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

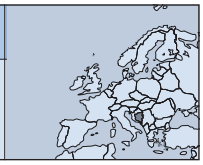
Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

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

BOSNIA AND HERZEGOVINA

The continuum of surveillance in Bosnia and Herzegovina



OneWorld Platform for Southeast Europe (OWPSEE) Foundation
Valentina Pellizzer and Aida Mahmutovic
www.oneworldsee.org

Introduction

Dissent has its grounding in the understanding of individuals, groups or communities about their entitlement to rights. When it comes to privacy, security, and the internet in general, citizens in Bosnia and Herzegovina are still far from considering themselves entitled to rights. Yet like anyone else in the world they actively use technology and social media to get informed and communicate with friends.

Activists use the internet and in particular social networks such as Facebook to engage the general public and to organise protests against the political establishment. For many who do not know much about Bosnia and Herzegovina, the immediate association is with the Balkans War of the 1990s and the fall of Yugoslavia. For human rights activists, Bosnia and Herzegovina holds the title of the most corrupt country in the western Balkans. It is also the only country in the region which still has to sign the pre-accession agreement to the European Union due to a stalemate on constitutional reform and the unwillingness of its politicians to negotiate necessary cross-party agreements and to go beyond rigid ethnic quotas. A good example of this situation is the country's failure to comply with the anti-discrimination decision of the European Court of Human Rights in the case of Sejdic-Finci[1] regarding his eligibility for official posts. This meant five years of deadlock on constitutional reforms, and left citizens of Bosnia and Herzegovina trapped in the narrow and discriminatory framework of the Dayton Peace Agreement.[2]

Policy and political background

The primary purpose of the Bosnia and Herzegovina legislative and administrative system is to enforce the rigid ethnic divisions in the country set up by the Dayton Peace Agreement, rather than developing policies and laws which respond to the needs of the country and its people. This ethnic structure constantly traps any new policy, law or decision that needs to be taken or developed in futile disputes about jurisdiction among the existing 14 governmental or legislative levels: the state, two entities, one district and ten cantons.

The agency for the information society was supposed to be the state's concrete mechanism for developing, coordinating and overseeing the information and communications technology (ICT) sector, as described in policy and strategy documents signed by the Council of Ministries in 2004. But this never happened, with the effect that the sector lacks a serious and consistent development strategy.

Dependent on a plethora of bodies and authorities whose mandates are often not understood, citizens struggle to believe in or even follow the work they do, and very often remain passive spectators of violations.

The bodies with competences on security, privacy and surveillance at state level are the Personal Data Protection Agency (AZLP, *Agencija za zaštitu ličnih podataka u Bosni i Hercegovini*);[3] the Agency for Identification Documents, Registers and Data Exchange (IDDEEA, *Agencia za identifikacione dokumente, evidenciju i razmjenu podataka*); the Ministry of Security; the sector for combating terrorism, organised crime, corruption, war crimes and misuse of narcotics; the sector for IT and telecommunication systems; the entity ministries of interior and the Brcko district; police apparatuses at entity and cantonal level; and the judiciary. In 2008 the Republic of Srpska created its own agency for the information society to act as a central body for policy and regulation on ICTs and the internet.

From wiretapping to the internet: Someone is listening to us...

When we started to research the right to privacy and surveillance in Bosnia and Herzegovina, we suddenly realised how short our memory sometimes

1 Wakelin, E. (2012, October 31). The Sejdic and Finci Case: More Than Just a Human Rights Issue? *E-International Relations*. www.e-ir.info/2012/10/31/the-sejdic-and-finci-case-more-than-just-a-human-rights-issue-for-bosnia-and-herzegovina

2 The General Framework Agreement for Peace in Bosnia and Herzegovina, 1995. www.ohr.int/dpa/default.asp?content_id=380

3 www.azlp.gov.ba/o_agenciji/nadleznosti/default.aspx

is. We immediately came across dozens of articles on wiretapping and illegal interception by various intelligence agencies, among others.

We suddenly realised that privacy in Bosnia and Herzegovina is more threatened than we thought, and that the internet simply serves as a new way in which information can be obtained, in violation of privacy rights. When talking to civil society representatives and participants in workshops on online safety for youth and women, their answers confirmed the assumption that there is almost a non-existent level of awareness on the right to privacy and information amongst the average citizen.

In 2011 *Nezavise Novine,*[4] a daily newspaper from Republic of Srpska published a list with more than 5,000 phone numbers under surveillance by the security intelligence agency OSA and the State Agency for Investigation and Protection (SIPA). Among people wiretapped from 2008 to 2010 were security experts, lawyers and representatives from the civil society sector. The newspaper at the time defined this as a cancer that started in Sarajevo, and spread to the rest of the country. It also accused the international community of being involved. Journalists were also reporting that Bosnia and Herzegovina intelligence was targeting international diplomats, and that in 2009 during his visit to the country, the director of the US Federal Bureau of Investigation (FBI) had asked that top officials from the Ministry of Security be dismissed.

In 2013 Zoran Čegar, chief of the police intelligence department in Bosnia and Herzegovina, admitted that the online communications of thousands of citizens, among them politicians, their wives and lovers, were intercepted with the purpose of blackmailing them. In both cases the public was not informed of any action taken, whether arrests or sanctions.

In March 2014 new leaks on the illegal interception of communications and wiretapping of journalists at the newspaper *Oslobodjenje* and the weekly paper *Bosni Herzegovina Dani* emerged. Excerpts from conversations between Zivko Budimir, president of the Federation of Bosnia and Herzegovina and Avdo Avdic, editor-in-chief of Federal Television, appeared on the internet. Vesna Budimir, the deputy state prosecutor and a candidate for appointment to the Supreme Court, also informed prosecutors that his communications had been illegally monitored and intercepted.

There is a pattern to all these scandals: the existence of parallel systems for intelligence structures that control legitimate security institutions – the result of former war intelligence agencies that never quite went away, and were not brought under the control of the new system.

Regardless how many reforms and new bodies are created, the constant practice of spying on people survives, and the authorities – as well as other interest groups – access the data held by public assets such as telecoms providers without court orders. Eavesdropping appears to be routine, which gives political leaders and their parties material for blackmailing and intimidating rival politicians, their partners and journalists. As Petar Kovacevic, director of the Agency for Personal Data Protection, said in an interview: "In 2007 the Council of Ministers formed a Joint Committee for the lawful interception of telecommunications, which has the authority to adopt procedures that govern the operation of telecoms operators." In this way it annulls the power of the Agency. It is important to know that the current chairperson of this committee is the deputy minister of security. When, in 2013, the agency checked on the three telecoms operators (BH Telekom d.d. Sarajevo, Telekom Srpske a.d. Banja Luka, and JP Hrvatske Telekomunikacije d.d. Mostar), to verify the lawfulness of personal data processing, and to understand if interception was taking place using court orders, the operators simply did not allow access to documents, claiming that they were "confidential". As a result the agency could not determine anything.

Personal data protection can easily be considered by many as irrelevant to public interest and reserved for police investigation. This was the case this year during riots and protests in Sarajevo (February 2014) where media footage and video footage from CCTV cameras was acquired by police authorities in order to identify people suspected of having caused damage to public property, and who were accused of "terrorism". Yet personal data protection all of a sudden became an inviolable human right when citizens asked to access and use the same CCTV footage to identify a court police driver who hit a protestor. Privacy rights are also being used as a way to avoid answering requests based on the access to information act, and to not provide information to investigative journalists or citizens regarding the salaries of public officers, among other things. As confirmed by the Agency for Personal Data Protection's report: "It is not rare that public administrative bodies use personal data protection or decisions by the Agency to hinder access

4 A. Ducic,Telekomi kriju podatke o prislu\u353\'61kivanju, Dnevni Avaz, 2014. www.avaz.ba/vijesti/teme/telekomi-kriju-podatke-o-prisluskivanju

to information to which citizens have a right, or to cover up certain irregularities in their work."[5]

Since existing legislation is not in line with European standards, authorities can easily find excuses to maintain the status quo.[6] In particular, the Law on Communications does not follow European standards because parliament failed to approve the amendments proposed in 2010. Other relevant laws are the Law on Personal Data Protection, already mentioned; the Law on the Protection of Secret State Information; a set of related provisions in the four existing criminal codes; and laws on criminal procedure, which all define the crime of unlawfully processing personal data.

Since public statements on transparency remain on paper rather than in practice, the role and work of the Agency for Personal Data Protection becomes essential, not only to establish the rule of law, but also to provide citizens with an independent body that they can turn to.

Citizens who have asked the agency to intervene have won all five cases of video surveillance against the Federation Ministry of Veterans and People Disabled in the Defence and Liberation War, the Federation Ministry of Finance, an elementary music school in Ilidza, the Golden Grain Bakery in Bratunac, G-Petrol Ltd. in Sarajevo, and a residential building at 17 Armije Street in Tuzla. The rationale in all cases was almost the same: video surveillance was being used against its declared function of securing property, and used instead as a means of intimidation, blackmailing and controlling employees. In the case of the music school, the headmaster allowed footage of the teachers' staff room to be uploaded to YouTube, and then used the ensuing scandal to dismiss a disobedient teacher who had been videotaped. The agency's decision was that people clearly need to know when areas are under surveillance, and who to contact for information regarding video surveillance. Video surveillance installed without knowing to whom it belongs, who can see the recordings, or who can hand these recordings to third parties, is unacceptable.

Conclusions

Over the years politicians have continued to use whatever a system allows to suit their own particular purposes. Ministries have changed, heads of security agencies and the police have been replaced, but the same scenario plays out with new people under surveillance, the same scandals but different names – and no solutions. The Agency for Personal Data Protection has introduced a new concept to authorities and even if it is fragile, it is trying to establish its reputation on new ground. In a closed system such as the one in Bosnia and Herzegovina, it is really important to refer substantially to legality, adequacy and proportionality, and introduce the concept of user notification.

Bosnia and Herzegovina, similar to all new democracies, has wonderful copy-and-paste laws in place, but they are mostly never implemented. The real power remains outside institutions, while rhetoric is used during official visits and good-sounding statements are produced easily. The participation of Bosnia and Herzegovina as a state in the global conversation around internet rights is non-existent, and security is understood in a very conservative way. The first action plan for children's online safety is a perfect example, with a blacklist, measures for parental control, internet service provider (ISP) responsibility and other conservative measures.

Traditional actors seem not to grasp the urgency and the necessity of moving beyond the usual scheme of endangered human rights. Technology and the regulation of telecoms remain a distant world approached only in terms of the potential for corruption, and privatisation.

There is a world of non-traditional activism that is represented by internet users which can recognise the connection between technology, online platforms and tools, and the policy and legislation surrounding them. This is unique.

Action steps

Participatory awareness campaigns that use visual tools are key to helping citizens value their personal information and data and to pressurise institutions to fulfil their role when it comes to privacy rights. Since its inception, the Agency for Personal Data Protection has slowly been receiving more expert input and extended its controls over institutional decisions. There is still a need to build a bridge between the work of the agency and the average citizen and to translate the complexity of personal data processing into personal stories.

Public opinion in Bosnia and Herzegovina had become so disillusioned about its ability to bring

5 Report by the Agency for Personal Data Protection, 2013.

6 The Report states: "The rules of the Council of Ministers about the participation of the Agency for Personal Data Protection in relevant legislative processes are not satisfactory. The principle of purposeful use and by-laws regulating the protection of personal data by the police have still not been fully implemented. The Law on Personal Data Protection does not apply to the Bosnia and Herzegovina Intelligence and Security Agency. Overall, preparations for personal data protection are still at an early stage. It is necessary to ensure the independence of the Agency for Personal Data Protection." European Commission Progress Report in Bosnia and Herzegovina, 2012.

about change. The silent majority is afraid to take risks, because it would be defending something it does not really understand, or is genuinely scared about the repercussions. In this as in other issues, it is important to leave behind the feeling of an overwhelming and invincible Big Brother that can see and control everything. To do this it is important to talk outside of the usual circles of activists, and also to produce and distribute information in a format that citizens can understand and use.

The internet has proved to be a space where people convene and take action in creative and personal ways, and more than ever has become the place where actions start: content is easily distributed and memes are generated. With a mobile phone penetration rate of 90.8%, an internet penetration of 56.96%, and a total of 2,188,429 internet users in 2013, this is the place where ongoing awareness campaigns can generate *ad hoc* coalitions ready to take up the challenge of creating a positive sense of privacy. This can help build campaigns against the continuum of surveillance and its pervasive expansion under the paternalistic vest of protecting vulnerable communities.