GLOBAL INFORMATION SOCIETY WATCH 2019

Artificial intelligence:
Human rights, social justice and development

Association for Progressive Communications (APC),
Article 19, and Swedish International Development Cooperation Agency (Sida)

Global Information Society Watch

2019

Global Information Society Watch 2019
Artificial intelligence: Human rights, social justice and development

Operational team
Valeria Betancourt (APC)
Alan Finlay (APC)
Mallory Knodel (ARTICLE 19)
Vidushi Marda (ARTICLE 19)
Maja Romano (APC)

Project coordination team
Valeria Betancourt (APC)
Cathy Chen (APC)
Flavia Fascendini (APC)
Alan Finlay (APC)
Mallory Knodel (ARTICLE 19)
Vidushi Marda (ARTICLE 19)
Leila Nachawati (APC)
Lori Nordstrom (APC)
Maja Romano (APC)

GISWatch 2019 advisory committee
Namita Aavriti (APC)
Rasha Abdul Rahim (Amnesty International)
Alex Comninos (Research ICT Africa)
Malavika Jayaram (Digital Asia Hub)
J. Carlos Lara (Derechos Digitales - América Latina)
Joy Liddicoat (Centre for Law and Emerging Technologies, University of Otago)
Andrew Lowenthal (EngageMedia)
Micaela Mantegna (Geekylegal/Machine Intelligence Lab, Center for Technology and Society, San Andres University)
Valeria Milanes (Asociación por los Derechos Civiles)

Project coordinator
Maja Romano (APC)

Editor
Alan Finlay (APC)

Assistant editor and proofreading
Lori Nordstrom (APC)

Publication production support
Cathy Chen (APC)

Graphic design
Monocromo

Cover illustration
Matías Bervejillo

We would like to extend a special note of thanks to a number of authors who have made ad honorem contributions to this edition of GISWatch.
We gratefully acknowledge the following:

Philip Dawson and Grace Abuhamad (Element AI)
Anita Gurumurthy and Nandini Chami (IT for Change)
Rasha Abdul Rahim (Amnesty International)

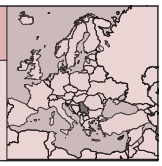
APC would like to thank the Swedish International Development Cooperation Agency (Sida) and ARTICLE 19
for their support for Global Information Society Watch 2019.

Published by APC
2019
Printed in USA

Global Information Society Watch 2019 web and e-book
ISBN 978-92-95113-13-8
APC Serial: APC-201910-CIPP-R-EN-DIGITAL-302

SERBIA

LIVING UNDER THE WATCHFUL EYE: IMPLICATIONS OF FACIAL RECOGNITION SURVEILLANCE IN SERBIA



SHARE Foundation
Bojan Perkov and Petar Kalezić
https://www.sharefoundation.info

Introduction

In early 2019, the minister of interior and the police director of Serbia announced[1] that 1,000 cutting-edge security cameras with facial recognition capabilities will be installed in 800 locations in Belgrade, the Serbian capital, in partnership with Chinese tech giant Huawei. However, despite the flaws of facial recognition and the intrusiveness for citizens' privacy when it is used for surveillance,[2] there is no transparency about the cameras and the partnership between the Ministry of Interior and Huawei, which is part of a broader cooperation between the Serbian and Chinese governments.

In November 2018, Serbia adopted a new Law on Personal Data Protection[3] based on the European Union's (EU) General Data Protection Regulation (GDPR).[4] The application of the law starts on 21 August 2019, after a nine-month adaptation period provided for compliance with the new rules. SHARE Foundation,[5] a Serbian non-profit organisation established in 2012 to advance human rights and freedoms online, submitted freedom of information requests to the Ministry of Interior asking for information about the cameras and supporting documents (e.g. memorandums, contracts, letters of intent). The Ministry withheld this information, meaning that the public in Serbia was left in the dark about a very problematic technology which can greatly impact the privacy of all citizens.

Legislative context

Similar to other countries with a history of repressive regimes and a broad state surveillance apparatus, there is little of a culture of privacy in Serbia. For example, the first data protection law in Serbia was adopted in 2008. After nearly 10 years of application, it turned out that the law was not good enough to provide an adequate level of protection, especially in a world of expanding technologies such as targeted advertising and a whole new digital economy based on personal data. Also, the law did not regulate video surveillance, which opened space for numerous abuses when it comes to data processing through CCTV systems, both state and privately owned. Introducing a new law was an opportunity to regulate this area of personal data processing, but the provisions on video surveillance were not included in the final text of the Law on Personal Data Protection.

In its annual report for 2018, the Commissioner for Information of Public Importance and Personal Data Protection, Serbia's independent authority for both freedom of information and protection of citizens' personal data, highlighted the fact that the Ministry of Justice argued to keep the regulation of video surveillance out of the new Law on Personal Data Protection. The Ministry's view was that this area of personal data processing should be regulated by a special law and that the GDPR does not contain provisions on video surveillance.[6] However, more than six months after the new Law on Personal Data Protection had been adopted in the National Parliament of Serbia and just two months before it is scheduled to start being applied, no specific law regulating video surveillance has been drafted or even proposed.

1 SHARE Foundation. (2019, 29 March). New surveillance cameras in Belgrade: location and human rights impact analysis – "withheld". https://www.sharefoundation.info/en/new-surveillance-cameras-in-belgrade-location-and-human-rights-impact-analysis-withheld

2 Big Brother Watch. (2018). *Face Off: The lawless growth of facial recognition in UK policing*. https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf

3 Republic of Serbia. (2018). Law on Personal Data Protection. Available in Serbian at: www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2018/87/13/reg

4 European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

5 https://www.sharefoundation.info/en

6 Commissioner for Information of Public Importance and Personal Data Protection of the Republic of Serbia. (2019). *Summary report on the implementation of the Law on Free Access to Information of Public Importance and the Law on Personal Data Protection for 2018*. https://www.poverenik.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2018/ENGRezime2018.pdf

Over the past six months, at the time of writing, Serbia has been in a state of political turmoil. There have been anti-government protests across the country after an opposition politician was assaulted by a group of men in December 2018.[7] It is in contexts such as these where facial recognition surveillance systems, which store large amounts of biometric data, could potentially be used for pressuring citizens who are protesting, as well as their families, because of their political views. Beyond political protest, the everyday use of the cameras comes with the risk of data breaches, which includes records of the daily routines and movements of citizens, and which could potentially result in harm to those unwittingly surveilled.

An opaque Panopticon: Citizens in the dark

As soon as Huawei's facial recognition cameras were announced in the media by the highly ranked officials in Serbia's internal affairs, SHARE Foundation decided to find out more about Huawei's cameras in terms of their location, public procurement and other relevant procedures by submitting freedom of information requests to the Ministry of Interior.

In their responses to our requests, the Ministry stated that all information about the procurement of Huawei cameras is "confidential" and therefore not for public access. Also, in an interview for Radio Television of Serbia, Police Director Vladimir Rebić said that the locations of stationary cameras were already determined based on "a broad examination and analysis of events, referring primarily to the criminal offences in Belgrade." We also requested a copy of this analysis, but the Ministry responded that the information, as well as the location of the cameras, were not contained in any document or other medium, meaning they cannot be provided upon a freedom of information request.[8]

According to Article 54 of the new Law on Personal Data Protection, if it is likely that certain data processing will present a high risk to the rights and freedoms of natural persons, the data controller is obligated to conduct a data protection impact assessment before the beginning of data processing.[9] When SHARE Foundation requested a copy of this impact analysis, the Ministry simply stated that the provisions of the new law are not yet being applied. Having read the official responses of the Ministry of Interior, which suggest that this information does exist, it seemed strange that information provided by a freedom of information officer about such a sensitive topic for citizens' privacy was contradictory to the statements made by the minister and the police director in the media.

While the Ministry was reluctant to provide any official information about the cutting-edge cameras and their procurement, Huawei on the other hand was more transparent about its cooperation with the Serbian authorities. A case study titled "Huawei Safe City Solution: Safeguards Serbia" was available on Huawei's official website and it provided detailed information about the cameras and related video surveillance solutions, claiming the cameras were already installed in Belgrade. SHARE Foundation published an article about Huawei's case study,[10] which strangely disappeared from the company's website shortly after the publication of our article. Having in mind the sensitivity of this content, we saved an archived copy[11] of the page so the case study can still be accessed online.

Huawei stated that for the test phase, nine cameras in five locations were deployed, with the locations being the Ministry of Interior headquarters, a sports arena, a commercial centre and a police station. After this test deployment, it is stated in the case study that Huawei and the Ministry achieved a Strategic Partnership Agreement in 2017 and that in the first phase of the project 100 high-definition video cameras were installed in more than 60 key locations, with the command and data centre in Belgrade being remodelled.[12]

It is very worrying that such advanced technology, which has great implications for privacy, is being deployed without citizens knowing about this digital "watchful eye" collecting and storing large amounts of their biometric data, even if they have done nothing wrong. Saša Đorđević, a researcher at the Belgrade Centre for Security Policy,[13] a Serbian think tank dedicated to advancing the security of citizens and society, said that

7 Vasovic, A. (2018, 8 December). Thousands protest in Serbia over attack on opposition politician. *Reuters*. https://www.reuters.com/article/us-serbia-protests/thousands-protest-in-serbia-over-attack-on-opposition-politician-idUSKBN1O70S7

8 SHARE Foundation. (2019, 29 March). New surveillance cameras in Belgrade: location and human rights impact analysis – "withheld". Op. cit.

9 Republic of Serbia. (2018). Op. cit.

10 SHARE Foundation. (2019, 29 March). Huawei knows everything about cameras in Belgrade – and they are glad to share! https://www.sharefoundation.info/en/huawei-knows-everything-about-cameras-in-belgrade-and-they-are-glad-to-share

11 https://archive.li/pZ9HO

12 SHARE Foundation. (2019, 29 March). Huawei knows everything about cameras in Belgrade – and they are glad to share! Op. cit.

13 www.bezbednost.org

although video surveillance can improve security and safety, primarily in road traffic safety, the list of unknown things about Huawei's video surveillance in Belgrade is long. "The situation can still be corrected if and when it is determined which video surveillance equipment is being purchased, how much it costs the citizens of Serbia, where it is placed and how the personal data will be processed and protected," he added.[14]

Another problematic aspect of facial recognition technology when used for video surveillance is that it is prone to mistakes, which is especially important for law enforcement and legal proceedings. Research by Big Brother Watch has shown that in the United Kingdom the overwhelming majority of the police's "matches" using automated facial recognition have been inaccurate and that on average, 95% of "matches" made by facial recognition technology wrongly identified innocent people as crime suspects.[15]

In addition, Big Brother Watch found that the police stored photos of all people incorrectly matched by automated facial recognition systems, meaning that biometric photos of thousands of innocent people have been stored.[16] Storing such sensitive biometric data of citizens is also a privacy and security risk, which is even greater taking into account information leaks during police investigations, which are common in Serbia. "The media in Serbia frequently publish information relating to investigations conducted by the police and the prosecution, quoting mostly unknown sources allegedly 'close to the investigation' and sometimes with photos," explained Đorđević. He mentioned an example when information from the investigation of the murder of a Serbian singer was constantly published on the front pages of tabloid newspapers. Another case Đorđević highlighted occurred in February 2017, when one daily newspaper covered the arrest of a member of a football club supporters' group on its front page the evening before the police informed the public about his arrest.[17]

In other parts of the world there are similar concerns. With all the recent controversy surrounding facial recognition, two cities in the United States have so far banned the use of facial recognition by the city administration – the first was San Francisco, California, followed by Sommerville, Massachusetts.[18] It is highly likely that more cities will join them, particularly since there is more and more awareness of the negative impacts of facial recognition surveillance.

Conclusion

SHARE Foundation will again approach the Ministry of Interior for information, especially relating to the data protection impact assessment of data processing using Huawei's cameras, after the application of the new Law on Personal Data Protection starts. Of course, data processing through video surveillance systems should be regulated without delay, either though amendments to the Law on Personal Data Protection or through a separate law. It is also important to introduce citizens to the risks of such invasive technologies and call them to action, as it will provide momentum to further pressurise the authorities and demand more transparency. People feel more secure when they see a camera, as Đorđević noted,[19] but there is also a general lack of understanding of who may collect their personal data, the purposes for which it will be collected, and their rights as data subjects.

Moreover, it is also necessary that the new Commissioner for Information of Public Importance and Personal Data Protection is appointed as soon as possible and in a transparent manner,[20] as the second and final term of Rodoljub Šabić, the previous Commissioner, expired in December 2018. As head of an independent institution, the Commissioner plays a key role in protecting citizens' personal data and freedom of information and it is of utmost importance that the position is given to a person who has personal integrity, expertise and political independence. Otherwise, affairs such as the one with Huawei's facial recognition cameras may never be resolved, which would leave citizens exposed to huge risks to their privacy and without appropriate safeguards in cases of data breaches and abuse of personal data. There will also be many doubts around how to apply the new Law on Personal Data

14 Email correspondence with Belgrade Centre for Security Policy researcher Saša Đorđević, 29 June 2019.

15 Big Brother Watch. (2018). Op. cit.

16 Ibid.

17 Email correspondence with Belgrade Centre for Security Policy researcher Saša Đorđević, 29 June 2019.

18 Haskins, C. (2019, 28 June). A Second U.S. City Has Banned Facial Recognition. *VICE*. https://www.vice.com/en_us/article/paj4ek/somerville-becomes-the-second-us-city-to-ban-facial-recognition

19 Email correspondence with Belgrade Centre for Security Policy Researcher Saša Đorđević, 29 June 2019.

20 Delegation of the European Union to the Republic of Serbia. (2019, 28 January). Fabrizi: Appointment of new Commissioner for Information of Public Importance should be kicked off as soon as possible. https://europa.rs/fabrizi-appointment-of-new-commissioner-for-information-of-public-importance-should-be-kicked-off-as-soon-as-possible/?lang=en

Protection, which could prove to be quite a challenge if the Commissioner is not up to the task or is easily influenced by other state institutions and political actors.

Action steps

Having taken into account the lack of transparency surrounding Huawei's surveillance cameras in Belgrade, we propose the following action steps:

- Insisting on the proper application of the new Law on Personal Data Protection and conducting the necessary data protection impact assessment.
- Advocating for the regulation of video surveillance by law in order to provide legal certainty.
- Engaging the wider community (e.g. civil society organisations, human rights defenders, tech experts, journalists) to help raise awareness among citizens about the impact of video surveillance.
- Pressuring the Ministry of Interior and other relevant state institutions to provide information about video surveillance and facial recognition in a transparent way.

GLOBAL INFORMATION SOCIETY WATCH 2019

Artificial intelligence:
Human rights, social justice and development

Artificial intelligence (AI) is now receiving unprecedented global attention as it finds widespread practical application in multiple spheres of activity. But what are the human rights, social justice and development implications of AI when used in areas such as health, education and social services, or in building "smart cities"? How does algorithmic decision making impact on marginalised people and the poor?

This edition of Global Information Society Watch (GISWatch) provides a perspective from the global South on the application of AI to our everyday lives. It includes 40 country reports from countries as diverse as Benin, Argentina, India, Russia and Ukraine, as well as three regional reports. These are framed by eight thematic reports dealing with topics such as data governance, food sovereignty, AI in the workplace, and so-called "killer robots".

While pointing to the positive use of AI to enable rights in ways that were not easily possible before, this edition of GISWatch highlights the real threats that we need to pay attention to if we are going to build an AI-embedded future that enables human dignity.

GLOBAL INFORMATION SOCIETY WATCH
2019 Report
www.GISWatch.org

APC
ARTICLE 19
Sida