HEINRICH BÖLL STIFTUNG
BRUSSELS

HEINRICH BÖLL STIFTUNG
WASHINGTON, DC

E-PAPER

Shaping the Future of Multilateralism

Biometrics in Belgrade: Serbia's path shows broader dangers of surveillance state

BY DANILO KRIVOKAPIĆ, MILA BAJIĆ AND BOJAN PERKOV

Published by Heinrich-Böll-Stiftung, May 2021

About the Author

Danilo Krivokapić is director of SHARE Foundation, Belgrade based digital rights organisation. Lawyer by education, his fields of work and expertise include data protection, impact of data-driven business models on privacy, legal standards for information security and cybercrime. He is a founder of the initiative #hiljadekamera (thousands of cameras), a community of individuals and organisations that advocate the responsible use of surveillance technology.

Mila Bajić works at SHARE Foundation on the protection of digital human rights and online freedoms. Her work focuses on the intersection of analogue and digital spheres, popular culture, conspiracy theories and visual theory and practice. Another important sphere of interest is assessing the negative effects of biometric mass surveillance technologies and practices and learning more about them. She is a CEU graduate where she obtained her MA in Nationalism Studies dealing with generational memories and attitudes. She is also working on the Strengthening Quality News and Independent Journalism in the Western Balkans and the Media Influence Matrix projects at the Center for Media Data and Society.

Bojan Perkov is a Policy Researcher at the SHARE Foundation. His interests and areas of work include freedom of expression and online media, as well as other issues related to digital rights and freedoms, such as hate speech, net neutrality, censorship, data protection, digital security, etc.

Contents

Biometrics in Belgrade: Serbia's path shows broader dangers of surveillance state

On the EU's periphery, Serbia has deployed enough biometric surveillance technology from China's Huawei for law enforcement and "Safe City" solutions to cover practically all of Belgrade's public spaces. Public pressure has raised the bar for turning on the technology, but the alarming project illustrates the need for transparent regulation of such systems everywhere, to ensure the protection of fundamental human rights.

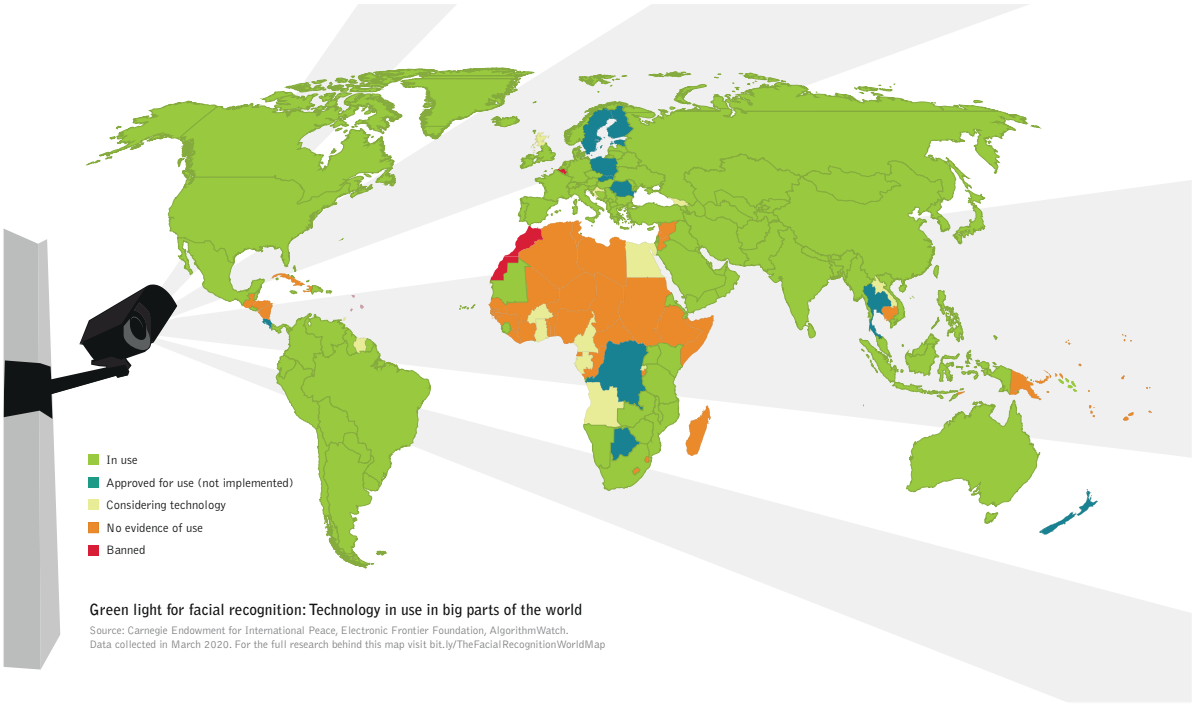
At the start of the pandemic in the early months of 2020, Serbia was one of the first countries in the world to impose a state of emergency and a strict statewide curfew. Dial forward to early 2021, and Serbia was near the front in the race for vaccinations per capita, after the United Kingdom. In between those two laudable markers, however, Serbia became a European pandemic pioneer in a more dubious field: citizen surveillance. As of early 2021, Belgrade was on track to become what we believe is the first capital in Europe with public spaces practically fully covered by cameras enabled with biometric technology for mass surveillance.

Thus far, the cameras appear to be used mainly for traditional video surveillance, but the biometric features could be activated with the turn of a switch. Growing pressure by civil society as well as a legal opinion by the Serbian data protection commissioner seem to have stalled the technology's deployment thus far, but many details of the program remain murky. The case illustrates the urgency for a clear ban on facial-recognition technology, not only in Serbia, but across Europe, rather than leaving loopholes for law enforcement, as does the European Commission's draft Artificial Intelligence (AI) Regulation.

Liberal democracies are missing an opportunity to strengthen civil liberties, as they persist in maintaining ambiguity in their positions on high-risk AI applications such as biometrics at a time when mass surveillance is becoming one of the biggest threats to human rights and data privacy. As of 2020, a study conducted by Surfshark reported that 109 countries are either using or have approved the use of facial-recognition technology for surveillance. In the United States, for instance, the facial-recognition software developer Clearview AI has won business from thousands of law enforcement agencies, including the U.S. Immigration and Customs Enforcement Agency (ICE). Clearview is known for its databases containing billions of photos scraped from social media sites and the internet more broadly. Government use of facial-recognition software in the United States spiked last year amid mass protests against police brutality and systemic racism and this year in the aftermath of the right-wing attack on the U.S. Capitol on Jan. 6, 2021, as law enforcement sought to identify protesters and rioters. Still, multiple U.S. cities have decided to refrain from using biometric surveillance until adequate regulation is passed. And lawsuits are beginning to take advantage of new laws in places like

San Francisco and Illinois aimed at curbing the use of facial-recognition technology that violates privacy rights.

However, there are some positive trends when it comes to curbing these mechanisms. In Sweden, for example, the Swedish Authority for Privacy Protection (IMY) investigated and cited police forces for their unauthorized use of Clearview AI facial-recognition services for identifying individuals.



Green light for facial recognition: Technology in use in big parts of the world

Source: Carnegie Endowment for International Peace, Electronic Frontier Foundation, AlgorithmWatch.
Data collected in March 2020. For the full research behind this map visit bit.ly/TheFacialRecognitionWorldMap

These examples are strong indicators of a growing awareness of the risks, but there is a lack of clear guidance from legislators. The European Commission's draft AI Regulation, which was released on April 21, 2021, is the most far-reaching attempt to address these issues so far, but from a civil rights perspective, it does not go far enough. The bill identifies "high-risk" applications, such as the use of biometrics or facial recognition, and subjects them to additional regulatory scrutiny. The measure would impose a ban on "real time" facial recognition in public spaces for the purpose of law enforcement, but it would also create exceptions for anti-terrorism measures and for other vaguely defined "serious crimes," creating risks of abuse and over-profiling of vulnerable minorities. Additionally the European Commission's own supervisory authority, the European Data Protection Supervisor (EDPS), strongly criticized the document, noting that: "A stricter approach is necessary given that remote biometric identification [...] presents extremely high risks of deep and non-democratic intrusion into individuals' private lives."

The unease among Serbian civil society but also among many European governments about facial recognition is compounded by the fact that these surveillance technologies primarily come from Chinese companies. This is understandable in light of China's well-established record of mass surveillance of its own citizens, the feared spying capabilities of Huawei and ZTE technology in the telecommunications sector, and China's push for economic and political influence over parts of Europe through an initiative dubbed "China and the Cooperation of Central and Eastern European Countries" (China-CEEC). This cooperation forum, established in 2013 and also known as the "17+1" group, includes Albania, Bosnia & Herzegovina, Bulgaria, Croatia, Estonia, the Czech Republic, Hungary, Greece, Latvia, Lithuania, North Macedonia, Montenegro, Poland, Romania, Serbia, the Slovak Republic, and Slovenia. The platform has become an entry point for China's Belt and Road Initiative (BRI) into Europe, through infrastructure investment and cooperation agreements with many EU member and candidate states.

Belgrade's introduction of its surveillance system has been cloaked in secrecy and public misinformation. On May 10, during a hearing in the Serbian Parliament, Assistant to the Ministry of Police (MoP) Slobodan Nedeljković, said publicly that the facial recognition system is not in use at the moment, in part because the Serbian data protection commissioner determined that there is no legal basis for processing of biometric data (more discussion on that below).

Moreover, such a deployment of mass biometric surveillance technology with so little transparency in a governance system compromised by corruption and public distrust can be nothing but dangerous at best, with the potential for breaches of privacy and other human rights violations. The experience of Belgrade and its citizens with this surveillance system thus far illustrates the need to raise public awareness, increase oversight, and study the effects of such systems across Europe and the globe.

In order to curb the potential detrimental effects of these practices, civil society organizations in Serbia and across Europe are raising awareness not only among the public but among policymakers on multiple levels about the risks of facial-recognition technology. A push via a European Citizens Initiative (ECI) to ban the use of facial recognition and to increase dialogue among government authorities, international organizations, and civil society is promising. But much more work is needed by Serbia and other countries, as well as by the EU, the Council of Europe, and similar bodies, and via courts such as the European Court of Human Rights (EctHR).

These European institutions as well as international, national, and local structures and data-protection authorities at all levels can take concrete steps toward protecting individual rights. In addition to responding to deployment of such technology, they must be proactive in preventing its use in the first place.

The road to biometric mass surveillance in Belgrade

Information technology (IT) companies are spearheading the expansion of China's international influence, both in political and economic terms. Companies such as Huawei or ZTE have aimed their efforts at markets in Africa and Latin America through infrastructure projects enabled by Chinese state loans. And Europe seems to be no exception.

According to a September 2020 report from the Washington-based Center for Strategic and International Studies (CSIS), Serbia is a hub for Beijing's ambitions in the Western Balkans. In addition to supplying biometric surveillance technologies made by Chinese companies, China is providing Serbian law enforcement with training on their use. This development is increasingly concerning, since Huawei has already been linked to major security scandals in other countries for acts such as systems hacking, stealing foreign data, and intercepting confidential information.

An important element of the technological cooperation between China and Serbia is the idea of "Safe Cities." Huawei is the strategic partner for implementation in the capital Belgrade as well as in the other two largest Serbian cities, Niš in the south and Novi Sad in the north. The cooperation is facilitated through the opening of an innovations and development center in the Serbian capital. Such a widespread deployment potentially sets the stage for the further spread of such technologies to other countries of the Western Balkans, and maybe at some point in the EU.

From the start, a shroud of secrecy surrounded the move to update Belgrade's video surveillance system with advanced features, such as facial- and vehicle license-plate recognition. The talks between the Serbian and Chinese governments date back to 2009, when they signed the first agreement on economic and technical cooperation on infrastructure. In 2011, the Serbian government started negotiations with Chinese tech giant Huawei concerning the "Safe Society" project, which stipulated the implementation of technology systems for increased surveillance of citizens in the country. The Memorandum of Understanding for the "Safe Society" project was signed between the Serbian Ministry of Interior (MOI) and Huawei in 2014.

But it was only in December 2017 when the ministry made its first major public announcement regarding the installation of the smart surveillance system in Serbia. In early 2019, the Minister of Interior gave a statement to Fonet news agency, and the Police Director of Serbia, whose force is part of the MOI, was interviewed on Radio Television of Serbia, each announcing that the project would be carried out over the next couple of years, and that it included the installation of 1,000 next-generation cameras enabled for facial and license-plate recognition in 800 locations across Belgrade.

The ministry is the data controller for the surveillance system, i.e. the entity responsible for ensuring all personal data processing is done in accordance with the law. All the data from the system is stored centrally in the ministry's Command & Operations Center, and the police have the authority to use information gleaned from the system for law enforcement purposes. Despite a new government taking office after elections in 2020 and a new interior minister being appointed, both remain controlled by the same ruling coalition led by the populist Serbian Progressive Party (SNS), which has a record of scandals involving technology. Namely, in March 2020, Twitter removed around 8,500 accounts linked to coordinated political propaganda efforts that were connected to SNS and that violated the social media giant's rules. More generally, SNS party officials are known for attacks and smear campaigns against political opponents, civil society and independent media.

In February 2019, as a result of the lack of specific information and broader public debate over such an intrusive system, SHARE Foundation, a Belgrade-based digital rights non-profit organization where we work, submitted a freedom of information request for relevant information, such as the locations of the cameras, how the locations were determined, and how the public procurement was conducted. The ministry denied the request, citing among other reasons the confidentiality of the public procurement documents, even though Huawei had published a detailed case study of the project on its website. Not long after SHARE Foundation published findings from Huawei's case study in March 2019, the information was removed from the company's website, though the page was archived online and remains accessible.

The ministry has been forced to submit to a certain degree of civil liberties scrutiny since a new Law on Personal Data Protection (LPDP) took effect in August 2019, aimed at aligning Serbia's data protection framework with EU standards. Under the law, data processing such as through massive video surveillance systems in public spaces requires a Data Protection Impact Assessment (DPIA) that must be approved by an independent Commissioner for Information of Public Importance and Personal Data Protection (known informally as the data protection commissioner) and the National Data Protection Authority of Serbia. The Ministry of Interior did send a DPIA for the new video surveillance system to the commissioner in September 2019, but the commissioner determined that it did not meet the requirements of the LPDP, an assessment echoed by civil society organizations including the SHARE Foundation.

During an annual conference held on Data Privacy Day in January 2021, the data protection commissioner, alongside the heads of major international bodies operating in Serbia such as the Organization for Security and Cooperation in Europe (OSCE), the Council of Europe (CoE), and the U.S. Agency for International Development expressed great concern about the potential risks to Serbia's citizens of the under-regulated field of facial-recognition technology. All noted the need for greater regulatory oversight, monitoring of how the system is used, and actions to ensure clear and transparent government communication to the public, to prevent potential abuses of human rights.

And yet, despite the fact that the system has not received the legal clearances it requires from the data protection commissioner, the cameras are still being installed throughout Belgrade neighborhoods. In April 2020, while a state of emergency was in force in Serbia due to the pandemic, the Ministry of Interior sent the commissioner a revised version of the DPIA for the surveillance system. This version revealed some new and alarming information, such as that the police will have a total of 8,100 cameras of different types at their disposal. In addition to stationary cameras mounted on poles, police officers will have cameras attached to uniforms (so-called "bodycams"), mobile cameras (eLTE terminals), and vehicle-mounted cameras. However, it seems unlikely that body cams or vehicle mounted cameras will reduce violent conduct by police officers, given the lack of effective response by the state to instances of police brutality that were clearly documented in other ways during anti-government protests in Serbia in July 2020.

The April 2020 DPIA also revealed plans for facial detection to be carried out on all persons walking through an area covered by the video-surveillance system, and that the police will use the system for "profiling," although the document doesn't explain what that means specifically. According to the DPIA, the data from the system can also be distributed to broadly defined "authorized recipients," and the use of facial-recognition software for general purposes is planned for the protection of vital interests (life and health) of data subjects or other persons. Such language essentially allows for arbitrary use of this very intrusive system.

The data protection commissioner again rejected the DPIA, stating that the ministry still hadn't delivered the required documents related to the project. The commissioner noted that the government has no legal basis for data processing of biometric personal data collected by video surveillance of public spaces.

Europe's civil society resistance against mass surveillance

The introduction of biometric mass surveillance in Serbia and elsewhere in Europe has spurred a wave of community-led opposition. Two of the largest initiatives are **Hiljadekamera** and **ReclaimYourFace**.

The Thousands of Cameras (@hiljadekamera) project is a community of individuals and organizations led by the SHARE Foundation that advocates for the responsible use of surveillance technology. The goal of the initiative is the protection of privacy and dignity of all citizens. The campaign includes a website to educate the public about the consequences of potential ubiquitous facial-recognition technologies across Belgrade. The website, which went live in May 2020, provides an interactive map of the city marked with the locations of all the city's surveillance cameras. As of March 20th, 2021, the number of cameras exceeded 1,055 at 473 locations, with more underway. That stands in contrast to the Ministry of Interior's website, which claims only 243 locations have cameras.

The initiative raised more than 1 million Serbian dinars (9000 EUR) in a crowdfunding campaign and called on citizens to sign a petition to oppose the installation and use of biometric surveillance, not only in Serbia but across Europe.

The petition, which has collected more than 16,800 signatures since its launch in November 2020, is an element of the SHARE Foundation's work as a member of the ReclaimYourFace movement.

ReclaimYourFace is a petition campaign organized by the advocacy group European Digital Rights (EDRi) with the goal of banning biometric mass surveillance across the continent. The campaign's petition, entitled, "Civil society initiative for a ban on biometric mass surveillance practices," was registered by the European Commission in January 2021 as an official petition under the European Citizens' Initiative, an EU legal mechanism for citizens to provide input on policies by gathering 1 million signatures.

The campaign is based on a May 2020 EDRi paper calling on the European Commission to ban biometric mass surveillance in the EU. The paper detailed the threats that under-regulated mass surveillance poses for fundamental human rights, including privacy, data protection, equality, freedom of expression and information, freedom of assembly and association, and due process.

Legal aspects of biometric mass surveillance

Biometric mass surveillance is illegal in Serbia, as it violates Serbian law and international standards against disproportionate and arbitrary restrictions on fundamental human rights and freedoms.

Serbia is a signatory to the Council of Europe's European Convention on Human Rights (ECHR) and its Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+). Additionally, although Serbia is not a member of the EU, its candidate status mandates the implementation of the bloc's General Data Protection Regulation (GDPR) and the Data Protection Law Enforcement Directive (LED) within the country. Both the GDPR and the LED found their place in the Serbian legal system almost to the point of literal translation in the Serbian Law on Personal Data Protection (LPDP). Effectively this means that the legal framework in the field of privacy and data protection in Serbia is almost identical to the one drafted for EU member states, not to mention the aforementioned conventions that cover a broader set of states.

ECHR (Art. 8) establishes that any interference with the right to private life must be "in accordance with the law and necessary in a democratic society." Convention 108+ (Art. 5) prescribes that "data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake."

The Serbian LPDP sets out strict rules for processing personal data in line with EU standards. Article 5 establishes basic principles for processing, including lawfulness, data minimization, transparency, and data-quality requirements. Data processing by enforcement authorities is lawful only if it is necessary for performing their tasks (Art. 13) and proportionate in relation to the purpose of data processing (Art. 14). Under Article 17, the processing of biometric data is prohibited, in principle, due to the sensitivity of such data. Article 38 furthermore prohibits fully automated decisions based upon processing any types of data, including, biometric data. Finally, it contains a formal requirement that the MOI, when implementing biometric surveillance systems, prepare a DPIA (the Data Protection Impact Assessment) that must be approved by Serbia's national data protection commissioner.

It is clear that deploying biometric mass surveillance on the streets of Belgrade is unlawful, since it cannot be considered necessary and proportionate due to the proposed scale of surveillance, the degree of threat to sensitive personal data, and the risks for fundamental human rights and freedoms. In addition to the right to privacy and data protection, such a system poses risks to freedom of assembly and association, the prohibition of discrimination, the presumption of innocence, and more.

Other legal requirements from LPDP also have not been fulfilled in this case, based on the lack of transparency, the principle of data minimization, and the prohibition of fully automated decisions based on biometric data. The issue of lawfulness is crucial, since Serbia's domestic legal framework does not provide an adequate legal basis for the processing of biometric data, a point noted in the data protection commissioner's opinion on DPIA. Consequently, since there is no approval from the commissioner, the prerequisites do not exist for such data processing.

The question of mass surveillance also has increasingly been a recurring point of discussion at the ECtHR, which has already ruled on a number of relevant cases involving other countries. Most notably, in the case of Roman Zakharov v. Russia, which was decided in the Grand Chamber of the ECtHR in 2015, it was discovered that Russian law-enforcement agencies were provided with copious amounts of data obtained by surveillance equipment illegally installed by Russian mobile operators. The Court ruled that these practices amounted to a blanket interception of communications, without any legal safeguards protecting citizens from arbitrary surveillance and personal data collection, which correlated to violations of Article 8 of the ECHR. It is important to note that, under Russian law, legal remedies for challenging an interception of communications are only available if the person is able to obtain proof of the interception. However, since

said person has no way of being notified about the interception and does not have access to their collected information, the Court ruled that Russia's legislation was insufficient in the case.

In Peck v. the United Kingdom, CCTV footage was captured of the applicant walking around the city while carrying a knife, with the intent of committing suicide. After the authorities were able to locate him and prevent him from harming himself through the use of the CCTV footage, the footage was subsequently released by local authorities in order to demonstrate the effectiveness of the surveillance system. The applicant's identity was not properly disguised, hence infringing on his right to private life (Art. 8). Article 8 was applicable in this case, since the applicant was not participating in a public act and was not a public figure.

In the case of S. and Marper v. the United Kingdom, in which a police department continuously retained biometric data after cases were closed or discontinued, the Court ruled in favor of the applicants, citing that the retention of fingerprints, cellular samples, and DNA profiles violated Article 8 of the Convention, since it was not found to be justifiable. In the judgment, the Court noted that it "was struck by the blanket and indiscriminate nature of the power of retention in England and Wales."

There is an additional array of pending cases in front of the ECtHR, such as Big Brother Watch and Others v. the United Kingdom, Association Confraternelle de la Presse Judiciaire and Others v. France, and Tretter and Others v. Austria.

In 2020, the United Nations special rapporteur on the right to privacy, Joseph A. Cannataci, released a thematic report in which he detailed the development of mass surveillance systems in conjunction with the spread of the coronavirus pandemic. The report warns of the risk of increased human rights violations via the use of biometric data and mass surveillance technologies to, for example, "track citizens and those they encounter." The special rapporteur noted that, in accordance with Convention 108+, the protection of health and the right to privacy must not be mutually exclusive, and that states must work on facilitating adequate approaches to both address the pandemic and maintain privacy rights.

A significant issue is the inherent biases embedded in the datasets used for creating databases and recognizing faces. Most of the datasets are predominantly white and male, which results in discriminatory practices towards non-whites and women. Examples of this in practice have cropped up in places such as the U.S. and the U.K., and more instances will surface as research expands. In Special Rapporteur Cannataci's 2020 thematic report, when discussing security and surveillance, he noted that states should "provide legal protections against non-consensual, predatory, commercial surveillance that enables profiling, monitoring and marketing at a micro level and infringes upon privacy according to gender using big data techniques, such as mobile geofencing and geospatial location markers."

Another legal issue related to surveillance technology arises when citizens exercise their rights to freedom of expression and assembly. During the protests that took place in Belgrade and throughout Serbia in July 2020 against the government's lockdown to curb the coronavirus, Amnesty International expressed concern that police use of the city's surveillance system to identify protesters would have detrimental effects on freedom of expression and the right of assembly. In a tumultuous era globally in which citizens increasingly are mobilized, justifiably or not, to contest their governments' actions, these same societies also must contend with the legal issues and potential rights violations involved with the use of biometric mass surveillance. Implementing mass surveillance technologies, especially those with biometric capabilities, can dangerously limit fundamental rights such as freedom of assembly and the right to privacy. Constant surveillance in public spaces can contribute to increasing state control and repression.

What's next in Europe?

As of now, one of the next battlegrounds for questions of biometric mass surveillance in Europe seems to be in Serbia, and more precisely Belgrade. The way this case plays out may affect discussions about the implementation of surveillance systems in cities across other parts of the continent as well. With Chinese expansion efforts in Europe, the continuing coronavirus crisis, and a growing EU push for regulation of mass surveillance and AI, regulators in member – and non-member states – and the courts that will referee disputes over these issues – will have their hands full.

In January, the Council of Europe released a new set of "measures that governments, facial-recognition developers, manufacturers, service providers and entities using facial-recognition technologies should follow and apply to ensure that they do not adversely affect the human dignity, human rights and fundamental freedoms of any person, including the right to protection of personal data." The guidelines were developed by the Consultative Committee of the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, and they directly address governments, lawmakers, and business.

Such guidelines, as well as the U.N. Special Rapporteur's calls for stricter legislative measures against biometric mass surveillance practices and the launch of the ReclaimYourFace ECI (see box) suggests progress in raising awareness among authoritative bodies and citizens. But there is still the issue of compliance by states. t is important to underline both the short and long-term consequences of these types of technologies, so that we can predict and prepare for the next wave of intrusive technologies and their potential impact on human rights and privacy.

Steps towards a multilateral response

The case against the implementation of biometric mass surveillance systems in Serbia would seem to be within the scope of the ECtHR, considering its rulings, as noted above, in similar litigation related to other countries. The recognition of the Serbia case by the ECtHR and other relevant international bodies such as the Council of Europe, OSCE, the U.N. special rapporteur and the EC is paramount in order to highlight the dangers of the implementation of such systems, not only in Serbia but also in the region and across Europe.

International support and cooperation may help encourage – or pressure, if needed – the Serbian government to limit and regulate the use of these surveillance systems. The biggest need in the fight for a transparent and humane approach to biometric surveillance is dialogue among the affected parties. The government controls the narrative, and it has shown no interest in consulting with civil society organizations or international organizations. SHARE Foundation, together with the Thousands of Cameras initiative (see box) are the only civil society organizations in Serbia actively tackling issues of digital privacy and online violations, albeit without much cooperation from the authorities.

A more just and balanced order in the sphere of data governance requires a more demonstrative push to check existing power structures and to encourage the international community to support such an effort. As previously mentioned, the EC's decision to register an ECI that will deal with curbing biometric mass surveillance practices is welcome and serves as a step in the right direction. In addition, it will be imperative to ensure that the government and companies involved in developing these systems comply with international norms set by the appropriate international bodies and councils.

Recommendations

To ensure that AI systems in the future are designed to respect and advance human rights rather than violate them, the companies and governments developing and implementing these systems must take a more transparent approach. In depth communication must be ensured between authorities and both civil society organizations and citizens about the capabilities of such systems and whether or how they should be used. It is past time to adopt regulation against the potential weaponization of mass surveillance systems, not only in the EU but everywhere this technology may have the chance to influence everyday life and potentially harm societies and its members.

The following measures could significantly advance those goals:

- International bodies such as those mentioned above (the Council of Europe, the OSCE, the U.N., the EC) must issue stronger, firmer statements opposing rights-violating mass surveillance technologies, and become more involved in issues such as facial-recognition practices, not only in Serbia but in Europe generally, in order to push forward a rights-protection agenda on a broader scale.
- The European Commission should amend the draft AI Regulation, which was released on April 21, 2021, to include a comprehensive and indefinite ban on biometric personal-data processing that enables mass surveillance of public places. The current proposal leaves a dangerous gap that governments and companies can exploit to pursue rights-abusing surveillance.
- International bodies should, in partnership and dialogue with civil society organizations, facilitate a concrete exchange of ideas and experiences to promote a more inclusive and all-encompassing approach to the protection of the right to privacy and other human rights affected by AI and biometric mass surveillance technology.
- The international community should develop a global mechanism of accountability to hold tech companies responsible for their role in any misuse of these systems, regardless of the country where they are being employed.
- National and local governments must develop procedures, in conjunction with civil society, to ensure that all officials are transparent with their publics about the limitations of these technologies and the criteria for retaining and processing personal data they collect. That should include prohibiting its use in profiling citizens based on race, social status, ethnic origin, sexual preference, age, gender, or political or religious affiliation.

- Governments must put mechanisms in place to enable authorities to guarantee to their publics that any use of these technologies is based on and proscribed by transparently developed legal provisions, including those related to necessity and proportionality.
- National data protection authorities should dramatically increase their oversight of issues related to mass surveillance and personal-data processing.

Reference list

Amnesty International. "Serbia: Violent Police Crackdown Against COVID-19 Lockdown Protesters Must Stop". July 9, 2020. https://www.amnesty.org/en/latest/news/2020/07/serbia-violent-police-crackdown-against-covid-19-lockdown-protesters-must-stop/ (accessed January 14, 2020)

Bush, Daniel. "'Fighting Like a Lion for Serbia': An Analysis of Government-Linked Influence Operations in Serbia". *Stanford Internet Observatory,* April 2, 2020. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/serbia_march_twitter.pdf (accessed March 23, 2020)

Center for Strategic & International Studies. "Becoming a Chinese Client State: The Case of Serbia". September 2020. https://www.csis.org/analysis/becoming-chinese-client-state-case-serbia (accessed January 10, 2021)

China Daily. "Huawei opens innovation hub in Serbia". September 16, 2020. https://global.chinadaily.com.cn/a/202009/16/WS5f617b77a31024ad0ba79db7.html (accessed January 14, 2021)

Convention 108 and Protocols. https://www.coe.int/en/web/data-protection/convention108-and-protocol

EDRi. "Ban Biometric Mass Surveillance A set of fundamental rights demands for the European Commission and EU Member States". May 13, 2020. https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf (accessed January 14, 2021)

EDRi. "#ReclaimYourFace and help prevent the end of privacy as we know it!". 10 March 2021. https://edri.org/our-work/reclaim-your-face-and-help-prevent-the-end-of-privacy-as-we-know-it/ (accessed January 14, 2021)

European Commission, "European Citizens' Initiative: Commission decides to register an initiative for 'a ban on biometric mass surveillance practices'". 7 January 2021. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_22 (accessed January 9, 2021)

European Convention on Human Rights (ECHR). https://www.echr.coe.int/documents/convention_eng.pdf

European Court of Human Rights factsheet on mass surveillance. https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

ECtHR, Peck v the United Kingdom (2003)

ECtHR, S. and Marper v the United Kingdom (2008)

ECtHR, Roman Zakharov v Russia (2015)

Freedom House. Freedom in the World 2020: China Report.
https://freedomhouse.org/country/china/freedom-world/2020

Freedom House. Freedom in the World 2020: Serbia Report.
https://freedomhouse.org/country/serbia/freedom-world/2020 (accessed March 23, 2020)

Good, Richard. "Serbia Has Second Fastest COVID-19 Vaccine Rollout in Europe Thanks to China". *Euronews*. January 27, 2021.
https://www.euronews.com/2021/01/27/serbia-has-second-fastest-covid-19-vaccine-rollout-in-europe-thanks-to-china (accessed February 12, 2021)

Guidelines on Facial Recognition (January 28, 2021), available at:
https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3

Hatmaker, Taylor. "Lawsuits Allege Microsoft, Amazon and Google Violated Illinois Facial Recognition Privacy Law". *Techcrunch*. July 15, 2020.
https://techcrunch.com/2020/07/15/facial-recognition-lawsuit-vance-janecyk-bipa/
(accessed March 17, 2021)

Hatmaker, Taylor. "Clearview AI Landed a New Facial Recognition Contract With ICE". *Techcrunch*. August 15, 2020. https://techcrunch.com/2020/08/14/clearview-ai-ice-hsi-contract-2020/ (accessed January 14, 2021)

Hatmaker, Taylor & Whittaker, Zack. "Massachusetts Lawmakers Vote to Pass a Statewide Police Ban on Facial Recognition". *Techcrunch*. December 2, 2020.
https://techcrunch.com/2020/12/01/massachusetts-votes-to-pass-statewide-police-ban-on-facial-recognition/ (accessed January 14, 2021)

Huawei. "Huawei Safe City Solution: Safeguards Serbia". Archived case study available at: https://archive.li/pZ9H0

Jakubowska, Ella & Naranjo, Diego. "Ban Biometric Mass Surveillance: A set of fundamental rights demands for the European Commission and EU Member States", p. 37. *European Digital Rights (EDRi)*. May 13, 2020. https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf
(accessed February 12, 2021)

Jeremić, Ivana, Stojanović, Milica & Dragojlo, Saša. "Serbian Protests: Police Brutality Mapped". *Balkan Insight*. July 10, 2020. https://balkaninsight.com/2020/07/10/serbian-protests-police-brutality-mapped/ (accessed March 19, 2021)

Lecher, Colin. "San Francisco Becomes the First US City to Ban Facial Recognition by Government Agencies". *The Verge*. May 14, 2019.'
https://www.theverge.com/2019/5/14/18623013/san-francisco-facial-recognition-ban-vote-city-agencies (accessed January 14, 2021)

List of camera locations in Belgrade on the Ministry of Interior's website.
http://www.mup.gov.rs/wps/wcm/connect/d52f1b79-f728-4870-8da4-0462c9561157/lokacije+kamera.CIR.pdf?MOD=AJPERES&CVID=nqp4ma4
(accessed January 13, 2021)

N1. "Plan with China endorsed, Huawei will make Serbia's cities smart". April 22, 2020. https://rs.n1info.com/english/news/a478212-smart-cities-in-serbia-by-huawei/ (accessed January 14, 2021)

O'Flaherty, Kate. "Huawei Security Scandal: Everything You Need to Know". February 26, 2019. *Forbes*. https://www.forbes.com/sites/kateoflahertyuk/2019/02/26/huawei-security-scandal-everything-you-need-to-know/?sh=51b481f373a5 (accessed January 12, 2021)

Perkov, Bojan. "Will Serbia Adjust Its Data Protection Framework to GDPR in Practice?". *Internet Policy Review.* April 17, 2019. https://policyreview.info/articles/news/will-serbia-adjust-its-data-protection-framework-gdpr-practice/1391 (accessed January 13, 2021)

SHARE Foundation. "New surveillance cameras in Belgrade: location and human rights impact analysis – 'withheld'". March 29, 2019. https://www.sharefoundation.info/en/new-surveillance-cameras-in-belgrade-location-and-human-rights-impact-analysis-withheld/ (accessed January 13, 2021)

- "Huawei knows everything about cameras in Belgrade – and they are glad to share!". March 29, 2019. https://www.sharefoundation.info/en/huawei-knows-everything-about-cameras-in-belgrade-and-they-are-glad-to-share/ (accessed January 13, 2021)
- "Kamere bez upotrebne dozvole/Procena uticaja 2.0". July 31, 2020. https://www.sharefoundation.info/sr/kamere-bez-upotrebne-dozvole-procena-uticaja-2-0/ (accessed January 14, 2021)
- "NE SNIMAJ MI LICE – Peticija protiv biometrijskog nadzora". https://hiljade.kamera.rs/sr/peticije/ne-snimaj-mi-lice/ (accessed January 9, 2021)
- "New surveillance cameras in Belgrade: location and human rights impact analysis – 'withheld'". March 29, 2019. https://www.sharefoundation.info/en/new-surveillance-cameras-in-belgrade-location-and-human-rights-impact-analysis-withheld/ (accessed January 13, 2021)
- "Unlawful video surveillance with face recognition in Belgrade". December 4, 2019. https://www.sharefoundation.info/en/unlawful-video-surveillance-with-face-recognition-in-belgrade/ (accessed January 13, 2021)

Stanley, Alyse. "Police Use of Clearview AI's Facial Recognition Tech Spiked After Capitol Raid" Gizmodo. January 10, 2021. https://gizmodo.com/police-use-of-clearview-ais-facial-recognition-tech-spi-1846030687 (accessed January 14, 2021)

Stojanović, Milica. "Serbia Launches State of Emergency to Counter Coronavirus". Reuters. March 15, 2020. https://www.reuters.com/article/us-health-coronavirus-serbia-idUSKBN21215E (accessed December 29, 2020)

Surfshark. "The Facial Recognition World Map". https://surfshark.com/facial-recognition-map (accessed January 12, 2021)

Swedish Authority for Privacy Protection (IMY). "Police unlawfully used facial recognition app". February 11, 2021. https://www.imy.se/nyheter/police-unlawfully-used-facial-recognition-app/ (accessed February 12, 2021)

Thousands of Cameras Twitter feed. https://twitter.com/hiljadekamera

United Nations, General Assembly, Preliminary Evaluation of the Privacy Dimensions of the Coronavirus Disease (COVID-19) Pandemic: thematic report by the Special Rapporteur on the right to privacy, A/75/147 (July 27, 2020), available at: https://undocs.org/A/75/147

United Nations, General Assembly, Promotion and Protection of the Right to Freedom of Opinion and Expression: note by the Secretary General, A/73/384 (August 29, 2018), available at: https://undocs.org/A/73/348

United Nations, General Assembly, Security and surveillance, health data, and business enterprises use of personal data: thematic report by the Special Rapporteur on the right to privacy, A/HRC/43/52 (March 24, 2020), available at: https://undocs.org/A/HRC/43/52

Vincent, James. "NYPD Used Facial Recognition to Track Down Black Lives Matter Activists" The Verge. August 18, 2020. https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram (accessed January 14, 2021)

Vladisavljev, Stefan. "How Did Serbia And Huawei Cooperate: A Chronology". Belgrade Fund for Political Excellence. July 29, 2019. https://en.bfpe.org/in-focus/region-in-focus-focus/how-did-serbia-and-huawei-cooperate-a-chronology/ (accessed March 18, 2021)

Imprint

Heinrich-Böll-Stiftung European Union, Brussels, Rue du Luxembourg 47-51,
1050 Brussels, Belgium

Heinrich-Böll-Stiftung Washington, DC, 1432 K St NW, Washington, DC 20005, USA

Contacts, Heinrich-Böll-Stiftung European Union
Anna Schwarz, Head of Programme, Global Transformation,
Heinrich-Böll-Stiftung European Union, Brussels,
E Anna.Schwarz@eu.boell.org
Lisa Tostado, Head of Programme, Climate, Trade and Agricultural Policy,
Heinrich-Böll-Stiftung European Union, Brussels,
E Lisa.Tostado@eu.boell.org

Contacts, Heinrich-Böll-Stiftung Washington, DC
Sabine Muscat, Programme Director, Technology and Digital Policy,
Heinrich-Böll-Stiftung Washington, DC,
E Sabine.Muscat@us.boell.org
Liane Schalatek, Associate Director, Heinrich-Böll-Stiftung Washington, DC,
E Liane.Schalatek@us.boell.org
Christin Schweisgut, Programme Director, Infrastructure and Development,
Heinrich-Böll-Stiftung Washington, DC,
E Christin.Schweisgut@us.boell.org

Place of publication: https://us.boell.org/ | http://eu.boell.org

Release date: May 2021

Editor: Viola Gienger, Washington, DC

Illustrations: Pia Danner, p*zwe, Hannover

Layout: Micheline Gutman, Brussels