons who prepare, commit or have committed a crime or is aware of the above; [or]
- instruction, direction or decision of an investigative authority in relation to a criminal case, complaint or report"[137]

Most of these grounds do not appear to have been clarified or narrowed elsewhere in the law. One exception is the concept of national security, which is defined in a specific Presidential Edict. However, the definition in this edict is so broad as to offer little guidance as to when surveillance might be legally justified.[138]

Companies that are not required to grant the government access via SORM – such as some domestic e-mail providers hosting foreign-owned e-mail services – may nonetheless be compelled to turn over customer data on the basis of a request from a prosecutor's office. At least one email provider noted that such requests are made regularly and generally are for the company to turn over a username and password, thus granting the authorities access to a user's account in its entirety, and not limited by any restrictions on date, subject or specific correspondence.[139]

## 6.4 ACCESSIBILITY OF DOMESTIC LAW

In the Russian SORM system at issue in *Zakharov*, the technical requirements for surveillance equipment to be installed by providers are specified in addenda to Order no. 70 of the Ministry of Communications. Because these technical requirements may impact users' right to private and family life, the ECtHR urged that they must be made public.[140]

In Belarus, the technical requirements of SORM are developed and approved by the Ministry of Communication and Information, in consultation with the KGB and OAC, under Art. 6 of Presidential Edict 129 of 2010. These requirements do not appear to be publicly available.[141]

## 6.5 AUTHORIZATION OF SURVEILLANCE MEASURES

In *Zakharov*, the ECtHR noted that the Russian requirement of judicial authorisation for surveillance was an important safeguard against abuse. However, this safeguard was undermined by several problems, including the lack of requirement for judges to verify the existence of reasonable suspicion and to apply the test of necessity and proportionality. The ECtHR was also concerned at the lack of requirement – in one law – to specify a person or telephone number as a target. The Court also criticized the fact that in "urgent" cases, judicial authorization was not required to start surveillance, and that a judge's review of authorization, once

136 Criminal Procedure Code, Article 214.
137 Act of July 15, 2015, No. 307-Z "On operational search activity," para. 16, http://kgb.by/ru/zakon289-3/
138 http://naviny.org/2010/11/09/by18748.htm Presidential Edict 575 of 2010 reflects the "totality of official views on the nature and content" of national security. It is a lengthy and extremely broad document. For instance, paragraph 27 of Chapter 4, on "national security threats," lists 30 separate types of threats. While some these threats cover topics such as terrorism, the list also contains such topics as "decline in well-being and quality of life," "rise in unemployment," "inadequate and poor quality of foreign investment," and "attempts to destroy national spiritual and moral traditions and biased revisions of history."
139 Interview with Belarusian e-mail provider, Minsk, December 2015.
140 Zakharov at para. 241; See also, A/HRC/23/40 at para. 91, ("States should be completely transparent about the use and scope of communications surveillance techniques and powers.")
141 Edict of the President of the Republic of Belarus, March 3, 2010 No. 129, "On the Interaction of Telecommunication Operators with the Authorities Conducting Operational Search," Art. 6, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm; Amnesty International sought clarification on this point from the Belarusian authorities, and did not receive a response.

subsequently notified, was limited to the question of whether to extend the authorization, not to whether the initial authorization was justified or whether the data obtained should be kept or destroyed.[142]

In Belarus, under Article 19 of the OSA Law, several types of operational searches, including by installation of secret observation devices, listening devices, and control of telecommunication networks or of mail require the authorization of a prosecutor or a deputy, but not a judge.

Numerous agencies can request authorization to carry out operational searches, which includes various forms of secret surveillance under the OSA Law. These include: agencies of the Ministry of Internal Affairs, agencies of the State Security Committee (KGB); agencies of the Belarusian Border Service, Presidential Security Service, Operational and Analytical Centre under the President of the Republic of Belarus; agencies for Financial Investigations of the State Committee of Control, the Customs Authorities Republic of Belarus, and the intelligence services of the Armed Forces of the Republic of Belarus.[143]

Authorities requesting authorization to conduct such searches must provide a written request to the prosecutor or deputy and include the documents that provide the grounds for the search. If approved, the prosecutor or deputy must specify the duration for which the search is approved. In cases of refusal, the requesting agency has the right to apply again to a higher-level prosecutor.[144]

Under Article 214 of the Criminal Procedure Code, listening to and recording of conversations may be authorized by a prosecutor, deputy prosecutor, or in some cases, by the chairpersons of the Investigative Committee or the State Security Committee (KGB).[145]

There is no requirement that prosecutors authorizing such techniques verify reasonable suspicion or apply the test of necessity and proportionality, nor any requirement to specify a single person or address as target.

In Belarus, there are also numerous circumstances in which even prosecutorial authorization is not required for surveillance. Article 35 of the OSA Law states that operational searches which normally require the authorization of a prosecutor or deputy prosecutor may instead be authorized by the Minister of Internal Affairs, or the President or Deputy of the State Security Committee (KGB) "in urgent cases requiring immediate action to ensure the security of society and state; in order to prevent, detect, or deter serious or especially serious crime, search for and arrest a citizen who has committed such a crime, or if there is information about events and actions that endanger the national security of Belarus."

Under Article 37 of the OSA Law, searches may be carried out without authorization of a prosecutor or deputy, provided they are notified within 24 hours, and approve the search activity within 48 hours, "in cases of urgency, in order to prevent, detect, deter serious or especially serious crime, search and detention of citizens who committed it, to prevent action which can lead to the destruction of objects and documents that may be considered material evidence, and if there is information about events and actions that endanger the national security of the Republic of Belarus."

Under Article 38, searches, including by installing auditory monitoring or monitoring of telecommunications networks within a building, vehicle or other structure, may be undertaken without the authorization of a prosecutor or deputy at the request, or with the written consent, of the owner, a relative, guardian or trustee on the basis of a fear related to the life, health or property of the owner. In such cases, a prosecutor or deputy must be given written notice within 48 hours.

## 6.6 SUPERVISION OF SURVEILLANCE MEASURES

In *Zakharov*, the ECtHR expressed concern at the lack of adequate supervision of surveillance measures in order to prevent abuse. The court was concerned that the fact that the SORM system did not leave logs of search activity denied supervising authorities a key tool to discover unauthorized surveillance. The ECtHR noted that in Russia, the question of whether prosecutors' supervision was adequate depended on their powers and competence as well as their independence from the authorities carrying out the surveillance.

142 Zakharov, at paras. 57-67.
143 Act of July 15, 2015, No. 307-Z "On operational search activity," Art. 12, http://kgb.by/ru/zakon289-3/
144 Act of July 15, 2015, No. 307-Z "On operational search activity," Art. 19, http://kgb.by/ru/zakon289-3/
145 CPC, Article 214.

The ECtHR found that prosecutors' independence was undermined by the fact that they are appointed and dismissed by the Prosecutor General. The ECtHR further noted that the "blending of functions within one prosecutor's office, with the same office giving approval to requests for interceptions and then supervising their implementation […] may also raise doubts as to the prosecutors' independence." The ECtHR noted that supervisory authorities should have access to all relevant documents, have powers to remedy breaches and should be open to scrutiny, such as by publishing reports on their supervisory functions. The Court also considered that the authorities did not provide examples of prosecutors taking steps to remedy breaches in practice.[146]

In Belarus, prosecutors are granted certain powers to supervise operational searches and investigations, however there is no legal obligation to exercise these powers. They may, for instance, access search files, demand explanations, cancel operational searches, or even, in cases of violation, initiate disciplinary or criminal proceedings.[147] Records of access to SORM databases are held for five years, but are held by the investigating authorities themselves, not prosecutors.[148] As noted by the European Court of Human Rights in the Russian context, the lack of records denies prosecutors a key means of discovering violations. Also as in Russia, prosecutors are appointed and dismissed by the Prosecutor General, who in Belarus is appointed by the National Assembly.[149] Additionally, the fact that prosecutors play the roles of both authorizing and supervising surveillance measures potentially creates a conflict of interest. In general, prosecutors' offices do not appear to publish any public reports or data regarding their supervisory functions.

## 6.7 DURATION OF SECRET SURVEILLANCE

In *Zakharov*, the ECtHR stressed that in order to guarantee against arbitrary surveillance, there must be a clear indication in law of the period after which an interception warrant will expire, the circumstances in which a warrant can be renewed, and the circumstances in which a warrant must be cancelled.[150]

In Russia, because the third criteria is met only in criminal cases, and not in national security cases, adequate safeguards do not exist.

In Belarus, under Article 214 of the Criminal Procedure Code, "An Investigative body shall issue a resolution on the necessity of the interception and recording, which shall state among other things the term for which the interception and recording will be performed.

Interception and recording cannot last longer than the investigative work in this particular case and shall be cancelled by a resolution issued by the investigative body."

Thus while interceptions under this article must be cancelled at the end of investigatory work, there is no guidance on the length interception may last, nor any requirement of renewal.

Under Article 19 of the OSA Law, the prosecutor or deputy authorizing an operational search should specify the duration of the authorization, which, under Article 41, should be no more than 90 days in a number of specified cases, including audio and telecommunications surveillance, and up to 180 days in other types of cases.

Article 43 provides that most types of surveillance can be extended on the basis of a motivated application for up to 180 days if authorized by the prosecutors or deputy prosecutors of the City of Minsk or other

146 Zakharov, at paras. 272 – 285. See also A/HRC/23/40 at para. 86, ("The provision of communications data to the State should be monitored by an independent authority, such as a court or oversight mechanism.")
147 Law of the Republic of Belarus, "About the Prosecution Service", arts. 28-31, http://www.pravo.by/webnpa/text.asp?&p0=H10700220; Articles 69 and 70 of the OSA Law also provide for supervision of operational searches by prosecutors and for control over such searches by the heads of bodies carrying them out, Act of July 15, 2015, No. 307-Z "On operational search activity," http://kgb.by/ru/zakon289-3/
148 Edict of the President of the Republic of Belarus, March 3, 2010 No. 129, "On the Interaction of Telecommunication Operators with the Authorities Conducting Operational Search," Art. 15, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm
149 Law of the Republic of Belarus, "About the Prosecution Service", arts. 13-14, http://www.pravo.by/webnpa/text.asp?&p0=H10700220
150 Zakharov at paras. 250-252; See also, A/HRC/23/40 at para. 81, ("Safeguards must be articulated in law relating to the … duration of the possible [surveillance] measures.")

regional prosecutors, up to 365 days by the Deputy Prosecutor General of Belarus, and up to 545 days by the Prosecutor General of Belarus.

Article 46 requires that operational searches be terminated in the absence of grounds justifying ongoing search, or at the expiration of the term of the authorization.

Thus while the OSA Law does require the setting of limits for the duration of surveillance measures, these measures are quite long. Surveillance, if renewed, may take place for as long as a year and a half without ever involving the approval of a judge.

## 6.8 TREATMENT OF DATA

In *Zakharov*, the ECtHR noted that the law must put in place adequate safeguards regarding the storage, accessing, examining, use, communication and destruction of data. In the Russian context, it noted several concerns, especially the lack of a requirement for the immediate destruction of data irrelevant to the purpose for which it was gathered and the unlimited discretion left to judges as to whether or not to destroy data used as evidence at the end of trials.

In Belarus, Articles 14 and 50 of the OSA Law place requirements on operational search staff not to disclose private information obtained during searches and not to use such information to the detriment of search targets. Operational search agencies may decide to share information gathered as part of an operational search with other agencies, or international organizations. However, a risk of making private data about citizens public may be a grounds for refusal to do so.

Under article 14 of the OSA law, authorities are required to destroy operational search data that is irrelevant to unlawful activity. However, there is no time frame specified, nor is there any mention of when data deemed relevant to unlawful activity must ultimately be destroyed, such as at the end of trials.

## 6.9 NOTIFICATION OF SURVEILLANCE

The ECtHR in *Zakharov* noted that a requirement to notify people that they are or have been subject to surveillance "is inextricably linked to the effectiveness of remedies." While acknowledging that secrecy is sometimes essential to surveillance, it nonetheless noted that "[a]s soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned."[151]

In Belarus, there is no requirement to pro-actively notify subjects of surveillance. This is especially problematic in light of the facts that government has direct access to communications and associated data via SORM, is not required to notify communications providers of such access, and that information about secret operational searches are generally required to be kept confidential.[152]

Indeed, even in circumstances where providers are shown authorization – such as with certain e-mail providers not accessible to SORM – they may be legally prohibited from disclosing any information about the accessing of data.[153]

A person who nonetheless manages to come by information that they were under surveillance and believes their rights were violated may request that operational search bodies disclose information, provided there is

151 Zakharov, at paras. 286-7; See also A/HRC/23/40 at para. 82, ("Recognizing that advance or concurrent notification might jeopardize the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath.")
152 Act of July 15, 2015, No. 307-Z "On operational search activity," Arts. 8 - 10, http://kgb.by/ru/zakon289-3/
153 Minsk 20, Article 407 of the Criminal Code prohibits disclosing of data of an investigation.

not a criminal case ongoing, or a criminal case has resulted in acquittal. However, this information can also be withheld, provided reasons for withholding are approved by a court.[154]

As the ECtHR noted, regarding the very similar notification scheme in Russia, given the limitations on disclosure and the fact that "the person concerned is unlikely ever to find out if his or her communications have been intercepted," this does not amount to an effective notification system.[155]

# 6.10 REMEDIES

International human rights law requires that remedies be granted to victims of human rights violations.[156] In Belarus, there are several legal routes by which one might theoretically seek a remedy for rights violations linked to secret surveillance. However, as noted below, many of the people who spoke to Amnesty International are reticent to try to use such legal routes for a number of reasons. Also, as the ECtHR noted in *Zakharov*, the absence of a notification requirement often in practice undermines the effectiveness of remedies for violations of rights linked to secret surveillance.

The government of Belarus points out that the OSA Law, Articles 10 and 11, grant individuals the right to complain about surveillance measures, in accordance with legislative acts. However, as shown below, such legislative acts contain problematic requirements, such as requiring preliminary appeal to a direct superior of the party against whom the complaint is made.

Chapter 16 of the Criminal Procedure Code provides for complaints by people involved in criminal proceedings. Such complaints, if regarding a prosecutor or investigator should go to a prosecutor or investigator of higher rank.[157]

Chapter 29 of the Civil Procedure Code allows individuals to file complaints against government agencies if their rights have been harmed. Complaints can only be filed to a court after complaining to a body of higher rank to that alleged to have committed the wrong.[158]

Under Article 938 of the Civil Code, people may also seek reimbursement for damages caused by government agencies.[159]

These remedies are not generally effective in practice. As noted below, many activists are reluctant to seek remedies due to lack of faith in the independence or efficacy of the justice system. In addition, requirements to complain to a hierarchical superior undermine the effectiveness of remedies since, as the ECtHR stated in *Zakharov*, **"a hierarchical appeal to a direct supervisor of the authority whose actions are being challenged does not meet the standards of independence needed to constitute sufficient protection against the abuse of authority."**[160] Further, as the ECtHR also noted, in civil or criminal complaints where complainants bear the burden of proof, "in the absence of notification or some form of access to official documents relating to the interceptions such a burden of proof is virtually impossible to satisfy."[161]

Belarusian civil society activists echoed this, noting that while it may be theoretically possible to contest suspected unlawful surveillance, it was in practice nearly impossible, due to the unlikelihood of being able to provide hard evidence.[162] As one independent journalist noted: "Many of the cases we just don't know. Only

154 Act of July 15, 2015, No. 307-Z "On operational search activity," paras. 14.16 and 14.21, http://kgb.by/ru/zakon289-3/
155 Zakharov, at para. 289.
156 See for example, ICCPR, article 3: "3. Each State Party to the present Covenant undertakes:
(a) To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity;
(b) To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy;
(c) To ensure that the competent authorities shall enforce such remedies when granted."
157 Criminal Procedure Code, Chapter 16, Article 139, http://kodeksy.by/ugolovno-processualnyy-kodeks/
158 Civil Procedure Code, Chapter 29, Article 354, http://kodeksy.by/grazhdanskiy-processualnyy-kodeks/VII-glava-29
159 Civil Code of the Republic of Belarus, Article 938, http://xn----7sbakgchdukjdc8auvwj.xn--90ais/statya-938
160 Zakharov, at para. 292.
161 Zakharov, at para. 296.
162 Interview with human rights defender, Minsk, December 2015.

during trials does this evidence come to light."[163] A human rights lawyer said he was unaware of any cases of victims of suspected unlawful surveillance successfully seeking a remedy.[164]

Lack of faith in the efficacy of available remedies also disincentivizes people from trying to seek actual evidence of potentially unlawful surveillance. As one opposition politician, who also said he was certain his email had been hacked by the KGB, put it: "What is the reason to discover who is hacking? Because you cannot take any legal action against it in Belarus. So it didn't matter. What matters is to restore [one's hacked accounts] as quickly as possible and continue working."[165] A youth activist noted, "I have an impression I'm under surveillance most of the time. But I would never challenge surveillance. After all, I am the person who was arrested just for being on the street with ridiculous charges. If you complain about everything, you spend your life in court with no result."[166]

> **"The judiciary continues to be fully dependent on the President, in spite of some recent reforms. Besides the lack of independence of the courts and law enforcement agencies, intimidation is used against lawyers, who are forced to join the bar association that is directly supervised by the Government."**
>
> United Nations Special Rapporteur on the Situation of Human Rights in Belarus, April 2015[167]

Many people who spoke to Amnesty International also cited their lack of faith in the fairness of the justice system as a disincentive to seeking a remedy for suspected unlawful surveillance. Under the law, as noted above, certain complaints about official wrongdoing must be made – at least in the first instance – to direct superiors of those accused of wrongdoing, a system which, as the European Court of Human Rights has observed, lacks adequate independence to safeguard against abuse.[168] When Amnesty International asked one activist why he had not sought a remedy for incidents of surveillance, he explained, "First, I have no evidence to support my complaint. Second, I think I won't file any kind of complaint. I've got enough communication with our judicial system and law-enforcement agencies to be aware of how they work. Besides, I'm generally not in favour of complaining to an 'executioner' about the actions of another 'executioner.'"[169] Similarly, another activist, when asked whether he had tried to seek a remedy for harms suffered as a result of surveillance, responded: "To complain to exactly those people who persecuted me? The only way of complaining I would have considered would be sending a complaint to the European Court of Human Rights. But sadly it is not available to us, as Belarus is not a member of the Council of Europe."[170] Another journalist who had been imprisoned in part on the basis of surveillance evidence she believed to be unlawful said she did not consider seeking a remedy as she simply did not want any more interactions with the police.[171]

163 Interview with independent journalist, Minsk, December 2015.
164 Interview with human rights defender, Minsk, December 2015.
165 Interview with opposition political activist, Warsaw, August 2015.
166 Remote interview with youth activist, London, March 2016.
167 Report of the Special Rapporteur on the Situation of Human Rights in Belarus, Miklós Haraszti, A/HRC/29/43, (29 April 2015).
168 Zakharov, at para. 292
169 Interview with youth activist, Minsk, December 2015.
170 Remote interview with youth activist, London, April 2016.
171 Interview with independent journalist, Minsk, December 2015.

As one journalist put it: "There [are] no free courts here. All the judges are signed with a decree of the President… That is why appealing to the courts doesn't exist here as a measure of counter action to the authorities."[172]

Others worried that their personal profiles put them at a disadvantage in terms of seeking a remedy. One student activist noted that even opposition presidential candidates had failed to get a remedy for unlawful surveillance, and so doubted that a student activist could.[173] An opposition politician pointed out that pursuing remedies for surveillance may even involve legal risk for activists, "There were some ways to submit legal complaints to some authorities. For instance, it was possible return to their office and complain, ask why I was surveilled, because I knew my conversations were listened to and what had been heard. Of course, it is possible but there is no point to do that. No point at all. You will just get the runaround. Besides, our everyday activity is of such a kind that we need to realise that they can use the Article 193-1 of the Criminal Code against us. It is an article about the activities of public associations. According to this article we can be arrested any moment, as our organisation is not registered."[174]

In some cases, possible hacking victims such as Leonid Sudalenko and Aliaksandr (above), seek to initiate police complaints not out of a belief that it will lead to a result, but rather to protect themselves against prosecution.

Against this backdrop of general scepticism about the utility of seeking remedies from the justice system, the attempt by opposition politicians to seek an investigation into the apparent listening device they found in the napkin holder in a café in which they met [see above] is relatively rare. However, this effort was ineffective.

The politicians filed a request for an investigation to the Prosecutor General's Office on 15 October, 2015, and demanded to know whether there was a warrant for the interception of their communications, and whether they remained under surveillance. They received a reply just a few days later from the Central Department of Internal Affairs of Minsk stating simply that they had made checks and refused to open a case on the basis of their complaint due to lack of proof. According to the politicians, the police never requested to interview them, not did they request to examine the bug. They elected not to appeal the decision not to open an investigation, arguing that they believed the decision would certainly be upheld on appeal.[175]

172 Interview with independent journalist, Minsk, December 2015.
173 Interview with student activist, Minsk, December 2015.
174 Interview with opposition political activist, Minsk, December 2015; Activities of unregistered organizations are prohibited under the Criminal Code in Belarus, see Restrictive Legal Framework for Civil Society, above.
175 Interview with United Civic Party, Minsk, December 2015.

# 7. ROLE OF PRIVATE COMPANIES

Secret surveillance in Belarus is made possible by the state's direct access to both retained and real-time data of communications providers operating in Belarus.

As laid out in the UN Guiding Principles on Business and Human Rights (UNGPs), companies have a responsibility to respect human rights wherever they operate in the world. The UNGPs require that companies take pro-active steps to ensure that they do not cause or contribute to human rights abuses within their global operations and respond to any human rights abuses when they do occur. In order to meet this responsibility, companies must carry out human rights due diligence to "identify, prevent, mitigate and account for how they address their human rights impacts," and those that may arise from their business relationships, or subsidiaries. The corporate responsibility to respect human rights exists independently of a state's ability or willingness to fulfil its own human rights obligations and over and above compliance with national laws and regulations protecting human rights. This means that, where Belarus law does not meet international human rights law and standards, companies working in Belarus must still act to ensure respect for human rights in their Belarus operations. For example, the interpretative guidance on the UNGPs specifically notes that a company may contribute to a human rights violation if it provides "data about Internet service users to a Government that uses the data to trace and prosecute political dissidents contrary to human rights".[176]

> **"Where enterprises are faced with government demands for access to data that do not comply with international human rights standards, they are expected to seek to honour the principles of human rights law to the greatest extent possible, and to be able to demonstrate their ongoing efforts to do so."**
>
> United Nations High Commission for Human Rights[177]

176 The Corporate Responsibility to Respect Human Rights: An Interpretative Guide, p. 17
http://www.ohchr.org/Documents/Issues/Business/RtRInterpretativeGuide.pdf
[177] UNHCHR Privacy in the Digital Age, para. 45.

The three largest mobile phone providers in Belarus are MTS, Life:) and Velcom. MTS (Belarus) is jointly owned by the Russian company MTS and Beltelecom, the state-owned Belarusian telecom and internet provider. Life:) is 80% owned by the Turkish company Turkcell.[178] Turkcell, in turn, is 38% owned by the Swedish company Teliasonera.[179] Velcom is a wholly-owned subsidiary of Telekom Austria Group, which in turn is nearly 60% owned by América Móvil.[180]

Amnesty International contacted TMS (Belarus), Life;), Velcom, Beltelecom, Telekom Austria Group, Teliasonera and Turkcell to seek information regarding measures they had undertaken to identify, prevent, mitigate or account for unlawful surveillance of their customers in Belarus.

Of those companies who responded to letters from Amnesty International, Teliasonera noted several positive measures they have taken regarding their operations and their subsidiaries in other countries. They stated that they have a firm policy opposing direct access to telecommunications and related data: "We advocate that governments should not have direct access to a company's networks and systems. The company should retain operational and technical control". They have publicly spoken out against direct access requirements.[181] They also pointed to their participation in the Telecoms Industry Dialogue Initiative[182] and noted that they publish a Transparency Report[183], which includes information on numbers of requests for customer data in many countries in which Teliasonera operates, and in direct access countries where such information is impossible to obtain, includes information on the relevant legal framework as well as the company's policy on freedom of expression.[184]

These are welcome steps, however, they do not relate directly to Belarus. The company's position is that they do not operate in Belarus since they are not the majority owner of Turkcell (the parent company of Life:)) and do not have representation on Turkcell's board. In response to media reports, Teliasonera confirmed that two people they nominated to the board of Turkcell in 2013 were accepted, but stressed that they two people in question view themselves as independent. Teliasonera also said that since that time, they have not had another opportunity to nominate members of the board. Teliasonera also argued that they say they have "raised with Turkcell the importance of freedom of expression and privacy, and we have shared our Policy and how we work."[185] As relates to Life:) customers in Belarus, Amnesty International considers that this position is at odds with the Teliasonera's obligation to address human rights concerns "which may be directly linked to its operations, products or services by its business relationships."[186]

Telekom Austria Group (owner of Velcom), also responded. In a meeting, and in subsequent e-mail exchanges, with Amnesty International, they stated that they were obliged to follow Belarusian law. They stated that they had shared information on international standards with Belarusian authorities and had raised "challenges" to problematic government practices regarding user data, but declined to provide examples. Telekom Austria Group do not publish transparency reports or other information regarding legal frameworks or practices governing access to Velcom customer data in Belarus.[187] Accordingly, it appears that Telekom Austria Group is failing in its duty to exercise its due diligence obligations regarding human rights concerns arising from the operations of its wholly-owned Belarusian subsidiary, Velcom.

The other telecoms and internet companies to whom Amnesty International write – Velcom, Life:), MTS (Belarus), Beltelecom, América Móvil and Turkcell – did not respond to our letters. Our desk research was not able to identify information in the public domain to indicate that these companies have taken steps to identify, prevent, mitigate or account for the human rights consequences of their operations. Accordingly,

---

[178] http://www.life.com.by/private/about/life/myi_-_chast_bolshoy_gruppyi
[179] http://www.teliacompany.com/en/about-the-company/markets-and-brands/turkey/
[180] http://www.telekomaustria.com/en/group/belarus; http://www.telekomaustria.com/en/ir/shareholder-structure
[181] See Freedom Online Coalition, WG2: Rule of Law Blog Series, Blog #2: Direct Access Systems and the Right to Privacy, https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-2/direct-access-systems/
[182] http://www.telecomindustrydialogue.org/
[183] http://www.teliacompany.com/en/sustainability/reporting/law-enforcement-disclosure-report/
[184] http://www.teliacompany.com/globalassets/telia-company/documents/about-teliasonera/public-policy/teliasonera_group-policy_freedom-of-expression-in-telecommunications.pdf
[185] E-mail correspondence 25 May 2016, on file with Amnesty International. Turkcell did not respond to Amnesty International's request for information.
[186] UN Guiding Principles on Business and Human Rights, Principle 17(a), http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf
[187] Telephone meeting with representatives of Telekom Austria Group, 9 June 2016. Velcom did not respond to Amnesty Internationals' request for Information.

and in the absence of evidence to the contrary, they appear to be failing in their duty to exercise due diligence regarding these human rights concerns.

# 8. CONCLUSION

The law in Belarus allows the authorities to undertake wide-ranging surveillance for nearly any reason, and does not require independent judicial authorization or oversight. Through the use of the SORM system, authorities have direct, non-stop, remote control access to communications and associated data. Mobile phone and internet providers, and other telecommunications companies facilitate this problematic direct access to the data of their customers. The pervasive secrecy surrounding surveillance practices make it nearly impossible to know about, let alone challenge, unlawful surveillance practices. This system falls far short of what international law and standards require in order for surveillance to be a lawful tool of law enforcement.

The use of private data and communications to prosecute people following the 2010 elections sent a message to many Belarusians that they should presume they are at perpetual risk of surveillance.

This has a debilitating effect on civil society in Belarus, already severely constrained by the restrictive legal framework that governs other aspects of their work in Belarus. Because such legitimate acts as acting on behalf of an unregistered organization or attending a peaceful protest may lead to prosecution, many activists self-censor and refrain from exercising their rights. Their legitimate work becomes more difficult as a result, as simple tasks such as seeking funding for their organization, making phone calls, or arranging meetings become fraught with risk – real or perceived.

While the use of encryption and other privacy tools can help protect some private data, it cannot obviate the risks of surveillance that activists face. Mobile phones may still be used to listen to private conversations and track locations. Computers and phones remain vulnerable to hacking, and the authorities have the power to confiscate devices, leading activists to fear using them further.

The chilling effect this causes leads to a shrinking space for civil society and has a detrimental impact on human rights across Belarus, including the right to information, as fewer and fewer activists, independent journalists or others are able to present views that contradict official ones.

The chilling effect that results from the fear of surveillance is not an accident. Comparing surveillance in Belarus to international law and standards, notably the *Zakharov* judgment of the European Court of Human Rights, underscores that this chilling effect is the direct result of the law and practice governing surveillance. This causes violations of the rights to privacy, to free expression, to peaceful assembly, to association and others. The government violates these rights not only when it directly targets activists for surveillance because of their legitimate work, but also through the maintenance of laws and practices around surveillance that drive people to self-censor.

# 9. RECOMMENDATIONS

## 9.1 TO THE EXECUTIVE AND LEGISLATIVE BRANCHES OF GOVERNMENT OF BELARUS:

1. Reform laws governing surveillance - including the Law on Operational Search (No. 307-Z of July 15, 2015) and the Criminal Procedure Code – to bring the legal regime and related surveillance practices in line with international human rights law and standards.
2. Ensure that the public has access to information related to surveillance law and practice at least to the extent provided in *The Global Principles on National Security and the Right to Information ("Tshwane Principles")*.
3. Among other things, measures should be taken with a view to ensure that:

    - State authorities are required to submit judicially authorized requests for data to telecommunications providers, rather than be given direct, remote-control access
    - Telecommunications providers are not required to retain communications-related data outside the context of ongoing criminal investigations and on the basis of a judicial warrant containing proper individualisation and reasonable suspicion of wrongdoing
    - Interception and access to communications and-related data can occur only when authorized – or respectively renewed - by an independent judicial body required to assess the existence of individualized reasonable suspicion of wrongdoing by the target of surveillance and otherwise to be satisfied that the requirements of necessity and proportionality are met
    - Legal grounds justifying secret surveillance, including the definition of "national security", are set in law and sufficiently narrowly circumscribed to meet a standard of clarity and precision that is sufficient to ensure that individuals have proper indication as to the circumstances which can lead to surveillance
    - Secret surveillance powers are supervised by a truly independent oversight authority which is adequately resourced, transparent to the public, has access to all information, and has the power and mandate to detect, investigate, put an end to, and provide remedies for, abuses of human rights linked to secret surveillance.

- The law is amended to set clear limits on the duration of secret surveillance in all cases.
- The law sets clear requirements for the destruction of all surveillance related data.
- Targets of secret surveillance are notified that they were subject to surveillance wherever it does not jeopardise, or no longer jeopardises, the legitimate purpose of an ongoing investigation.
- People have access to effective remedies and are allowed to challenge surveillance measures, or abuses of their rights linked to surveillance, before independent courts providing all necessary guarantees of due process.
- Sufficient information about the technical specifications of surveillance systems, including hacking tools, is made publicly accessible.

## 9.2 TO PROSECUTORS:

Pending authority for the authorisation of secret surveillance being transferred to an independent judge, prosecutors should:

1. Ensure that requests for secret surveillance are authorized only when based on individualized reasonable suspicion of wrongdoing by the target, and when such requests meet the requirements of necessity and proportionality.

2. Publish regular public reports detailing – at a minimum – the number of requests for secret surveillance made, approved and rejected, disaggregated by requesting authority and legal basis.

3. Ensure that no authorization is granted on the basis of the exercise of human rights, including participation in unregistered groups or participation in any peaceful assemblies.

4. Exercise powers to oversee the conduct of surveillance measures, and where there is evidence of violations of the law or human rights, ensure they are terminated, and those responsible held to account.

## 9.3 TO AUTHORITIES CARRYING OUT OPERATIONAL SEARCH:

Pending the adoption of the reforms recommended above:

1. Publish regular public reports detailing – at a minimum – the number of requests for secret surveillance made, approved and rejected, disaggregated by legal basis.

2. Publish information on the numbers of times SORM technology was used to access data, and the legal basis for such uses.

3. Refrain from seeking authorization for surveillance based on the exercise of human rights, including participation in unregistered groups or participation in any peaceful assemblies.

# 9.4 TO TELECOMMUNICATIONS COMPANIES:

1. Carry out human rights due diligence to identify, prevent, mitigate and account for human rights impacts of your operations, or those of your subsidiaries, in Belarus and elsewhere, including – at a minimum - by:

    - Challenging legal requirements which conflict with international human rights law and standards
    - Regularly publishing data about the number of requests for, and instances of, access to customers' communications and related data. Where this is not possible, publish detailed and accessible information regarding the legal framework and practices governing disclosures of customer data to government authorities.
    - Pushing for renegotiation of requirements for the application of SORM, and for revision of legal or other obligations to disclose customer data in a manner inconsistent with international law and standards.

# AMNESTY INTERNATIONAL IS A GLOBAL MOVEMENT FOR HUMAN RIGHTS. WHEN INJUSTICE HAPPENS TO ONE PERSON, IT MATTERS TO US ALL.


CONTACT US

info@amnesty.org

+44 (0)20 7413 5500

JOIN THE CONVERSATION

www.facebook.com/AmnestyGlobal

@AmnestyOnline

# “IT’S ENOUGH FOR PEOPLE TO FEEL IT EXISTS”

## CIVIL SOCIETY, SECRECY AND SURVEILLANCE IN BELARUS

The law in Belarus allows the authorities to undertake wide-ranging surveillance for nearly any reason, and with no independent oversight. This system of secret surveillance has had a debilitating effect on civil society in Belarus, whose work is already seriously undermined by the threat of criminal or administrative punishment merely for exercising their human rights, such as by attending protests.

In this environment, the fear of surveillance creates a chilling effect that makes even basic daily tasks – such as making phone calls, arranging meetings and planning public events - more difficult and dangerous. Mobile phones may listen in on private conversations, track users’ locations, and reveal with whom a person has met. Private information from e-mail or social media accounts can land activists in legal jeopardy if exposed through hacking.

The system in Belarus allows few remedies in practice for those whose rights are violated by surveillance. This system is facilitated by the cooperation of Belarusian and foreign telecommunications companies, who grant the government direct access to customers’ communications and data via the SORM system.

This report contains recommendations to the Belarusian government as well as to Belarusian and international telecommunications companies to bring an end to surveillance-related human rights abuses in Belarus.

INDEX: EUR **49/4306/2016**
JULY 2016
LANGUAGE: ENGLISH

**amnesty.org**

AMNESTY INTERNATIONAL