GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

BULGARIA

Zigzagging away

BlueLink.net
Pavel Antonov
www.bluelink.net

Introduction

Over 40 representatives of internet service providers (ISPs) gathered on 10 June 2014 in the imposing grey building of Bulgaria's Ministry of Interior (Министерство на вътрешните работи – MVR). The meeting was called by the State Agency of Technical Operations (Държавна агенция „Технически операции" – DATO) and did not go easy, according to a report by Bulgaria's authoritative business weekly Capital. ISPs were asked to provide DATO and the State Agency for National Security (Държавна агенция „Национална сигурност" – DANS) with unlimited real-time access to all internet traffic, with data storing options. Apart from concerns that the cost of equipment and technology necessary for fulfilling such a request might be too high, especially for smaller providers, it raised alarm for at least two more reasons: it confronted recent civil society accomplishments against excessive surveillance in Bulgaria; and the piece of European Union (EU) law that it was legally grounded in had just been abolished by the Union's highest court in Luxemburg.

This report seeks to explain the political and policy context that perpetuates internet surveillance by Bulgaria's security services and averts civil society's efforts to limit them. The following analysis is based on unstructured online interviews and query responses from internet rights activists, ISP proprietors and members of the "Free and Neutral Internet" Bulgarian language group on Facebook[1] during April-May 2014.

Policy and political background

In fact, DATO's surveillance requirements were anything but new. They were added to Bulgaria's Electronic Communications Act (Закон за електронните комуникации – ZES) back in 2010 to comply with the EU's Data Retention Directive 2006/24/EC. The former EU Data Retention Directive was originally transposed into MVR's Ordinance 40 as early as 2008, but its texts regarding access to stored information were cancelled by Bulgaria's Constitutional Court in 2009 and consecutively added to ZES. Remarkably, Ordinance 40 was never cancelled and is still technically in force, including a requirement for ISPs to send yearly reports to the Minister of Interior.

The ZES surveillance provisions oblige telecommunications operators to ensure real-time possibility for security services to "capture" electronic messages, "monitor" communication continuously, and access "data related to a certain call". If real-time is not possible, ISPs should provide requested data as soon as possible. They need to also maintain special interfaces that allow the transferring of captured electronic communication to DATO and DANS, following specifications approved by DATO's chair. ISPs are expected to both provide details about every call and its content, and establish the identity of their users. But no one ever put pressure on ISPs to actually implement these requirements, so they never did – apart from the country's three GSM (mobile) operators, *Capital* reported.[2]

A separate Special Surveillance Devices Act adopted in 1999 stipulates that surveillance requests can be filed by MVR, DANS or a prosecutor's office. Then a district judge's approval is required before DATO implements them.

On 8 April 2014 the European Court of Justice invalidated the EU's Data Retention Directive because it contradicts the Union's human rights and personal protection principles.[3] But how to comply with the ruling was left up to each member state to decide. And while none of the political parties represented in Bulgaria's parliament have made a move to ease ZES's draconic e-surveillance requirements since April, all of a sudden in June DATO called up ISPs asking them to tighten their implementation.

The "state" of state security

It was not a coincidence that the awkward meeting between ISPs and law enforcement agencies took place in the once notorious building which used to

1 https://www.facebook.com/groups/bginternetfreedom

2 Mihaylova, P. (2014, June 20). Op. cit.

3 Court of Justice of the European Union. (2014, April 8). Press release №54/14: The Court of Justice declares the Data Retention Directive to be invalid. curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

host the most redoubtable units of the Committee for State Security – Bulgaria's equivalent of the KGB during the authoritarian rule of 1944-1989. Haunted by memories of mass surveillance and terror from these times, Bulgaria's civil society has been alert for over two decades against the activities of the former and present – supposedly reformed – security and enforcement agencies of its democratic government. And for a good reason: the former regime's state security staff, agents and informants have held a tight grasp of Bulgaria's post-socialist politics, governments, business and mass media.[4] As a result, over the years, the public saw various initiatives fail or get significantly watered down,[5] while individuals and groups linked to the former state security apparatus almost inevitably held political and economic power.

Instead of getting its security services reformed and accountable, Bulgaria's democratic institutions seemed to be getting subdued and further infiltrated by them, their non-transparent and manipulative methods, and their abusive and controlling culture. The country's late accession to the EU in 2007 did not bring the expected improvements, and progress monitoring reports by the EU indicate systematic problems with the independence of the judiciary and corruption of authorities and law enforcement,[6] while Freedom House reports reflect a decline in freedom of speech and human rights, among others.[7]

Civil society to the rescue

For a while the third sector compensated to some extent for the decline of democratic institutions. Empowered by the increasing availability of high-speed internet in Bulgaria, social networks like Facebook and Twitter, or local networking sites such as Association for Progressive Communications (APC) member BlueLink.net,[8] mass protests in 2012 forced Bulgaria to retract from signing the Anti-Counterfeiting Trade Agreement (ACTA).[9] Suggestively, its centre-right government at the time was led by Prime Minister Boyko Borissov, who had started his political career as Chief Secretary of MVR and held a police general's rank. In spite of backing off from ACTA, Borissov's government was accused of excessive and often illegitimate use of electronic surveillance.[10] Allegedly, the main illicit surveillance culprit was Borissov's interior minister at the time and trusted in-party ally Tsvetan Tsvetanov. A former Police Academy gymnastics instructor, Tsvetanov was criticised for – and eventually charged with – sanctioning allegedly illicit eavesdropping by security services.[11]

An escalating row of public protests over a piling number of environmental and social problems eventually forced Borissov's government prematurely out of power in February 2013. Soon after, senior prosecutors investigated MVR to discover a lack of clear rules on the use of surveillance and dereliction of duty by senior officials, and faced obstruction by an official who allegedly destroyed evidence.[12] Already in opposition, Tsvetanov was taken to court on various counts related to the use of surveillance equipment and eavesdropping; final rulings are pending. Raychin Raychev, chair of Future 21 Century Foundation and an internet rights activist based in Plovdiv, found it only natural that the internet and other surveillance peaked during the rule of Borissov. He blamed the phenomenon on the mentality and origin of key government figures and Borissov himself; then their snobbishness and eagerness to show off.

Mounting criticism created an expectation that the government of Bulgaria's Socialist Party and Muslim minority-based Movement for Rights and Freedoms that took power after preliminary elections would significantly tighten up surveillance procedures and decrease surveillance practices. But an analysis by the Sofia City Court released in February revealed a disappointing discovery: phone and internet tapping requests were actually on the rise during the next government's tenure in office.

4 Hristov, H. (2013). Държавна сигурност и влиянието върху политическия елит по време на прехода [State security and its influence over the political elite during the time of transition]. Report presented at the East Europe's Transition in the Documents of Communist Secret Services conference held by the Committee for disclosing and announcing affiliation of Bulgarian citizens to the State Security and Intelligence services of the Bulgarian People's Army, Sofia, Bulgaria, 26 November. www.comdos.bg/media/Novini/Doklad-Hr.Hristov-26-11-2013.doc

5 Ibid.

6 European Commission. (2014, January 22). *Report from the Commission to the European Parliament and the Council: On Progress in Bulgaria under the Co-operation and Verification Mechanism*. ec.europa.eu/cvm/docs/com_2014_36_en.pdf

7 Freedom House. (2014). *Freedom of the Press Report: Bulgaria*. www.freedomhouse.org/country/bulgaria

8 www.bluelink.net

9 Chipeva, N. (2012, February 11). Thousands march in Bulgarian cities against ACTA: Photo gallery. *The Sofia Echo*. sofiaecho.com/2012/02/11/1764539_thousands-march-in-bulgarian-cities-against-acta-photo-gallery

10 Nikolov, K. (2013, April 20). Гарантирано от ГЕРБ: Пълен произвол с подслушването [Guaranteed by GERB: Completely Arbitrary Surveillance]. *Mediapool*. www.mediapool.bg/garantirano-ot-gerb-palen-proizvol-s-podslushvaneto-news205487.html

11 Leviev-Sawyer, C. (2013, April 16). Borissov and GERB back Tsvetanov in eavesdropping controversy. *The Sofia Globe*. sofiaglobe.com/2013/04/16/borissov-and-gerb-back-tsvetanov-in-eavesdropping-controversy

12 Ibid.

The Court reported some 8,345 requests for phone and internet traffic surveillance filed during 2013 by the police and DANS, with each request containing tens of phone numbers and IP addresses.[13] The number appeared to have grown significantly compared to 2011, when the requests were 6,918, although court refusals had also increased from 12% in 2012 to 14.3% in 2013.

The number of cases where law requirements were neglected is on the rise, confirmed Atanas Chobanov, a Paris-based investigative journalist and co-publisher of *BalkanLeaks.eu* and whistleblowing online journal *Bivol.bg*. He sees the genesis of the problem in the fact that the secret services have access to the technical possibilities for surveillance and it is easier for them to use it, in spite of using other methods for investigation which are supposed to be used first. As a WikiLeaks' Bulgarian partner, *Bivol.bg* revealed in 2013 that Bulgaria's government is among the clients of FinSpy – a software product by Dreamlab and Gamma International, specialised for internet and phone surveillance.[14]

Internet surveillance is as serious as it was in the beginning of the previous government's term, commented Delian Delchev, a senior networking engineer and IT consultant based in Sofia. Delchev, who is the administrator of the Free and Neutral Internet Bulgarian language group on Facebook, assessed all recent attempts to reform surveillance mechanisms as incomplete, including the separation of DATO from MVR's structure and allowing DANS, the military and customs to request surveillance requests directly. Another reason for concern for Delchev is the political appointment of DATO's chair, whose position is not subject to any public or civic scrutiny and accountability.

The increase in the number of requests was not the only sign of policy zigzagging over e-surveillance. In May 2014 state prosecutors suddenly burst into the offices of DATO and DANS to investigate the legality of their surveillance methods and practices.[15] Just a month later DATO suddenly became eager to get ISPs to fulfil their surveillance obligations under ZES.

Respecting laws and changing laws

In spite of all this most ISPs fulfil their obligations under ZES article 250a consciously and respect the law, said Assen Totin, a former ISP manager, now working for a small telecommunications operator. It is smaller "one-block LAN [network]"-type providers who turn a blind eye to the law, not making any effort to comply with it. "Not because they embrace the European Charter for Human Rights, but because most Bulgarians think that the laws apply for everyone else but them – and it is a pity that no one can bring them back to shape," Totin commented. The EU's Data Retention Directive may be invalidated, but Bulgarian law provisions that comply with it are still valid and no serious operator could unilaterally decide to stop complying with them, Totin explained. Failure to do so might lead to substantial fines of up to USD 68,400 – a serious amount even for large players. Benefits from non-compliance are questionable, with substantial possibilities for negative consequences in terms of bad public relations, said Totin.

But as an industry insider he sees clearly how hard it is for providers to comply with e-surveillance obligations. Larger operators receive some tens of requests for data access every day. Handling them requires a great resource of people, labour and so on, especially given that in order to "cover" a specific subject of "operational interest", much more information is often required than actually needed. For example, instead of simply asking whether X was in area Y at a given point in time, a request arrives that information of all users who appeared in the area should be handed over. And little of the requested information is acceptable as legitimate proof by Bulgarian courts, Totin explained. The Committee for Protection of Personal Data (Комисията за защита на лични данни – KZLD) is the body authorised under ZES to keep track of ISPs' compliance with this part of the law – namely, whether data under article 250a is accessible only for the appropriate persons, whether it is destroyed afterwards and so on. ISPs account in front of KZLD on a yearly basis. Totin thinks that the committee did a lot to make the life of ISPs easier, and listened to most recommendations by larger operators and by the Society of Electronic Communications – one of the professional associations in the sector – particularly with regard to legitimising refusals of access to information whereby a request did not meet the requisites of the law, and also in defending the ISPs' position that they should not interpret the data provided.

A representative of another trade association, the Society of Independent Internet Suppliers, was quoted by *Capital* as saying that DATO's requests

13 Sofia News Agency. (2014, February 17). Number of Surveillance Requests in Bulgaria on the Rise. *Novinite.com*. www.novinite.com/articles/158260/Number+of+Surveillance+Requests+in+Bulgaria+On+the+Rise

14 Bivol. (2013, September 4). WIKILEAKS: БЪЛГАРИЯ РЕАЛНО ИЗПОЛЗВА ШПИОНСКИЯ СОФТУЕР FINSPY [WikiLeaks: Bulgaria effectively uses FinSpy spying software]. *Bivol.bg*. https://bivol.bg/finspy-bulgaria.html

15 Angarev, P., & Dachkova, D. (2014, May 16). Прокуратурата изненадващо влезе в спецслужбите заради подслушването [Prosecutors surprisingly entered into special services because of surveillance]. *Sega*. www.segabg.com/article.php?id=698787

are unconstitutional and in breach of EU law and individual privacy rights, and that ISPs might sue the state in the International Human Rights Court in Strasbourg over them.

As former associate to the Sofia-based Centre for the Study of Democracy, Totin believes that abiding by applicable law is a must in a democratic society, and that there are legitimate ways to change a bad law. A couple of days after the EU court's decision was announced, Totin sent a complaint to the Ombudsman's Office as a private individual, asking him to alert the Constitutional Court. Ombudsman Konstantin Penchev was quick to act and a case is now pending at the Constitutional Court for the cancellation of the ZES requirements affected by the cancelled directive.[16] There is a proposal to get an opinion from the Communications Regulation Committee (Комисия за регулиране на съобщенията – KRS) and all interested parties might send their opinions to them. Eventual success in the Constitutional Court might be of substantial importance for demonstrating the superiority of public interest over applicable law.

Conclusions

For 25 years since 1989, Bulgaria's political and economic landscape remains marked by power structures linked to the security services of the former authoritarian regime. The style and methods of the former state security persist in today's unreformed security and enforcement agencies that tend to practise excessive and often unnecessary internet surveillance. Internet surveillance is over-regulated, with different regulations appearing in various legal texts, and regulated by different bodies. Policy zigzagging and conflicting signals sent by different institutions and politicians – depending if they are in opposition or in power – creates the sense that no significant motivation to limit internet surveillance exists in Bulgaria's governing circles. With business, politics, mass media and justice marked by corruption, non-transparency and lack of public accountability, civil society remains often the most viable guardian of privacy and human rights online. EU institutions, a few independent journalism publications, and the few functioning democratic institutions, such as the Ombudsman, also play their part.

The cancellation of the EU's Data Retention Directive by the European Court of Justice offers Bulgaria and all member states a great opportunity to redesign their national legislations so that internet surveillance should not hamper fundamental rights of privacy and freedom of expression. But the resistance of conservative structures linked to the state security apparatus slows down and often reverses such changes. A paralysing legal and administrative framework imposes new technological and financial burdens on ISPs who are willing to comply with data retention and surveillance requirements. The idea of refusing to comply with the applicable law's draconian requirement is new to most ISPs, but there is already the thought of legally challenging the obsolete national law provisions. Conscious citizens and internet connectivity proprietors abide by the law, but are willing to take legal action to remove the obsolete legal texts that force them to spy on internet and phone users.

Action steps

Some steps that could lead Bulgaria to resolving the problems with excessive and sometimes illicit internet surveillance include:

- An in-depth assessment of the existing administrative and legal framework to establish all norms and agencies that regulate internet surveillance.
- Conceptualising a complex set of changes that would lead to minimising the number of surveillance requests and strengthening the ability of both special services and ISPs to cooperate effectively.
- Having Ordinance 40 of MVR ultimately cancelled.
- Raising public awareness of the negative implications of excessive internet surveillance and creating political demand for limiting it; limitations that politicians need to comply with when they get elected.
- Building broad coalitions of actors who are interested in limiting internet surveillance, including ISPs, human rights advocates, pro-democracy think tanks and other groups that could participate in decision making when it comes to surveillance.
- Removing the internet surveillance provisions related to the former EU Data Retention Directive from ZES.
- Concentrating efforts on policy advocacy at the EU level to obtain a favourable replacement for the cancelled Data Retention Directive that would have a lasting impact over internet surveillance policies at national and EU level.

16 Mihaylova, P. (2014, June 20). Op. cit.