Biometric surveillance during protests: a security matter or a violation of human rights?

By Valentina Luna Colella

ITSS Verona Magazine, Vol. 2, n. 2

Fall/Winter 2023

Biometric surveillance during protests: a security matter or a violation of human rights?

Valentina Luna Colella

To cite this article: Valentina Luna Colella, *Biometric surveillance during protests: a security matter or a violation of human rights?*, ITSS Verona Magazine, Vol. 2, no. 2, Fall/Winter 2023.

Keywords: Biometric surveillance, Protests, Freedom, Cybersecurity, Human Rights, Privacy

ITSS Verona website: https://www.itssverona.it/itss-magazine

LinkedIn: https://www.linkedin.com/company/itss-verona/

Instagram: https://instagram.com/itss_verona?igshid=YmMyMTA2M2Y=

Published online: December 29th, 2023

Abstract: Biometric surveillance is the latest use in police forces to check on protesters and to simplify the identification of potential criminals. However, extensive surveillance does not discriminate between citizens and poses a lot of problems to civil and basic human rights. The right to peaceful assembly, along with many other privacy rights, along with the possible degradation of human dignity as well. Different types of surveillance require different types of devices that are mostly regulated by Artificial Intelligence, a branch that still has little control and that nevertheless requires human interaction to be precise. International regulation is insufficient and police officers feel entitled to use these types of devices during protests for the sake of protection and to maintain peace and security in the cities. As citizens still wonder if they feel safer or more scared, I will argue how the advancement in these technologies has caused more of a security threat than the one it was developed to resolve. The paper underlines the absence of regulation in this environment and the exploitation of the mass surveillance tools by enforcement authorities and possible solutions and approaches that can improve this issue. The author refrains from any possible accusations and wrongful assumptions towards police forces and governments in general; it is not in the author's view to criticise law enforcements procedures or use of technologies, indeed to shed light on the factual events that might provoke any misuse and wrongful accusations towards these technologies.

Moscow, January 2021: Alexey Navalny has just been arrested by the Russian government and he is about to spend, allegedly, two years and a half in prison. Protests in the capital start to arise, but something peculiar characterises these events: during the rallies, there are almost no police officers in the streets. Participants in the riots almost feel safer and free to demonstrate their disappointment for Vladimir Putin's government. However, after a few days, officers started to knock on the doors of all the citizens suspected, arresting them, and beginning the trials after a few days. But how did it happen? How were they aware of who the people were, where they lived, and if they were present at the protests?

Protests are in our human nature. People yearn to engage in public movements and make the best use of them to achieve common goals and aspirations. During the pandemic, the number of movements skyrocketed; from those who wanted to fight for a better future to those who desired a revision in current administrations, protests have always represented the demonstration of human freedom to engage in dissent or liberation.

According to the United Nations Office of the High Commissioner for Human Rights, in 2019 alone there were more than 100 protests in various countries.[1] However, police checks during protests have been evolving and going through digital growth side by side with the increase of rallies. After the Navalny protests, on Twitter and other social media, claims that people were stopped days after the protests at their houses, in the subway station, and in other public places by police officers arose. They argued that the officers used facial recognition to identify citizens attending the rallies and proceeded to arrest them.

Russian citizens have not been the only victims: after the tragic death of George Floyd on May 25, 2020, Black Lives Matter movements grew exponentially, protesting police brutality towards black people. Many demonstrators claimed that they were targeted with facial recognition software and artificial intelligence powered tools used by law enforcement agencies to gather data and suspects' information. Police officers have been using the latest technology to collect

[1] United Nations Human Rights, Office of the High Commissioner, "Press Briefing Note on Protests and Unrest around the World", 2019.

information and data about the individuals protesting; from body cameras, and security systems of large food chains (who will provide the footage directly to the agents) to all the videos found online via social media[2] police work highly relied on surveillance to arrest dissenters. Furthermore, tech companies are expanding their offerings in terms of surveillance cameras for houses, small businesses, and even supermarkets. With all these devices, dispersed around cities and on different streets, citizens do not feel safe anymore, on the contrary, the fear of being targeted or recorded by these systems is significantly higher.

Many organisations, as well as the UN High Commissioner for Human Rights, are shedding light on the problem and trying to find the best solution. Mutale Nkonde, the founder of A.I. for the People, has spoken to Amnesty International saying that: "Police use of facial recognition technology places innocent New Yorkers on a perpetual line-up and violates our privacy rights. Facial recognition is ubiquitous, unregulated and should be banned."[3] But is it just a matter of privacy rights? The excessive surveillance and the use of powered A.I. tools to try to recognize different individuals during protests have been putting at risk another essential right: the right to peaceful assembly.[4] Firstly, by describing how different instruments can be used for surveillance objectives and how police officers can rely on a multitude of equipment to profile citizens. Then I will move into the history of surveillance, how it has developed from Foucault to the post-panopticon theories and how contemporary studies link this activity with human rights infringement. Furthermore, this paper will also consider a personal analysis based on different legal instruments that explore the misuse of surveillance systems by police officers and by governments.

---

[2] Heather Kelly, Rachel Lerman, *America Is Awash in Cameras, a Double-Edged Sword for Protesters and Police*, Washington Post, June 3, 2020, https://www.washingtonpost.com/technology/2020/06/03/cameras-surveillance-police-protesters/.

[3] Amnesty International, "Ban Dangerous Facial Recognition Technology That Amplifies Racist Policing." Amnesty International, August 8, 2022, https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/.

[4] United Nations Human Rights, Office of the High Commissioner, A/HRC/44/24: "Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests", 2020, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/154/35/PDF/G2015435.pdf?OpenElement.

Ethical visions will be examined as we move towards the concluding remarks that will discuss if these technologies are an actual security threat and infringe on a variety of human rights.

Different devices, different uses, different outcomes

The two main protests mentioned, have used very different tools to collect the data that police officers required. To a greater extent, there are many ways to retrieve personal information from mass surveillance.

Biometric data is defined in Article 14 of the GDPR as: "personal data retrieved from specific technical processing relating to the physical physiological or behavioural characteristics of a person, which [...] confirms the unique identification of that person.".[5] But how do local enforcement authorities retrieve this unique information?

Considering the different types of surveillance, police officers have the chance to access personal data such as a home address, location or behavioural surveillance in numerous ways. Nowadays, all this information can be retrieved even by just staying at the desk. If needed, and with the appropriate authorizations, they can use security cameras of different stores, or they can gain access to smart home devices and cameras.[6] Some police officers have also gained access to social media groups to monitor conversations and retrieve information directly from there. Live streaming by journalists that were present at the protests (specifically at the Black Lives Matter movement in the United States), showing the faces of all the protesters, was meticulously analysed; it displays how the use of social media can impact the growth of biometric surveillance. Police have access to the video like everyone else, and some departments also have tools that can inspect the different metadata left by videos and photos posted to retrieve only relevant information.

From this perspective, there are many problems with handling this surveillance. It is not just targeted surveillance of those protesters that can harm or create problems for the population, it is mass surveillance. Moreover, this extensive control gives the motive to create permanent records of

[5] European 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), Article 14, European Commission, May 24, 2016.

[6] See note 2.

the data collected by police officers. In this way, they are also allowed to "identify all those that participated in a protest even at a later time".[7]

Amazon's Rekognition, a cloud-based "Software as a Service" (SaaS) that runs with an algorithm that can detect faces and their activities based on pre-loaded labels, gained popularity in recent years. It has been used by different police departments across the U.S., especially during the B.L.M. movements, as well as by Immigration and Customs Enforcement (I.C.E.). The algorithm that runs inside the software is simple: it detects different faces during protests, and can easily identify, by an instantaneous Internet search, the individuals observed. It then proceeds to give all the information found to the police officer, or whoever has purchased the device, who now possesses all the personal details of the protester[8]. Since there is no national regulation or standard for facial recognition algorithms in the U.S. local officers are almost able to use this device freely, and its lawfulness is questionable.

Biometric Surveillance: a History that Starts in the Past

Surveillance creates many problems in terms of privacy laws and additionally to the right to freedom of assembly. It is not merely just a matter of privacy; it is also a matter of morality. The right to keep your identity private, is an important feature during protests; it allows participants to avoid stigmatisation in their society and to preserve their status, which can be infringed using this indiscriminate surveillance. But how was it developed in the first place?

The history of surveillance finds traces from the early theories of the British philosopher Jeremy Bentham and its own "Prison Panopticon": an innovative planning for the redesign of prisons. The architecture builds an "illusion of constant surveillance, where prisoners are not

[7] Ilia Siatitsa "Freedom of Assembly under Attack: General and Indiscriminate Surveillance and Interference with Internet Communications," International Review of the Red Cross, March 1, 2021, https://international-review.icrc.org/articles/freedom-assembly-under-attack-surveillance-interference-internet-communications-91.

[8] Drew Harwell, "Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use," Washington Post, December 19, 2019, https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

watched constantly but believe that they are".[9] Surveillance here is human-based and carried out from just one single point of view, the main inspector, who holds the most power and impersonates an "eye in the sky" and creates a somewhat reign of terror. He is "an utterly dark spot"[10] inmates do not see him and cannot attribute to someone the surveillance that they are experiencing, although knowing that it is present. This provokes a sense of anxiety that leads prisoners to behave in the best manner possible to avoid possible punishment, although they are never able to see the potential agent and still have not committed anything (besides the motive to which they were imprisoned in the first place).

The resemblance between the theory developed in the 18th century and current protests in the 21st century is noteworthy. The only difference that can be found is that surveillance during protests is not human-based anymore; today machines are taking over the duty. However, the extreme fear and anxiety now that these technologies are out in the open and used almost regularly is still the same as the one described by Bentham. A report showed how 70% of respondents do not believe that technologies used in surveillance are effective against security threats, but that "they are deployed to create the appearance of action."[11]

In Foucault's panopticon, drawing from Bentham's theories, he theories surveillance as an all-seeing inspector. This continuous control is perceived by him as a form of control of both punishment and correction, which: "can model and transform individuals"[12]. However, the state's behaviour towards humans changed over time; central governments' desire to obtain power over people's minds and bodies materialised. That is why, in modern Western societies we can notice that the panopticon model has been invading different situations in daily lives. The Panopticon society has been introduced by Foucault as a system that can discipline the individual and it regained

[9] Maša Galič, Tjerk Timan, and Bert-Jaap Koops, "Bentham, Deleuze and beyond: An Overview of Surveillance Theories from the Panopticon to Participation," *Philosophy & Technology* 30, no. 1 (2016): 9–37, https://doi.org/10.1007/s13347-016-0219-1, 12.

[10] Miran Božovič "An utterly dark spot': the fiction of god in bentham's panopticon.", Qui Parle 8, no. 2, 1995, 83–108. http://www.jstor.org/stable/20686026.

[11] Jacobi, Anders, and Mikkel Holst, Synthesis Report - Interview Meetings on Security Technology and Privacy, PRISE, 2008, https://prise.oeaw.ac.at/docs/PRISE_D_5.8_Synthesis_report.pdf.

[12] Foucault, Michel, James D. Faubion, and Robert Hurley. Power, "The New Press's Essential Works of Foucault series", New Press, 2000, 370.

importance in modern societies with the advancement in technologies. They have been reinvoking these theories by enabling these centralised and decentralised forms of surveillance and theorising on the policing of society and its citizens.

Technologies from one side helped to achieve uniformity by highlighting who, in a society, is not “conventionally normal” and behaves in a non-conforming manner. By removing these individuals from society, we are left with a unified community where everyone is able to result invisible. The Panopticon served as a visual representation for Foucault of the relationship between power, surveillance, and discipline in contemporary society, where power is largely diffused and hidden.[13] The subject responsible for the surveillance remains in the shadow and can count on its anonymity to be able to control the prisoners in the best possible way. For Panopticon's theories, the people surveilled are criminals or at most suspects, however, modern surveillance systems control and trace every citizen, beyond their grade of imputability. The tension that is felt in the prison is the same one perceived during protests, especially when you know that you are being surveilled though by not committing any unauthorised activity.

Biometric surveillance paved the way to punish and recognise who acts unlawfully to achieve stability, which is long researched by Western states today. The narrative towards controlling the individual has now been portrayed as a way to protect it; here lies another discrepancy between Foucault's and Bentham’s visions. Biometric surveillance is now liberalised with the excuse of making people safer, not to educate them; technology is used to help citizens to live more peacefully and to worry less about who could pose a threat to their security.

However, some argued that in reality, the purpose of control with the evolution of digital technologies embedded in surveillance systems, could be a security threat to both human rights and the emancipated fulfilment of life.

[13] Albu, Oana Brindusa, and Hans Nørgaard Hansen, “Three Sides of the Same Coin: Datafied Transparency, Biometric Surveillance, and Algorithmic Governmentalities.” Critical Analysis of Law, vol 8, no. 1, April 2, 2021, https://cal.library.utoronto.ca/index.php/cal/article/view/36277/27580, 11.

A contemporary interpretation of biometric surveillance

We are moving towards a new rationale for biometric surveillance; its use in protests and the wrongful arrests that emerged from its deployment caused a shift in public opinion and security perspectives.

To understand how the perception of this mass control has changed it has to be considered not as another means of inspection, but rather as a new form of control. What was present before with Foucault and Bentham's vision of surveillance as supervision, is now a full-on reign of inspection and forced vigilance. People are not perceived any more as subjects with sovereignty over their bodies and over what they can or cannot display; the state enters into play and enacts jurisdiction vis-à-vis what it considers as public objects that can be analysed without their consent. For example in 2004, the United States Department of Homeland Security established a program that could support border management; via this program the DHS created a biometric database that stored and processed fingerprints, photographs and facial images taken at border crossings that identified with "person of interests".[14] The government, in this case, came into play over the sovereignty of individuals to enact its jurisdiction for a "greater good"; in this case the protection of its borders and citizens.

Individuals do not have the power to administer what can be presented to the public and what needs to remain private; moreover, biometric surveillance leaves no choice but to let citizens be analysed regardless of their consent or not. Inevitably this has created a shift in public opinion when operating in different political contexts. Police and government institutions promote this mass collection of data and surveillance. They advocate for them and endorse their use because of all the potential benefits they can obtain, for example arresting criminals more easily or even before they might commit other felonies and therefore prevent any possible catastrophes such as terrorist attacks.

[14]Avi Marciano, "Reframing Biometric Surveillance: From a Means of Inspection to a Form of Control." Ethics and Information Technology 21, no. 2. June 1, 2019, 127-136, https://doi.org/10.1007/s10676-018-9493-1, 13.

Thus, two main concerns emerge from the use of biometric surveillance by police forces: the fear of routine victimisation and the prospect of a controlled society.[15] During protests, the fear of getting hurt or having your neighbourhood dismantled by vandalism plays a big part in seeing surveillance as a necessity. It has been seen as a fundamental requirement that prevents a town, a district or a whole state from falling into anarchism and being ruined by criminals. On the other side of the spectrum, we find the "prospect of a totally controlled society", a Big Brother that watches and evaluates all your actions and emotions. Here, police surveillance is portrayed as a more menacing weapon that runs the potential to be comparable to an Orwellian dystopian vision of total control.[16] It contrasts with the concept of traditional surveillance aimed at gathering information, with a precise objective to achieve.

Civil liberties and rights struggle to be respected when security becomes a justification for domination rather than a necessity[17] and these policing techniques fail to correctly address these issues.

Controlling citizens indiscriminately during protests only reinforces the concept that new surveillance wants to extract or even create information to go beyond what is offered and voluntarily reported. It is designed to be *extensive surveillance* since the development of the technologies has helped police officers to go in-depth over their control of citizens. An asymmetrical withdrawal of information, especially in the case of the Black Lives Matters protests, happening in a "democratic" society that should promote equality over treatment. Surely, the footage of various cameras helped police officers to arrest the responsibles of violent attacks that happened during the protests; however, while the statement of "making the world safer" creates a perfect alibi for police forces, the mass collection of data that comes from surveillance infringes on the actual safety that the demonstrators, and broadly all citizens, might feel around the streets. The

[15] Kevin D. Haggerty, "Surveillance, crime and the police" , in The Routledge Handbook of Surveillance Studies ed. Kirstie Ball, Kevin D. Haggerty and David Lyon, Abingdon: Routledge, Routledge Handbooks Online, March 27, 2012, 235.

[16] Stanley Cohen, Visions of Social Control: Crime, Punishment and Classification, Oxford, PolityPress, 1985, 14.

[17] Bigo Didier, "Security, Surveillance and Democracy", in Routledge EBooks, 2011, 388.

state must act efficiently to not only identify the perpetrators of violent acts after they have occurred but to intervene before they take place so that violence can be avoided.[18]

After the ever-changing events of 9/11 surveillance changed its patterns of development and increased usage for security purposes. These incidents helped the increase of investments that the U.S. and its Western allies (including the European Union) had to better these technologies. However, the urgency that the War on Terror created, failed to address the safe use of surveillance systems, proving still now that they are unsuccessful to use at most times, and they can themselves be considered as a security threat. The systems have neglected their impact on human dignity and the human rights framework in which privacy is recognized, therefore violating often many privacy laws.[19] A new report of the United Nations High Commissioner for Human Rights precisely claims: "Previous practical limitations on the scope of surveillance have been swept away by large-scale automated collection and analysis of data" and that "Governments often fail to adequately inform the public about their surveillance activities, and even where surveillance tools are initially rolled out for legitimate goals, they can easily be repurposed, often serving ends for which they were not originally intended."[20]

The long-standing argument for using any monitoring during these events comes from the balance between security and freedom. A new form of social contract where a citizen is quasi-forced to lose part of their freedom to express and to manifest dissent, as a means to have the guarantee of safety. The individual does not grant permission to have this freedom removed and it is forced to give away its privacy for security matters decided by the states.

[18] Marx, Gary T., "Personal and Professional Encounters with Surveillance.", In The Routledge Handbook of Surveillance Studies, ed. Kirstie Ball , Kevin D. Haggerty and David Lyon, Abingdon: Routledge, Routledge Handbooks Online, March 27, 2012, xx, https://web.mit.edu/gtmarx/www/survhandbook.html.

[19] Article 12, United Nations, Universal Declaration of Human Rights, 1948.

[20] OHCHR *Spyware and surveillance: Threats to privacy and human rights growing, UN report warns*, 2022 https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report,.

Privacy rights rely on the assertion that individuals are not singular citizens or general subjects but persons.[21] The conflict emerges when the state is called to be responsible for its security from outside threats but also for defending the autonomy of the individual. A clash of different responsibilities where, currently, states fail to defend both.

Biometric surveillance, from a broader perspective, might certainly help law enforcement agencies to pursue their objectives of a protected and secure environment, nonetheless, the practice of how it is being used now is threatening to privacy and human rights in general. The technologies are still unsuccessful to collect accurate and precise information that can discriminate between an unlawful protester and a law-abiding citizen. Algorithms that are developed are far from being precise and the result is that many wrongful arrests have been made based on algorithmic assumptions.[22] The automatic decision-making and few human interactions that these technologies have, raised ethical questions about "mediated social sorting and discrimination"[23]. Racial sorting is common and routinely absolved by police officers, causing confusion within black and indigenous communities that find themselves continuously wrongfully accused just based on their skin colour. Bauman emphasises this concept claiming that biometric technologies enforce the discriminatory division between "the extraterritoriality of the new global elite and the forced territoriality of the rest"[24], where the distinction is brought by allegedly dangerous categories of individuals and exclusive human beings that have the advantage of not being unjustly accused. Facial Recognition Technology may contribute to a greater racial disparity in arrests, where a positive relationship

[21] Eric Stoddart, "A Surveillance of Care Evaluating Surveillance Ethically." In *The Routledge Handbook of Surveillance Studies*, ed. Kirstie Ball , Kevin D. Haggerty and David Lyon, Abingdon: Routledge, Routledge Handbooks Online, March 27, 2012, 369.

[22] Johana Bhuiyan, "First Man Wrongfully Arrested Because of Facial Recognition Testifies as California Weighs New Bills.", *The Guardian*, April 27, 2023. https://www.theguardian.com/us-news/2023/apr/27/california-police-facial-recognition-software.

[23] See note 14, 134.

[24] Bauman Zygmunt, 'Social Issues of Law and Order,' In *"The British Journal of Criminology"*, Volume 40 Issue 2, March 2000, 205-21.

between black arrests rates and a negative one with White rates exists, as shown by a study made in 1136 different U.S. cities.[25]

An analysis of the impact of surveillance technologies on human rights

The power that police officers hold when using surveillance systems is substantial considering the blurry definition of their duties in International Law. The United Nations basic principles give us a direct link between the task of law enforcement officials and the protection of human rights. The respect of H.R. is considered a full part of the public order[26], that shall not be neglected, therefore police officers have the mandate to respect both. The right to privacy is more at risk during mass surveillance in protests, simultaneously with the right to peaceful assembly.

The first one is the most peculiar since it is considered also an enabling right, meaning that it contains and sets up the enjoyment of other rights, including freedom of expression and peaceful assembly.[27] This proves to be useful when providing arguments towards the ethical violation that biometric surveillance puts forward. When violating the right to privacy, police officers violate a plethora of other human rights that causes a lack of protection for victims of illegal use of face recognition systems.[28] In addition, two resolutions of the Human Rights Council (21/16 and 24/5) preserve the right to peaceful assembly and the Committee specifies that even though an assembly takes place in public, the participant's privacy can still not be infringed, although it might happen with facial recognition devices and other technologies. The comment also clarifies that the same rules apply to monitoring social media to obtain information from participants. This activity must be "transparent, independent [...] and exercised over the decision to collect the personal information

[25] The full research is available here: Johnson, Thaddeus L., Natasha N. Johnson, Denise McCurdy, and Michael S. Olajide, "Facial Recognition Systems in Policing and Racial Disparities in Arrests." Government Information Quarterly 39 (4): 101753, 2022, https://doi.org/10.1016/j.giq.2022.101753.

[26] UN Commission on Human Rights. "Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights." *UN Commission on Human Rights*. September 28, 1984.

[27] European Court of Human Rights, ed. *Guide On Article 11 Of The European Convention On Human Rights - Freedom Of Assembly And Association*, 2022, https://www.echr.coe.int/documents/d/echr/guide_art_11_eng.

[28] ОВД-Инфо, "How the Russian State Uses Cameras against Protesters," January 17, 2022, https://en.ovdinfo.org/how-authorities-use-cameras-and-facial-recognition-against-protesters.

and data of those engaged in peaceful assemblies and over its sharing or retention, to ensure the compatibility of such actions with the Covenant".[29]

However, the major problem that emerged from the BLM protests was that the measure deployed by the police to recognize participants did not fall under a specific legal framework, or the existing frameworks were interpreted too broadly.[30] In addition, police officers and government officials have endorsed the use of store-bought home surveillance systems that still may cause citizens and protesters to live in constant fear of being identified and arrested for actions that you might not have done. It creates an environment where individuals live in constant threat, where fear of the possible disorder created by protests, encourages mass surveillance also from the public. Many problems in accountability and responsibility of who shall be liable for possible infringement of international law hatch because of this lack of regulations. Attributability fails to be addressed, considering that police officers and law enforcement might hide some violations of human rights behind the excuse to ensure security for the community, which can be done correctly through surveillance systems.

Risks to human rights cannot be infringed with the justification of internal security; humans, when monitored, tend to censor themselves and modify their behaviour.[31] This impact exists besides the actual influence that biometric surveillance might have on the individual. The risks posed to private life go beyond the actual repercussions that these technologies have on a person; from the massive collection of data that is retrieved during protests, to the possible risks related to errors that these technologies might have.

The actual accomplishment of biometric surveillance during protests did not offer exhaustive and sweeping results. Commonly criminalised categories of people are often

[29] Christof Heyns, "General Comment No. 37." *Article 21: Right of Peaceful Assembly'*, Remark n. 72, 2020, 12.

[30] Drew Harwell, "Oregon Became a Testing Ground for Amazon's Facial-Recognition Policing. But What If Rekognition Gets It Wrong?" *Washington Post*, April 30, 2019, https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/.

[31] Greens/EFA, "Impacts of the Use of Biometric and Behavioural Mass Surveillance Technologies on Human Rights and the Rule of Law", February 2, 2022, http://extranet.greens-efa-service.eu/public/media/file/1/7487.

mismatched and targeted wrongfully, in addition, surveillance systems are most vulnerable to cyber-attacks. The considerable amount of data that police forces possess after using these technologies makes them highly exposed to potential data aggressions, where criminals could use them as a ransom to obtain specific objectives.

Mostly, the effect on public behaviours is what is more concerning about surveillance cameras caused by the fear of being targeted. The perception that with the installation of cameras, a whole new regime might come back into play, clashes against the misconception that such surveillance could reduce crimes. Such as the case brought by Big Brother Watch, a company based in London, that urged Britain's Information Commissioner's Office to investigate breaches of data protection legislation by a co-operative's use of biometric scans in a supermarket chain.[32] Still, it is difficult to establish what would crime rates during protests have been without the use of cameras, making comparisons highly problematic.[33]

The effect on individuals can be seen and established, and it is legitimate and undeniable; the right to privacy is an established human right, and it is no news that these systems are grounded in bases that violate this right. Above all, with these types of surveillance systems, especially if they are used during public movements such as protests, states might suffer from a democratic backlash and may fall into an autocratic state which endorses the use of indiscriminate surveillance. Particular care must be taken by public officials and political representatives to ensure that they act under citizens' preferences, especially when concerns are raised about a potential threat to inalienable fundamental rights.[34] Is of utmost importance to be able to restore the conditions for a democratic debate.

[32] "'Orwellian' Facial Recognition Cameras in UK Stores Challenged by Rights Group." *Reuters*, July 26, 2022, https://www.reuters.com/world/uk/orwellian-facial-recognition-cameras-uk-stores-challenged-by-rights-group-2022-07-26/

[33] See note 15, 242.

[34] See note 31.

Conclusions

Mass surveillance puts at risk many different rights, especially human rights. The legislation for the use of this type of surveillance is still not clear, and there are no proper guidelines to follow at the international level.

Despite the different improvements that the UN and the international organisations are working on, the warnings put out by IHL have proved inadequate to efficiently protect people from the infringement of their basic rights. Still, the UNGA has claimed that to ensure the enjoyment of human rights, [...] technical solutions to safeguard the confidentiality of digital communications, which may include measures for encryption, pseudonymization, and anonymity can be important.[35]

Facial recognition remains a "grey zone" in legal regulation, but its rapid development puts citizens in a distressing position both personally and socially. People have altered their behaviour according to these measures, avoiding going to protests to protect themselves, or not manifesting their opinions for fear of being always watched or listened to. States should promote a safe environment for the exercise of the right of peaceful assembly and to this extent, they did quite the opposite. This creates a sort of chilling effect between communities and movements; during the Black Lives Matter protests, when the idea that biometric data could have been gathered simply by protesting spread around citizens, people started to change their opinion about rallying.

Being categorised, and profiled, knowing that your data will be stored up by authorities just for expressing civil rights refrains from the exercise of that same right. Racial profiling and bias are more common if artificial intelligence is involved in digital vigilance. Native Americans have the highest false-positive rate of all ethnicities, and black people get often mistaken and wrongly accused. Likewise, women get more falsely identified than men as well as children and the elderly from other age groups while middle-aged white men benefit generally from the highest accuracy rates, leaving the door open to racial profiling and inequity.[36]

[35] UNGA Res. 73/179, A/RES/73/179, Paragraph 9, December 17, 2018.
[36] See note 8.

International bodies are struggling to cope with the fast growth of the digital world, but the pandemic, the Ukraine war and other crises have slowed down this process. Focus shifted on new current issues that have conveyed attention of International regulations bodies elsewhere. There is an urgent need to start working again simultaneously on the development of a clear framework to protect the right of peaceful assembly and a more rigid one regarding the protection of data following biometric surveillance during these public demonstrations, while still protecting all of the mentioned human rights.

Bibliography

Article 14, EU General Data Protection Regulation (GDPR): 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), OJ 2016 L 119/1R

Albu, Oana Brindusa, and Hans Nørgaard Hansen. "Three Sides of the Same Coin: Datafied Transparency, Biometric Surveillance, and Algorithmic Governmentalities." *Critical Analysis of Law* 8, no. 1 (April 2, 2021): 9–24. https://cal.library.utoronto.ca/index.php/cal/article/download/36277/27580.

Amnesty International. "Ban Dangerous Facial Recognition Technology That Amplifies Racist Policing." *Amnesty International*, August 8, 2022. https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/.

Bauman, Z. (2000) 'Social Issues of Law and Order,' British Journal of Criminology, 40(2): 205-21.

Bigo, Didier. "Security, Surveillance and Democracy." In *Routledge EBooks*, 2011. https://doi.org/10.4324/9780203814949.ch3_3_b.

Burchell, Graham, Colin Gordon, and Peter Miller. *The Foucault Effect: Studies in Governmentality : With Two Lectures by and an Interview with Michel Foucault*, 1991.

Božovič, M. (2010). Introduction: 'An utterly dark spot. In M. Božovič (Ed.), The panopticon writings (pp. 1– 28). London: Verso Books

Cohen, Stanley. *Visions of Social Control: Crime, Punishment and Classification*. Polity, 1991.

European Court of Human Rights, ed. *Guide On Article 11 Of The European Convention On Human Rights - Freedom Of Assembly And Association*, 2022.

Foucault, Michel, James D. Faubion, and Robert Hurley. *Power*, 2000.

Galič, Maša, Tjerk Timan, and Bert-Jaap Koops. "Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation." *Philosophy & Technology* 30, no. 1 (2016): 9–37. https://doi.org/10.1007/s13347-016-0219-1.

Greens/EFA. "Impacts of the Use of Biometric and Behavioural Mass Surveillance Technologies on Human Rights and the Rule of Law," February 2, 2022. https://www.greens-efa.eu/en/article/study/impacts-of-the-use-of-biometric-and-behavioural-mass-surveillance-technologies-on-human-rights-and-the-rule-of-law

Haggerty, Kevin P. "Surveillance, Crime and the Police." In *Routledge EBooks*, 2012. https://doi.org/10.4324/9780203814949.ch3_2_a.

Harwell, Drew. “Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use.” *Washington Post*, December 19, 2019. https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

———. “Oregon Became a Testing Ground for Amazon’s Facial-Recognition Policing. But What If Rekognition Gets It Wrong?” *Washington Post*, April 30, 2019. https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/.

Heyns, Christof. “General Comment No. 37.” *Article 21: Right of Peaceful Assembly’*, 2020.

ОВД-Инфо. “How the Russian State Uses Cameras against Protesters,” January 17, 2022. https://en.ovdinfo.org/how-authorities-use-cameras-and-facial-recognition-against-protesters

Jacobi, Anders, and Mikkel Holst. 2008. Synthesis Report - Interview Meetings on Security Technology and Privacy.

Johnson, Thaddeus L., Natasha N. Johnson, Denise McCurdy, and Michael S. Olajide. 2022. “Facial Recognition Systems in Policing and Racial Disparities in Arrests.” Government Information Quarterly 39 (4): 101753. https://doi.org/10.1016/j.giq.2022.101753.

Kelly, Heather, and Rachel Lerman. “America Is Awash in Cameras, a Double-Edged Sword for Protesters and Police.” *Washington Post*, June 3, 2020. https://www.washingtonpost.com/technology/2020/06/03/cameras-surveillance-police-protesters/.

Marciano, Avi. “Reframing Biometric Surveillance: From a Means of Inspection to a Form of Control.” *Ethics and Information Technology* 21, no. 2 (June 1, 2019): 127–36. https://doi.org/10.1007/s10676-018-9493-1.

Marx, Gary T.: Personal and Professional Encounters with Surveillance.” In *The Routledge Handbook of Surveillance Studies*, 1st ed., xx. Routledge, 2010.

OHCHR. “A/HRC/44/24: Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests,” n.d. https://www.ohchr.org/en/documents/thematic-reports/ahrc4424-impact-new-technologies-promotion-and-protection-human-rights

———. “Press Briefing Note on Protests and Unrest around the World,” n.d. https://www.ohchr.org/en/press-briefing-notes/2019/10/press-briefing-note-protests-and-unrest-around-world.

———. n.d. “Spyware and Surveillance: Threats to Privacy and Human Rights Growing, UN Report Warns.” https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report.

Reuters. 2022. “‘Orwellian’ Facial Recognition Cameras in UK Stores Challenged by Rights Group.” Reuters, July 26, 2022. https://www.reuters.com/world/uk/orwellian-facial-recognition-cameras-uk-stores-challenged-by-rights-group-2022-07-26/.

Scheinin, Martin. “Protection of Human Rights and Fundamental Freedoms While Countering

Terrorism : Note / by the Secretary-General." United Nations Archive, 2008. https://digitallibrary.un.org/record/635826.

Siatitsa, Ilia. "Freedom of Assembly under Attack: General and Indiscriminate Surveillance and Interference with Internet Communications." International Review of the Red Cross, March, 2021. https://international-review.icrc.org/articles/freedom-assembly-under-attack-surveillance-interference-internet-communications-913.

Stoddart, Eric. "A Surveillance of Care Evaluating Surveillance Ethically." In *The Routledge Handbook of Surveillance Studies*, 1st ed., 369. Routledge, 2012. https://www.taylorfrancis.com/chapters/edit/10.4324/9780203814949-58/surveillance-care-eric-stoddart.

UN Commission on Human Rights. "Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights." *UN Commission on Human Rights*. September 28, 1984. https://www.icj.org/wp-content/uploads/1984/07/Siracusa-principles-ICCPR-legal-submission-1985-eng.pdf.

UNGA Resolution, "The right to privacy in the digital age", Resolution n. 73/179, A/RES/73/179, Paragraph 9, 17 December 2018.