THE ADVENT OF FACIAL RECOGNITION AND THE EROSION OF THE RULE OF LAW IN "MOSCOW SMART CITY"

Antonina Semivolos[*]

TABLE OF CONTENTS

[*] Ms. Semivolos worked as a Trusts & Estates Paralegal in a boutique New York city law firm, and as an Electronic Discovery Paralegal for a large international law firm before attending Maurer School of Law. She later completed a joint degree in law and post-Soviet studies at Robert F. Byrnes Russian & East European Institute, and an MA in Telecommunications at the Media School, Indiana University Bloomington. Her professional focus is interrelation between personal data collection lawmaking and facial recognition technologies adaptation in Russia and the US.

INTRODUCTION

"It is perfectly proper to regard and study the law simply as a great anthropological document."
- Oliver Wendell Holmes[1]

Imagine searching your name on Google to find how much information about you is floating on the web, looking through all the posts you had shared on *Facebook*, *Instagram*, *LinkedIn*, or *VKontakte*[2] and, unexpectedly, your gaze meets a candid portrait of yourself. You hastily search your memory, and recognize the moment this photo was taken, although it was unbeknownst to you. You were riding the subway to work or back home, wearing your everyday clothes, leaning against a subway car wall, relaxing with your eyes closed, lost in your thoughts, or leaning forward to look at the screen of your cell phone—not posing.

This is how nearly one hundred of Egor Tsvetkov's unsuspecting models felt when they discovered that their faces were part of his 2016 online art exhibit "Your Face Is Big Data." When discussing the concept behind his work, the twenty-one-year-old St. Petersburg-based artist explained:

> Using free-for-all software [FindFace], I was looking for the profiles of people who sat in front of me in the subway car. I learned about the life of people without any contact with them through the photos on the social network [*VKontakte*] by comparing a real time image with a web representation. The ability [to] quickly and anonymous[ly] search . . . people in network helps trace not for impersonal subject. . . . [Indeed,] within seconds[,] [a stranger becomes] a friend incognito.[3]

Increasingly, an individual lacks control of when and how much of their personal information becomes public. One can remain invisible on the Internet, where a semblance of anonymity can still be preserved due to the nature of the web, but this same privilege cannot be exercised while taking a subway or strolling on the streets of such a megapolis as Moscow; equipped with over 200,000 closed circuit television ("CCTV")[4] cameras watching

---

[1] Oliver Wendall Holmes, *Law in Science and Science in Law*, 12 HARV. L. REV. 443, 444 (1899).

[2] *VKontakte* [*InContact*] – a Russian analogue of the American-based social media website *Facebook*. It is the most popular social network in Russia as approximately 75% of the Russian population uses it. *See* Human Rights Law Network, *A Conversation with Agora's Damir Gainutdinov on Internet Shutdowns, Facial Recognition and Backdoors in Russia*, YOUTUBE (June 4, 2021), https://www.youtube.com/watch?v=yS5MjyBBVss&ab_channel=HumanRightsLawNetwork.

[3] Egor Tsvetkov, *Your Face is Big Data* (photograph), KIND OF EXPOSITION FESTIVAL PRESENCE (2017) https://cargocollective.com/egortsvetkov/Your-Face-Is-Big-Data.

[4] CCTV is an acronym for "closed-circuit television" and is also known as video surveillance. "Closed-circuit" means broadcasts are usually transmitted to a limited (closed) number of monitors, unlike "regular" TV, which is broadcast to the public at large. For example, CCTV networks are commonly used to detect and deter criminal activities, record traffic infractions, but they can have multiple other uses. *See Monitor Your CCTV System with PRTG*, PAESSLER, https://www.paessler.com/cctv-monitoring (last visited: March 25, 2023).

vigilantly over every movement of the city's inhabitants.[5]

Tsvetkov's art project was possible because of the advent of a powerful artificial intelligence-based technology ("AI"): the facial recognition algorithm developed by the Russian NtechLab.[6] NtechLab's FindFace became publicly available in Russia for a short period in 2016.[7] Tsvetkov was one of the software's many first users; uploading it to his cell phone and using it as a tool in his art exhibit. FindFace access allowed the artist to scan social network profiles of fifty-five million users of *VKontakte*,[8] and to identify approximately seventy percent of unsuspecting strangers while working on his art exhibit.[9] Being a rather private user of social media, Tsvetkov wanted his artistic statement to make people see the capabilities of interplay between AI-based technologies and their social media habits of revealing too much personal information in a newer, more menacing light.[10]

> Technological developments take away the monopoly to identify an individual with the help of a photo or a video from government structures, and, in fact, give it to any interested party. Unaware of this, people continue to practice their habitual models of behavior, being private in public, but opening up on social media. They provide strangers with the ability to watch over their lives over the Internet, and this digital narcissism in many ways defines boundaries of what is private and public in our times. By not using privacy settings, we often provoke network stalking.[11]

Tsvetkov also stated that his "project is a clear illustration of the future that

---

[5] Jarron Kamphorst, *Mass Surveillance In Russia: In Moscow 200.000 Cameras Recognize Citizens Everywhere*, PARTITO RADICALE (Mar. 16, 2020), https://www.partitoradicale.it/en/2020/03/22/mass-surveillance-in-russia-in-moscow-200-000-cameras-recognise-citizens-everywhere/.

[6] One of the country's leading facial recognition AI startups, NtechLab won IARPA's 2017 Face Recognition Prize Challenge for its FindFace application, which allowed users to find people's profiles with a photo on Russia's popular social media network, *VKontakte*. *See* Stephen Mayhew, *Ntechlab wins two categories at Face Recognition Prize Challenge*, BIOMETRIC UPDATE (Nov. 7, 2017), https://www.biometricupdate.com/201711/ntechlab-wins-two-categories-at-face-recognition-prize-challenge.

[7] Shaun Walker, *Face Recognition App Taking Russia By Storm May Bring End To Public Anonymity: FindFace Compares Photos To Profile Pictures On Social Network Vkontakte And Works Out Identities With 70% Reliability*, GUARDIAN (May 17, 2016), https://www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte.

[8] LMA, *Russian Photographer Uses Facial Recognition to Find People He Snaps on Subway, and the Results Are Scary,* BOREDPANDA (2017), https://www.boredpanda.com/face-recognition-photography-your-face-is-big-data-egor-tsvetkov/?utm_source=google&utm_medium=organic&utm_campaign=organic.

[9] *Id.*

[10] Egor Tsvetkov, Konets anonimnosti: Identifikatsiia sluchaĭnykh poputchikov [The End of Anonymity: Identification of Accidental Travel Companions], BIRD FLIGHT (Apr. 6, 2016), https://birdinflight.com/ru/vdohnovenie/fotoproect/06042016-face-big-data.html (Russ.).

[11] *Id.; see also* EGOR TSVETKOV, https://cargocollective.com/egortsvetkov (last visited: March 25, 2023).

awaits us if we continue to disclose as much about ourselves on the internet as we do now."[12] Any stranger possessing elementary technological capabilities can use publicly available photos uploaded to social media—as well as facial recognition applications—as tools to collect even greater amounts of personal data, unbeknownst to the subjects of said data collection. The crux of his art project revolved around "the most personal part"[13] of human biometric data: the face.

Over the last several years, Moscow has been transformed into a "smart city," defined by the official website of the Mayor of Moscow as "a system of city service resources that are used as efficiently as possible to provide maximum convenience for its residents. It requires close connection between smart city projects (street CCTV cameras, public services, smart transport systems and others) in a megalopolis."[14] This article analyzes the administrative and legal techniques that the Russian government has utilized to commence the construction of the Moscow "Smart City," while also targeting the erosion of the rule of law[15] and of civil society.[16] Further, this article underscores that facial recognition is an important element in the contemporary smart city architecture and infrastructure.[17] More specifically, this article alludes to the Mayor of Moscow's official report "Moscow 'the Smart city—2030': Text of the Strategy" ("Moscow Smart City Report

[12] LMA, *supra* note 8.

[13] Alexander Von Humboldt Institute for Internet & Society, *Shoshana Zuboff: Surveillance Capitalism and Democracy*, YOUTUBE (Aug. 11, 2022), https://www.youtube.com/watch?v=fJ0josfRzp4&ab_channel=AlexandervonHumboldtInstitutf%C3%BCrInternetundGesellschaft.

[14] *Merging Reality and VR: How Does a Smart City Work?,* MOSCOW MAYOR OFFICIAL WEBSITE, https://www.mos.ru/en/city/projects/smartcity/#:~:text=Moscow%20is%20second%20in%20fixed,detectors%20and%202%2C000%20CCTV%20cameras (last visited Apr. 27, 2023); *see* Sharon Shea & Ed Burns, *Smart City*, TECHTARGET, https://www.techtarget.com/iotagenda/definition/smart-city (last visited Aug. 3, 2022). Some experts argue that, first and foremost, a smart city is an important means to collect large amounts of personal data from its inhabitants while the latter engage in their routine usages of home appliances, transportation (smart cars), shopping, etc. *Id. See also Shoshana Zuboff: Surveillance Capitalism and Democracy*, *supra* note 13; BRUCE STERLING, THE EPIC STRUGGLE OF THE INTERNET OF THINGS (Strelka Press 2014).

[15] The rule of law is defined as:

> [A] set of principles, or ideals, for ensuring an orderly and just society. Many countries throughout the world strive to uphold the rule of law where no one is above the law, everyone is treated equally under the law, everyone is held accountable to the same laws, there are clear and fair processes for enforcing laws, there is an independent judiciary, and human rights are guaranteed for all.

Rule of Law, American Bar Association, https://www.americanbar.org/groups/public_education/resources/rule-of-law/ (last visited: March 25, 2023).

[16] Masha Borak, *Inside Safe City, Moscow's AI Surveillance Dystopia: Moscow Promised Residents Lower Crime Rates Through an Expansive Smart Project. Then Vladimir Putin Invaded Ukraine.,* WIRED (Feb. 6, 2023), https://www.wired.com/story/moscow-safe-city-ntechlab/ .

[17] *Id.*

2030"), published in 2018.[18] Emerging trends such as AI-based technologies and the Internet of Things ("IoT"),[19] in which physical objects have sensors that communicate with computing systems via wireless or wired networks, are accompanying Moscow's technological emergence and growth.[20] The Mayor of Moscow, Sergey Sobyanin, describes what the administrators and futurologists involved in the creation of Moscow as a Smart City see as underlying principles of their work:

> We've accomplished a lot, but life keeps changing, giving us new responsibilities. New technologies appear, that's why we must progress to new levels as well. We must expand our electronic services, and those of the information city. Already today, we can talk not just about separate services, but about the creation of a complex program "Smart city," which would grow into all areas of our life.[21]

Broadly, Mayor Sobyanin depicts the smart city as an essential force behind the existence of every Moscovite, which allows everyone's life and sought-after services to become interconnected in one complex eco-system.[22] Interestingly, Mayor Sobyanin's argument is circular, in that he posits scientific advances as a major stimulus for Moscovites to become even more technologically advanced, with the help of more sophisticated innovations which, in turn, are closely interconnected with their everyday life.

On one hand, administrative and scientific accounts within the Moscow Smart City Report 2030 are rosy and optimistic. Some experts studying smart cities posit that the innovations, and the growing presence of informational technologies in citizens' lives, will make governance more

---

[18] Moskva "Umnyĭ gorod – 2030": Tekst strategii [*Moscow "Smart city – 2030": Text of the Strategy*] (2018), https://www.mos.ru/upload/alerts/files/3_Tekststrategii.pdf (last visited Aug. 15, 2022) [hereinafter "Moscow Smart City Report 2030"].

[19] STERLING, *supra* note 14. Importantly, according to Sterling, "The first thing to understand about the 'Internet of Things' is that it's not about Things on the Internet. It's a code term that powerful stakeholders have settled on for their own purposes. They like the slogan 'Internet of Things' because it sounds peaceable and progressive." *Id.* Sterling elaborates on this term, explaining that "[i]t disguises the epic struggle over power, money and influence that is about to ensue. There is genuine internet technology involved in the 'Internet of Things.' However, the legacy internet of yesterday is a shrinking part of what is at stake now." *Id.*

[20] *Moscow Smart City by 2030: Current Project: Russia's Capital is Among the World's Sustainable Mobility*, WE BUILD VALUE DIGIT. MAG. (Aug. 7, 2020), https://www.webuildvalue.com/en/megatrends/moscow-smart-city.html; *see also* Borak, *supra* note 16 ("'Facial recognition was supposed to be the 'cherry on top,' the reason why all of this was built,' sa[id] a former employee of NTechLab, one of the principal companies building Safe City's face recognition system.").

[21] Sergey S. Sobyanin, *Presentation at the official meeting of Moscow's government* (Apr. 10, 2018), https://www.mos.ru/mayor/media/video/6470057/; *see also* Moscow Smart City Report 2030, *supra* note 18.

[22] Shea & Burns, *supra* note 14.

accessible and efficient.[23] Well-established online platforms such as "Our City" allow Moscovites a way to openly critique city services, or alternatively the "Active Citizen" platform allows Moscow inhabitants to vote on urban development issues.[24] On the other hand, the emergence of a more sophisticated means to surveil the city's population is taking place simultaneously.[25] This article explores the more subtle, yet still important, processes that energize the smart city creation: the administrative and legal agendas that influence the adaptation of facial recognition technologies in Moscow, and how the latter affect the life of Russian civil society and its basic engine—i.e., the rule of law.

The distinguished American journalism historian David Nord once stated that the administrative processes accompanying the adaptation and spread of a novel technology are uniquely potent because "organization and administration . . . are much more important than the technology itself in the process of technological innovation."[26] More importantly, it is "[o]rganization and administration that give economic and social meaning to [a new] technology."[27] Similarly, AI researcher turned humanities professor Philip Agre wrote in his 2002 article "Real-Time Politics: The Internet and the Political Process" that it is still difficult to foresee whether or not novel communications technologies will lead to the expansion of civil freedoms and, as a result, to the democratization of societies.[28] According to Professor Agre's prescient theoretical model, our future can become a mere "amplification" of our past.[29] One such novel technology that preceded facial recognition was the Internet, which did not create any new norms; just as any

[23] Lily Sabol, *Smart Cities and Democratic Vulnerabilities*, NAT'L ENDOWMENT FOR DEMOCRACY (Dec. 15, 2022), https://www.ned.org/smart-cities-and-democratic-vulnerabilities/; *see also* Beth Kerley, Roukaya Kasenally, Bárbara Simão & Blenda Santos, *Smart Cities and Democratic Vulnerabilities,* NAT'L ENDOWMENT FOR DEMOCRACY 2, https://www.ned.org/wp-content/uploads/2022/12/Smart-Cities-and-Democratic-Vulnerabilities.pdf (last visited Mar. 25, 2023) ("Often viewed as tools to make governance more transparent, accountable, and inclusive, emerging technologies also present increasingly clear opportunities for current and aspiring authoritarians.").

[24] *Moscow: The Smart City That's About to Get (A Lot) Smarter . . .*, INTECHNOLOGY, https://www.intechnologysmartcities.com/blog/moscow-smart-city-to-get-much-smarter/ (last visited Aug. 11, 2022).

[25] *Interview: Authoritarian Governments Have Immensely Benefited from The Web, the Author Says*, RADIO FREE EUR./RADIO LIBERTY (Jan. 22, 2011), https://www.rferl.org/a/interview_morozov_internet_democracy_promotion/2284105.html.

[26] David P. Nord, *The Ironies of Communication Technology: Why Predictions of the Future So Often Go Wrong*, CRESSET 15, 18 (1986).

[27] *Id.*

[28] Philip E. Agre, *Real-Time Politics: The Internet and the Political Process*, 18 INFO. SOC'Y 311 (2002).

[29] *Id*. Per Agre, in case of any political institution's life, its "participants appropriate the technology in the service of goals, strategies, and relationships that the institution has already organized. This amplification model can be applied in analyzing the Internet's role in politics." *Id.*

other novel technology, it merely "amplified" existing societal norms.[30] Professor Agre uses Internet's role in politics as the context for his theoretical model, which can be applied to any other technology.[31] This model, the "amplification model," is a response to "technological determinism" which is an assumption that it is "the technology [that] imprints its own logic on social relationships."[32] Contrarywise, the "amplification model" demonstrates the ways "in which an institution's participants appropriate [any given] technology in the service of goals, strategies, and relationships that the institution has already organized."[33]

The administration and adaptation of AI-based technologies, including facial recognition, closely follow the path that had been paved for them by the adaptation processes of the Internet. According to Damir Gainutdinov, legal analyst at the international human rights NGO Agora,[34] when Vladimir Putin became the President of Russia in 2000, he established absolute control over televised media, while the Internet remained free.[35] In 2003, Russia's Internet audience included nearly three million users, only a small percentage of the country's population.[36] Now, there are approximately ninety-five million active Internet users in Russia, more than eighty percent of the country's population.[37] The Internet could no longer be viewed as an innocent communications platform, but rather as "a main source of social and political information, and a platform [for] mobilization for political activities."[38] This was one of the reasons that pushed the Russian government to establish stricter control over the Internet.[39]

The development of the AI industry in Russia has been closely interwoven with the agenda of President Putin's government from its very conception. AI-related scientific research in Russia is predominantly state-led and state-sponsored.[40] President Putin has stressed on numerous occasions that a nation leading in AI science will undoubtedly become the

---

30 *Id.* at 315.

31 *Id.*

32 *Id.*

33 *Id.*

34 *See Agora International Human Rights Group*, INT'L NETWORK C.L. ORG., https://www.inclo.net/members/agora/ (last visited Feb. 22, 2023).

35 Human Rights Law Network*, supra* note 2.

36 *Id.*

37 *Id.*

38 *Id.*

39 *Id.*

40 Margarita Konaev & James Dunham, *Russian AI Research 2010 to 2018: Topics, Trends, and Institutions, Center for Security and Emerging Technology Issue Brief*, CNTR. FOR SEC. & EMERGING TECH. (2020), https://doi.org/10.51593/20200040.

"ruler of the world."[41] The official agency, Russian AI Alliance, was founded in 2019 in order to facilitate "the development of AI . . . for education, research and practical applications."[42] As a result, the country is now rapidly catching up with the scientific research produced in China and the US.[43] The AI Alliance is tasked with the politically important goal of promoting Russia's AI-based technologies.[44] Russian society at large was led to swiftly adapt to this new technological era, characterized by omnipresent CCTV cameras and rapidly improving—but mostly unregulated—facial recognition technologies. Notably, even though facial recognition technologies have been used within Russia "for over ten years, there are almost no laws" addressing the existence and usages of such technologies by law enforcement agencies, the private sector, or individuals.[45]

In this article, I first outline notable characteristics of scientific origins of facial recognition technology from the 1960's through to today, including one of the technology's crucial operational features is its great dependance on the quantity and quality of personal and biometric data collected.[46] Part I examines the chronology of how facial recognition technologies have been developed, installed, and regulated specifically by Moscow's various governmental agencies. The adaptation of facial recognition technology in Russia has occurred in the absence of law-making and procedural processes that would otherwise guarantee necessary oversight. Notably, the lack of adequate legal regulation regarding AI-technologies has been accompanied by the decisions of the courts which time and again have ruled that collection of biometric data on the streets of Moscow and Russia does not warrant protections under Russia's existing personal data laws.[47]

In Part II, I demonstrate how the district courts do not view individuals' personal data collected on the streets of Moscow as "personal"

---

[41] James Vincent, *Putin Says the Nation that Leads in AI 'Will be the Ruler of the World'*, VERGE (Sept. 4, 2017), https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world.

[42] AI ALL. RUSS., https://a-ai.ru/en/ (last visited Nov. 16, 2022).

[43] Nikolai Markotkin & Elena Chernenko, *Developing Artificial Intelligence in Russia: Objectives and Reality*, CARNEGIE ENDOWMENT FOR INT'L PEACE (May 8, 2020), https://carnegiemoscow.org/commentary/82422.

[44] *See* AI ALL. RUSS., *supra* note 42.

[45] Damir Gainutdinov & Kirill Koroteev, Raspoznavanie lits: predchuvstvie antiutopii [Facial Recognition: the Vision of Dystopia], NETWORK FREEDOMS REP., https://runet.report/static/core/doc/Facial_recognition.pdf (last visited Nov. 16, 2022) (Russ.).

[46] Leif-Nissen Lundbæk, *The Road to Disastrous Biometric Data Collection is Paved with Good Intentions*, TECHCRUNCH (Jan. 10, 2022), https://techcrunch.com/2022/01/10/the-road-to-disastrous-biometric-data-collection-is-paved-with-good-intentions/.

[47] *Russia: Broad Facial Recognition Use Undermines Rights*, HUM. RTS. WATCH (Sept. 15, 2021), https://www.hrw.org/news/2021/09/15/russia-broad-facial-recognition-use-undermines-rights.

or "biometric data"—a necessary condition for such data's protections under Russia's personal data laws.[48]

Part III focuses on the phenomenon of *post factum* detention,[49] or detentions taking place surrounding any forms of protest. Ethnographically speaking, this detention is one of the more visible factual examples of how the Russian government utilizes novel technologies to extend its control and to prevent political opposition.[50] The Russian government achieves this goal with the help of most advanced technological means available, such as CCTV cameras equipped with facial recognition software, used ubiquitously on the streets of Moscow.[51]

I conclude that based on Agre's "amplification model,"[52] present political power dynamics in Russia are such that facial recognition technologies, and other AI-based technologies, are being used by the Russian government as potent tools to strengthen, perfect, and expand the current authoritarian regime.[53] The rule of law—as a foundational principle ensuring a just society—in tandem with Russian civil society may be the only means to challenge such autocratic tendencies, providing the potential for oversight and to hold those who govern accountable—especially so because there is no official non-government agency that would do so otherwise.[54] AI-based technologies are being adapted rapidly throughout the country despite many

---

[48] *Id.*

[49] *How the Russian state uses cameras against protesters,* OVD-INFO REPORT (Jan. 17, 2022), https://en.ovdinfo.org/how-authorities-use-cameras-and-facial-recognition-against-protesters#1.

[50] Zhaloba v Sovet po pravam cheloveka pri Presidente RF [Complaint from OVD-Info Attorneys, to Human Rights Council under the President of the Russian Federation] (Jun. 7, 2021) (on file with author).

[51] OVD-INFO REPORT, *supra* note 49 ("Our report is devoted to the use of facial recognition systems to restrict freedom of assembly. Although our research focuses on Moscow, according to our data, the geography of this phenomenon goes far beyond the capital.").

[52] Agre, *supra* note 28, at 311.

[53] Nicholas D. Wright, *Artificial Intelligence, China, Russia, and the Global Order*, AIR UNIV. PRESS (Oct. 19, 2019), https://www.airuniversity.af.edu/portals/10/aupress/books/b_0161_wright_artificial_intelligence_china_russia_and_the_global_order.pdf.

[54] From multiple talks by, and press interviews of digital rights attorneys, including those representing such civil society organizations as Roskomsvoboda, Agora, OVD-Info, Citizen Control, and the Moscow Helsinki Group (MHG). For instance, from the interview of Sarkis Darbinian, an attorney at Roskomsvoboda, Russia does not have an agency that would oversee personal data collection in an impartial manner. He compares this to what's taking place in Georgia, where such impartial agency is present. *See* Novaya Gazeta, Za vami slediat? Kak gosudarstvo ispol'zuet sistemu raspoznavaniia lits | Razberemsia s Vorob'evoĭ [Are you being watched? How the government uses system of facial recognition | Figuring it out with Vorob'eva], YOUTUBE (July 27, 2021) https://www.youtube.com/watch?v=DegHlfGuRGI&ab_channel=%D0%9D%D0%BE%D0%B2%D0%B0%D1%8F%D0%B3%D0%B0%D0%B7%D0%B5%D1%82%D0%B0 (Russ.).

violations of civil liberties due to how they are being utilized by the law enforcement in latter's effort to dampen civil protest.[55]

I. FACIAL RECOGNITION ORIGINS AND TECHNOLOGY'S CHARACTERISTIC DEPENDANCE ON PERSONAL DATA COLLECTION

The origins of facial recognition are shrouded in secrecy. Shaun Raviv of *WIRED Magazine* wrote an essay on the life of its founder—Woodrow Wilson Bledsoe, born in Oklahoma in 1921—beginning with the description of how the seventy-four-year-old scientist instructed his son to burn the contents of his secret garage safe.[56] No one will ever know what Dr. Bledsoe wanted to conceal from subsequent chapters of facial recognition history. "Woody's facial-recognition research in the 1960's prefigured all [current day] technological breakthroughs and their queasy ethical implications. And yet his early, foundational work on the subject is almost entirely unknown. Much of it was never made public."[57]

In the nineteen-page essay, titled "In Memoriam—Woodrow Wilson Bledsoe," fellow scholars commemorating their colleague's life and work wrote that "Woody was one of the founders of Artificial Intelligence . . . making early contributions in pattern recognition and automated reasoning."[58] Even as early as at the start of his scientific career in late 1950s, Dr. Bledsoe had been driven by his insatiable enthusiasm "to give machines one particular, relatively unsung, but dangerously powerful human capacity: the ability to recognize faces."[59]

Notably, the employment of facial recognition research by governmental institutions goes back to its very beginnings, when in 1967—more than a year after his move to Austin to teach at the University of Texas at Austin—Dr. Bledsoe took on one final assignment that involved recognizing patterns in the human face.[60] The purpose of the experiment was to assist law enforcement agencies to "sift through databases of mug

---

[55] OVD-INFO REPORT, *supra* note 49 ("In combination with the lack of transparency of usage and the lack of public control, it is possible to turn this technology into an instrument of politically motivated persecution.").

[56] Shaun Raviv, *The Secret History of Facial Recognition: Sixty years ago, a sharecropper's son invented a technology to identify faces. Then the record of his role all but vanished. Who was Woody Bledsoe, and who was he working for?*, WIRED (Jan. 21, 2020), https://www.wired.com/story/secret-history-facial-recognition/; *see also* Michael Ballantyne, Robert S. Boyer & Larry Hines, *Woody Bledsoe: His Life and Legacy*, AI MAG., 1996, at 7.

[57] Raviv, *supra* note 56.

[58] Ballantyne, Boyer, & Hines, *supra* note 56.

[59] Raviv, *supra* note 56.

[60] *Id.*

shots and portraits, looking for matches" at an accelerated speed.[61] The outcome was a success.[62]

Some of Dr. Bledsoe's scientific work has been recorded and preserved; all thirty-nine boxes of the black and white photographs of individuals' faces with which Dr. Bledsoe had initiated his studies are carefully kept at the Briscoe Center for American History at the University of Texas at Austin.[63] Some portraits display numbered arrows pointing to selected areas of facial landscape.[64] These archaic yellowish photos are some of the first prototypes of facial geometry images featured on websites of such AI-centered companies as the American Clearview AI, and their Russian analogues—NtechLab and VisionLabs.[65] They are the legitimate predecessors to what has become a familiar hallmark of facial recognition presence in international airports, on cruise lines, in popular theme parks, and governmental reports on smart cities and the IoT.[66]

Shortly after receiving his doctorate from the University of California at Berkeley, Dr. Bledsoe went to work for the Sandia Corporation in New Mexico, funded primarily by the Atomic Energy Commission for the purpose of nuclear and defense research.[67] In 1959, Dr. Bledsoe teamed up with a fellow Sandia employee, Iben Browning, to work on pattern recognition:[68]

> Woody took an interest in automated pattern recognition, especially machine reading—the process of teaching a computer to recognize unlabeled images of written characters. . . . The beauty of the *n*-tuple method was that it could recognize many variants of the same character: Most *Q*s tended to score pretty close to other *Q*s. Better yet, the process worked with any pattern, not just text. According to an essay coauthored by Robert S. Boyer, a mathematician and longtime friend of Woody's, the *n*-tuple method helped define the field of pattern recognition; it was among the early set of efforts to ask, "How can we make a machine do something like what people do?"[69]

---

61 *Id.*

62 *Id.*

63 *Id*.

64 *Id*. (Author's description of the photo featured within Raviv's article).

65 *See* NTECH LAB, https://ntechlab.com/ (last visited Nov. 28, 2022).

66 *See Internet of Things: Definition, Components & Examples*, STUDY.COM, https://study.com/academy/lesson/internet-of-things-definition-components-examples.html?src=ppc_adwords_nonbrand&rcntxt=aws&crt=646616438141&kwd=&kwid=dsa-1253079156202&agid=125582019081&mt=&device=c&network=g&_campaign=SeoPPC-desktop&gclid=EAIaIQobChMIn4jUsdeu_QIVAZ2GCh0l4QyLEAAYBCAAEgLe9PD_BwE (last visited March 25, 2023) ("The Internet of Things is the idea of everyday objects like light bulbs and thermostats being connected to the Internet, enabling us to communicate with devices and allowing devices to 'talk' to each other.").

67 Ballantyne, Boyer, & Hines, *supra* note 56.

68 *Id.*

69 Raviv, *supra* note 56.

At the outset of their collaboration, Dr. Bledsoe and his colleagues would attempt to teach a computer to recognize as few as ten faces.[70] It may seem like a negligible number today, but in 1963 this undertaking was deemed original and ambitious.[71] Furthermore, the leap from computer recognition of written letter characters to recognition of human faces was a major advancement in the science of the time.[72] Contemporary scientists working with facial recognition can train their algorithms on billions of publicly available selfies and other photos of faces by taking or "web scraping"[73] these images from such massively-used platforms as Facebook, Google, Twitter, and LinkedIn, without the consent of a particular website or that of its users.[74] In contrast, there was no established method for digitizing photos and database of digital images at the time Dr. Bledsoe and his colleagues' research.[75] The improvement and
ubiquitous usages of facial recognition algorithm in recent decades have been accelerating at a speed Dr. Bledsoe and his colleagues might not have imagined.

Interestingly, in terms of its long-term societal effects, the potentially dystopian capabilities and ethical concerns surrounding the use of facial recognition technology were apparent during its initiation at Panoramic.[76] Many of the possible biases that had been encountered by the

---

[70] *Id.*

[71] *Id.*

[72] Woodrow W. Bledsoe, *A Facial Recognition Project Report,* INTERNETARCHIVE, https://archive.org/details/firstfacialrecognitionresearch/FirstReport/page/n1/mode/2up (last visited March 25, 2023)

> The first report, 'A Proposal For A Study To Determine The Feasibility Of A Simplified Face Recognition Machine', dated 30 January 1963, aims to evaluate whether it is possible using existing technology to create a machine which can reliably solve a simplified face recognition problem: using only pictures from a single view (e.g. same angle & perspective) as well as high resolution pictures, identify the identity or a person from a picture that is not known to the machine." Further, the second report by Bledsoe concluded that "picture recognition by machines for a large sample of people is beyond the state of the art of the present pattern recognition and computer technology at this time."

Id.

[73] Zack Whittaker, *Web Scraping is Legal, US Appeals Court Reaffirms*, TECHCRUNCH (Apr. 18, 2022, 2:16 PM), https://techcrunch.com/2022/04/18/web-scraping-legal-court/?mkt_tok=mtm4luvats0wndiaaagd4breniy7c54t5jjupzo_eb7i4q4go48jvvpvvoqsmnmwzw4u-zoeb6qm4vz3m6zgzxx_n7mmzehdefi0evlhcesbndoufhmrfifcvauz2zx0.

[74] Isaiah Richard, *Web Scraping is Legal, US Appeals Court Reaffirms*, TECH TIMES (June 7, 2022, 12:06 PM), https://www.techtimes.com/articles/276430/20220607/web-scraping-is-legal-us-appeals-court-reaffirms.htm#:~:text=On%20September%209th%2C%202019%2C%20the,privacy%2C%20the%20ruling%20was%20issued.

[75] Raviv, *supra* note 56.

[76] *Id. See also* Harmon Leon, *How LSD, Nuclear Weapons Led to the Development of Facial Recognition*, OBSERVER (Jan. 29, 2020), https://observer.com/2020/01/facial-recognition-development-

technology's founders, such as working "sample sets skewed almost entirely toward white men[,] the seemingly blithe trust in government authority[,] the temptation to use facial recognition to discriminate between races,"[77] live on even today, empowered by the vast amounts of personal and biometric data being collected for the improvement of the facial recognition algorithm and that of other AI-related inventions.

A. The Russian Origins of Facial Recognition Software: Usages and Peculiarities in Moscow "Smart City"

The Russian government has viewed facial recognition algorithms as a rather sensitive area. At first glance, this technology's origins in Russian do not appear to be much different from its origins in the United States. But while studying respective histories deeper, it becomes apparent that the technology's emergence in the 1960s took place in science labs, with minimal access to personal data, for the Internet had not yet existed, as well as "web scraping" that would allow the collection of vast amounts of publicly accessible photos of individuals.[78] In contrast, since at least 2015, Russian NtechLab scientists have used the personal data of Russian citizenry as a feed for their controversial algorithm.[79] More than forty years after Dr. Bledsoe's pattern recognition research began, contemporary companies producing facial recognition software—such as the Russian NtechLab,[80] or the American Clearview AI[81]—now have access to billions of individuals' publicly posted photos that they "scrape" from the web in order to keep improving the precision of the facial recognition software.[82] These AI-related companies have complex relationships with their respective governments.[83] Ultimately, in the case of Russia, facial recognition

history-woody-bledsoe-cia/ ("In 1960, Bledsoe and [his] colleagues started a company in Palo Alto . . . Panoramic Research Incorporate. One of the company's projects was character-recognition technology.").

77 Raviv, *supra* note 56.

78 *Id.*; *see also* Whittaker, *supra* note 73.

79 Adrien Henni, *Business Insider: Western Tech Majors Tested or Used Controversial Russian Face Recognition Technology*, E.W. DIGIT. NEWS (Aug. 5, 2022), https://www.ewdn.com/2022/08/05/business-insider-western-tech-majors-tested-or-used-controversial-russian-face-recognition-technology/.

80 NTECH LAB, *supra* note 65.

81 To learn about history and work of the American Clearview AI, explore articles written by the investigative journalist Kashmir Hill for N.Y. Times. *See* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Nov. 2, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; *see also* Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

82 Shing Tse & Kristin L. Bryan, *hiQ Labs v. Linkedin,* NAT'L L. REV. (Apr. 19, 2022), https://www.natlawreview.com/article/hiq-labs-v-linkedin; HIQ Labs, Inc. v. Linkedin Corp, 273 F. Supp. 3d 1099 (N.D. Cal. 2017).

83 Wright, *supra* note 53.

software-producing companies NtechLab and VisionLabs[84] have been closely interconnected with the workings of various governmental agencies, including the Department of Information Technology ("DIT") overseeing the network of the city's CCTV cameras and Moscow city government.[85] Just as with experimentations undertaken by Dr. Bledsoe and his colleagues in the U.S. during the 1960s, the funding and work of NtechLab are closely interwoven with the government and its investment activities, fueling the present-day AI industry in Russia.[86] Having won multiple western technological competitions, NtechLab boasts of their recent achievements on the home page of their website:

> NtechLab technology is recognized as the most accurate face recognition neural network in the world, according to the National Institute of Standards and Technology ("NIST") testing in May 2021. Our algorithms have repeatedly proven their superiority in many other independent competitions and tests.[87]

NtechLab was chosen to be the producer of the facial recognition software FindFace used for Moscow's facial recognition cameras.[88] Previously, NtechLab had also been granted access by the Russian government to the personal data of about two hundred million *VKontakte* ("VK") users who had acquired their software around 2016, prior to the 2018 FIFA World Cup hosted in Russia—when CCTV cameras started being used on a massive scale in preparation for the sports competition.[89] This original "nation-wide experiment" was conducted to test the novel facial recognition software on a country-wide scale, and crucially without adequate protections under Russia's existing personal data laws.[90] It was this "nation-wide experiment"

---

[84] *See About Us*, VISIONLABS, https://visionlabs.ai/about-us/ (last visited Nov. 22, 2022) ("VisionLabs is a team of Computer Vision and Machine Learning experts. [They] specialize in developing products and solutions in the areas of face recognition, object recognition, augmented reality and virtual reality.").

[85] Borak, *supra* note 16 ("Although the system is run by the Moscow government, elected members of the Moscow City Duma say they are excluded from regulating face recognition systems and have little insight into how it is being used.").

[86] *Moscow Mayor's Office will hand over photos of mos.ru users to the police*, TIME NEWS (Oct. 13, 2021), https://time.news/moscow-mayors-office-will-hand-over-photos-of-mos-ru-users-to-the-police/.

[87] NTECH LAB, *supra* note 65 (*see* company's website to learn more about their services at https://ntechlab.com/).

[88] Borak, *supra* note 16 ("NtechLab, [is] one of the principal companies building Safe City's face recognition system.").

[89] Felix Light, *Russia is building one of the world's largest facial recognition networks,* CODA (Nov. 8, 2019), https://www.codastory.com/authoritarian-tech/russia-facial-recognition-networks/.

[90] *Id.*

> In both [China and Russia], underdeveloped data protection laws mean research is easier, with AI companies able to buy or mine huge amounts of data on which to train their algorithms. In Russia, *VKontakte*'s privacy policies, less restrictive than other social networks', have provided a huge bank of personal data for local AI researchers. Today, as

that became an inspiration for Egor Tsvetkov's "Your Face Is Big Data," the online art exhibit discussed earlier.[91] Further, the special treatment of the AI industry by the Russian government serves the government's interests as well, since the AI industry gives the government access to some of the most developed facial recognition software around the world.[92] Consequently, data collected through NtechLab's facial recognition technology—as well as through the DIT's CCTV network—is used as evidence in administrative hearings connected to *post factum* detentions,[93] discussed further in Part III.[94]

Notably, NtechLab[95] receives its main financial backing from Rostec,[96] a state-owned holding conglomerate headquartered in Moscow specializing in investing in strategically important companies, mainly in the defense and high-tech industries.[97] Rostec controls twelve-and-a-half percent of NtechLab, Ruben Vardanian's Fund[98] controls twenty five percent, and the rest is controlled by the five founders and original investors.[99] The full monetary value of the company's contract with the DIT is not known.[100] The initial price in contract documents was listed as 200 million rubles (3.1

> Russia continues to escalate its domestic facial recognition program, some fear that the system could be used to create the kind of surveillance apparatus taking shape over the Chinese border.

Id.

[91] Kevin Rothrock, *The Russian Art of Meta-Stalking,* GLOB. VOICES (Apr. 7, 2016), https://globalvoices.org/2016/04/07/in-russia-your-face-is-big-data/.

[92] Dioga Costa, *N-Tech.Lab is Pushing the Boundaries of Artificial Intelligence*, ENGADGET (Jul. 21, 2016), https://www.engadget.com/2016-07-21-n-tech-lab-is-pushing-the-boundaries-of-artificial-intelligence.html.

[93] *Russia: Broad Facial Recognition Use Undermines Rights, supra* note 47 ("*Post factum*" detentions are detentions of protesters that take place "after the end of the event." *Post factum* detentions can take place days, weeks, or even months after the protest in question.) (emphasis added).

[94] Gianluca Mezzofiore, *Moscow's facial recognition CCTV network is the biggest example of surveillance society yet*, MASHABLE (Sep. 28, 2017), https://www.engadget.com/2016-07-21-n-tech-lab-is-pushing-the-boundaries-of-artificial-intelligence.html.

[95] Ntechlab – kto eto? Horoshyĭ vopros [NtechLab – who is it? That's a good question], BANCAM.RU, https://bancam.ru/ntechlab2?fbclid=IwAR0JKG5JziXMU4W3d1K00Z3hDOV1Hgynfe3-9VpZcxKhrJ3dkYGhrJrIn40 (last visited Aug. 15, 2022) (Russ.). As to NtechLab's talent, Artem Kukharenko, one of the inventors of the 2015 FindFace facial recognition algorithm, is portrayed by the national media as a celebrity; among other tech competitors, Kukharenko won first place in a 2015 Washington University tech competition, defeating notable competitors, including Google. *Id.*

[96] *See* ROSTEC, https://rostec.ru/en/about/ (last visited Feb. 19, 2023). The State Corporation for the Promotion of the Development, Manufacture, and Export of High Tech Products "Rostec," a Russian state-owned holding conglomerate. *Id.*

[97] *Id.*

[98] *See* Vlasti Moskvy vybrali tekhnologii dlia sistemy poiska i raspoznavaniia lits [Moscow Mayor Office Decided Which Facial Recognition Software the City Will Use], LENTA.RU (Jan. 29, 2020), https://lenta.ru/news/2020/01/29/ntechlab/ (Russ.).

[99] *Id.*

[100] *Id.*

million US dollars), and Forbes[101] reported the company had said it would receive 3.2 million dollars in investments for its work.[102]

The government's trust in NtechLab's facial recognition software is evident in its decision to implement the algorithm in the city's infrastructure.[103] The founders of the Russian facial recognition software note that the "product made for Moscow's extensive CCTV system is capable of running simultaneously on hundreds of thousands of cameras,"[104] while NtechLab CEO Alexey Minin observes that "Moscow's new system is the largest live facial recognition project in the world."[105]

As to everyday life applications, the city's officials "touted" the advent of the facial recognition-based Face Pay[106] in Moscow's subway stations as a highly anticipated and progressive event.[107] A prominent proponent of this change is Maksim Liksutov,[108] the head of Moscow's Department of Transport, who announced this novel payment system to the capital's inhabitants by accentuating its many advantages, in a rather simplified manner, stating: "[t]o enter the metro, passengers won't need a card or a smartphone—just look at the camera on the turnstile."[109] There was no mention of possible transgressions or biometric data leaks as a result of technology's widespread implementation in Moscow's public transportation systems.

Consequently, urban projects expanding the utilization of facial recognition in Moscow are expected to continue proliferating, with industry leaders such as Aleksey Nekhaev, Director of VisionLabs, predicting that the

---

101 Thomas Brewster. *Remember FindFace? The Russian Facial Recognition Company Just Turned On A Massive, Multimillion-Dollar Moscow Surveillance System*, FORBES (Jan. 29, 2020), https://www.forbes.com/sites/thomasbrewster/2020/01/29/findface-rolls-out-huge-facial-recognition-surveillance-in-moscow-russia/?sh=5f573bc6463b.

102 Chris Burt, *Moscow Launches Live Facial Biometrics Surveillance Network NtechLab CEO Calls World's Largest*, BIOMETRIC UPDATE (Jan. 31, 2020), https://www.biometricupdate.com/202001/moscow-launches-live-facial-biometrics-surveillance-network-ntechlab-ceo-calls-worlds-largest.

103 Brewster, *supra* note 101.

104 Burt, *supra* note 102.

105 *Id.*

106 *Moscow Metro Introduces "World's First" Pay-by-Face System*, MOSCOW TIMES (Oct. 15, 2021), https://www.themoscowtimes.com/2021/10/15/moscow-metro-introduces-worlds-first-pay-by-face-system-a75300. Face Pay system started working at the turnstiles of a few Moscow subway stations in October 2021. *Id.* It allowed Moscovites to access subway services without having to pay with cash, card, or their cell phone: "To activate Face Pay, passengers [had] to connect their photo, bank card and transit card, known as 'Troika' card, to the service through the Moscow Metro's mobile app." *Id.*

107 *Id.*

108 *See Maxim Liksutov*, ROSCONGRESS FOUND., https://roscongress.org/en/speakers/liksutov-maksim/biography/ (last visited March 25, 2023) (The Deputy Mayor of Moscow who supervises the transportation unit).

109 MOSCOW TIMES, *supra* note 106.

Russian-based AI market has two key advantages over its international competitors: (1) low exchange rates of the local currency (as compared to that of international competitors); and (2) high quality math education in Russia.[110] According to Nekhaev, these advantages will lead to a swift growth in facial recognition development in Russia, and a rise in national and international investments in companies such as VisionLabs.[111]

Notably, Moscow officials, while increasingly relying on their administrative decisions regarding the collection of personal data, are also quick to stress in their communications with Moscovites that achieving security and safety—while guaranteeing citizens' rights and interests—is a priority for all state agencies dealing with advanced technologies.[112] Artem Ermolaev, Head of the DIT, stresses that the DIT's paramount goal "is a balance between confidentiality and safety, and [that department's administration] follow[s] a strict internal control system, which guarantees to account for citizens' rights."[113] Russian press highlights that Moscow's governing elites, including Mayor Sergey Sobyanin, increasingly depend on big data analysis during important decision-making meetings.[114] Sobyanin is often heard asking, "And what do[es] the data say?"[115]

It must be noted that, in context of the private sector's use of the technology, banks explain their ubiquitous uses of facial recognition as an attempt to improve: "personalized services, crime prevention, [and] dual authentication."[116] Kirill Koroteev and Damir Gainutdinov, attorneys from Agora, have stated on numerous occasions that the banking and financial sector's usage of facial recognition is well-regulated.[117] There are well-defined laws requiring customers' consent before photo or video recording takes place.[118] This is in contrast, however, to how facial recognition has

110 Andrey Ivanov, Iskusstvennyĭ intellect v Rossii. Dostizheniia i osnovnye napravleniia razvitiia [AI in Russia. Developments and Major Trajectories], IOT.RU (Aug. 5, 2016), https://iot.ru/gorodskaya-sreda/iskusstvennyy-intellekt-v-rossii-dostizheniya-i-osnovnye-napravleniya-razvitiya (Russ.).

111 *Id.*

112 Kamery s sistemoĭ raspoznavaniia lits nachali rabotat' v Moskve [Cameras with Facial Recognition have Started to Operate in Moscow], TASS.RU (Sept. 28, 2017), https://tass.ru/moskva/4601220?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (Russ.).

113 *Id.*

114 Andrey Zakharov, "Umnyĭ gorod" ili "Starshyĭ brat"? Kak meriia nauchilas' znat' o moskvichakh vsë ["Smart City" Or "Big Brother"? How Moscow City Government Has Learned How to Know Everything About Moscovites], BBC (Apr. 10, 2020), https://www.bbc.com/russian/features-52219260 ("During the official meetings incorporating discussions of problematic situations, Sobyanin started asking 'And what do[es] the data say?'") (Russ).

115 *Id.*

116 Ivanov, *supra* note 110 (Nekhaev describing LUNA, VisionLabs facial algorithm for banking and retail industries).

117 Gainutdinov & Koroteev, *supra* note 45.

118 Novaya Gazeta, *supra* note 54.

been used by Russian law enforcement.[119] OVD-Info attorneys argue that the implementation of existing personal data laws is politically-motivated, with the goal of terminating dissent against the current political regime, and to "dampen[] peaceful protests."[120]

The Moscow Smart City Report 2030 from the Moscow Mayor's Office contains many metaphors of progress, prestige, and security.[121] The city officials supporting rapid implementation of novel technologies—among them facial recognition—cite comfort and security as foundational goals in the smart Moscow city life of the near future.[122] Such positive descriptions of technology's features undoubtedly make it attractive to and desired by Moscovites. Yet Professor Sergeĭ Kamolov of Moscow State Institute of International Relations posits that new technologies do not "necessarily have an impact on the citizens' quality of life." Rather, he sees smart cities as "a deep marketing concept."[123]

Looking to the official Moscow city reports and the zealously optimistic websites of AI technology companies,[124] questions arise about whether it will be possible to live in Moscow in 2030 without the IoT, CCTV cameras, and constant surveillance, and if, without this technology, Moscow will fall behind global competitors such as Singapore, China, and the United States.[125] More importantly to the interests of individuals' privacy rights, the Russian government and the AI industry pay little attention in their official reports to the negative consequences of novel AI technologies—likewise failing to educate the public on the nature of such undesirable outcomes.[126] Official governmental reports do not elaborate on the possibilities of unwanted consequences in facial recognition uses, or how it might effect, and even diminish, individual privacy rights.[127] Moscow's government and Russian AI industry appear to work in tandem, paying little or no attention to the possible adverse side-effects of facial recognition technology in their

[119] *Id.*

[120] OVD-INFO REPORT, *supra* note 49.

[121] Moscow Smart City Report 2030, *supra* note 18.

[122] Celestine Bohlen, *In Moscow's Technological Advances, a "Double-Edged Sword,"* N.Y. TIMES (Nov. 16, 2021), https://www.nytimes.com/2021/11/16/world/europe/moscow-face-pay-technology-privacy.html.

[123] *Id.*

[124] NtechLab's is one of such websites. *See* NTECH LAB, *supra* note 65.

[125] Bohlen, *supra* note 122.

[126] The Russian press, when discussing issues surrounding facial recognition adaptation, often mentions viewpoints of city officials and those of AI industry leaders, which tend to be overly positive. *See Moscow Metro Introduces "World's First" Pay-by-Face System*, *supra* note 106. Such discussions also include negative features of this novel technology, which are voiced mostly by privacy advocates and human rights activists, such as attorneys from Agora and Roskomsvoboda. *See* Novaya Gazeta, *supra* note 54.

[127] *See* Moscow Smart City Report 2030, *supra* note 18.

official introduction of these technologies to the Russian public.[128] Both the public and private sectors in Russia consistently reassure civilians that "video analytics systems help society and businesses to respond to critical incidents in a timely and efficient manner," to quote NtechLab's CEO Andreĭ Telenkov.[129] Meanwhile, the suppression of the civil society has increased in Russia throughout President Putin's rule, which has lasted for over twenty years.[130] Some of the most recent developments evidencing such tendencies are: the dissolution of Memorial International, a well-respected human rights organization, by Russia's Supreme Court in April 2022;[131] an increase in censorship of media channels, the press, and citizens' communications;[132] as

[128] *Id.*

[129] *Ntechlab: AI-Powered Facial Recognition Technology For Safety and Security*, ENTER. SEC. MAG., https://biometric-europe.enterprisesecuritymag.com/vendors/ntechlab/2021 (last visited Aug. 17, 2022).

[130] *See* F. Joseph Dresen, *Vladimir Putin and the Rule of Law in Russia*, WILSON CENT. REP. (last accessed Mar. 30, 2023), https://www.wilsoncenter.org/publication/vladimir-putin-and-the-rule-law-russia. The author quotes Jeffrey D. Kahn, assistant professor of law, Southern Methodist University:

> Putin, with tremendous popular support, launched an immediate military campaign in Chechnya. Characterizing the war as a campaign on terrorism, Putin used the war to justify the centralization of executive power. . . . Putin's war substantially retarded the growth of a rule of law state. As the Russian military campaign in Chechnya continued, Kahn observed, "a certain callousness toward law spread north from the Caucasus as everything was covered in the sticky patina of fighting terrorism." Later Professor Kahn adds: "The [Russian] state destroys respect for the rule of law by using law as a political tool to oppress its opponents."

Id.

[131] Reshenie Plenuma Verkhovnogo Suda Rossiĭskoĭ Federatsii "O Likvidatsii Mezhdunarodnoĭ Obshchestvennoĭ Organizatsii 'Mezhdunarodnoe Istoriko-Prosvetitel'skoe, Blagotvoritel'noe i Pravozashchitnoe Obshchestvo 'Memorial'" ot 28 dekabria 2021 g., po delu N AKPI21-969 [Ruling of Supreme Court "On Closing of International Civic Organization 'International Historical and Educational, Charitable and Human-Rights Society 'Memorial'" Dec. 28, 2021 case N AKPI21-969], Juridico-Informational System LEGALACTS.RU (https://legalacts.ru/sud/reshenie-verkhovnogo-suda-rf-ot-28122021-po-delu-n-akpi21-969/) (Russ.). *See also* Verkhovnyĭ Sud Rossiĭskoĭ Federatsii: Kartochka Proizvodstva Delo No. AKPI21-969 ot 11 sentiabria 2021 do Zhaloba PAS22-112 ot 23 noiabria 2022 [Supreme Court of the Russian Federation: Production Card Case No. AKPI21-969 Dated Sep. 11, 2021 to Complaint PAS22-112 Dated Nov. 23, 2022], https://vsrf.ru/lk/practice/cases/11360276 (Russ.). *See also* FIDH, *Chronicle of a Death Foretold: the Liquidation of Legendary Human Rights Organizations in Russia*, No. 795a (Jul. 2022), https://www.fidh.org/IMG/pdf/fidh_chronicle_of_a_death_foretold_liquidation_of_memorials.pdf. (last visited Jun. 8, 2023).

[132] Aprel' 2020: rossiian vse chashche nakazyvaiut za kritiku gosudarstva [*April 2022: Russians are being punished more often for criticizing the government*], ROSKOMSVOBODA (May 2, 2022), https://roskomsvoboda.org/post/gigest-apr-2022-kritika-derzhavy/?fbclid=IwAR2KeY7xT7xhlgZJBC_FlsFrPh3ljgn8ro28fqDcgJCGtG32qGgsuo8oP28 (Russ.); *see also* F@CK THIS JOB (Mike Lerner &Vera Krichevskaia 2021) (About the closure of an independent TV channel *Dozhd'* (*The Rain*)). This documentary illuminates the circumstances of the media organization's complicated relationship with power institutions in Russia). *See also* Genprokuratura Rossii Vnesla v Roskomnadzor Trebovaniia o Priniatii Mer Po Ogranicheniiu Dostupa k Informatsionnym Resursam "Ekho Moskvy" i "Telekanal 'Dozhd'"" Prokuror N 01/2022, ot 1 marta 2022 [Prosecutor

well as Russia's ceasing to be a party to the European Convention on Human Rights on September 16, 2022.[133]

II. PERSONAL AND BIOMETRIC DATA COLLECTION TECHNIQUES IN MOSCOW, AND THE LIMITS THEY SET ON RUSSIAN CIVIL SOCIETY

The development and mass utilization of AI technologies have been progressing in contemporary Russia. Many important lessons about the intricate relationship between the Russian government and the advent of new technologies can be learned from AI's predecessor: the Internet. In 2012, Evgeniĭ Morozov, the author of the book "The Net Delusion: The Dark Side of Internet Freedom,"[134] argued that sooner or later the Internet would be used by authoritarian regimes as yet another instrument to suppress democratic aspirations within borders of authoritarian nations.[135] According to Morozov, not unlike Agre's "amplification model,"[136] the Internet has been political, likewise positing that "everything done with regard to Internet policy [would have] political consequences."[137] Further, Morozov argues that authoritarian governments have immensely benefited from the advent of the Internet.[138] In his work, Morozov highlighted three tendencies of Internet control under authoritarian rule: (1) dissemination of propaganda; (2) new ways of censorship; and (3) increased surveillance, or, what Morozov referred to as "more sophisticated surveillance."[139]

This overview of then-novel communications technology foreshadowed what Russian civil society activists—among them OVD-Info and Roskomsvoboda attorneys—would observe later with how facial recognition technologies are used to suppress political opposition in the

General's Office Has Demanded Roskomnadzor to Limit Access to Informational Resources "Echo of Moscow" and "TV Channel Dozhd'" Mar. 1, 2022, Prosecutor N 01/2022, LAWINFO.RU, https://lawinfo.ru/articles/1055/genprokuratura-rossii-vnesla-v-roskomnadzor-trebovaniya-o-prinyatii-mer-po-ograniceniyu-dostupa-k-informacionnym-resursam-exo-moskvy-i-telekanal-dozd (Russ.).

133 *Russia Ceases to be a Party to the European Convention on Human Rights on September 16 2022,* COUNCIL EUR. (Mar. 23, 2022), https://www.coe.int/en/web/portal/-/russia-ceases-to-be-a-party-to-the-european-convention-of-human-rights-on-16-september-2022. *See also* Postanovlenie Pravitel'stva Rossiĭskoĭ Federatisii "O Prekrashchenii Uchastiia Rossiĭskoĭ Federatsii v Chastichnykh i Rasshirennykh Chastichnykh Soglasheniiakh Soveta Evropy" ot 28 iiunia 2022 g., N 1155 [Ruling by the Government of Russian Federation "On Termination of Participation of Russian Federation in Partial and Extended Partial Agreements of the Council of Europe" of Jun. 28, 2022, N 1155], http://publication.pravo.gov.ru/Document/View/0001202207010042?index=0&rangeSize=1, (Russ.).

134 EVGENIĬ MOROZOV, THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM (Public Affairs 2012).

135 RADIO FREE EUR./RADIO LIBERTY, *supra* note 25.

136 Agre, *supra* note 28.

137 RADIO FREE EUR./RADIO LIBERTY, *supra* note 25.

138 *Id.*

139 *Id.*

country, starting around 2015.[140] Russia's unbridled Internet freedom was short-lived. By the end of the 1990s, the Russian government began to utilize Soviet era surveillance technology within the nation's digital domain, known as the System of Operative-Search Measures ("SORM").[141] Concurrently, starting in the early 2000s, the Russian government "began to implement a series of laws that *de facto* criminalize criticism of the government, legalize unfettered surveillance of citizens' online activities, and increase state control of the Russian internet or Runet."[142] In addition, President Putin signed "Zakon o 'suverennom runete'" ("'Sovereign Internet' Law")[143] in May 2019, allowing the government's media regulator, Rozkomnadzor, to control the Russian Internet if the country were to be unexpectedly cut off from the global web.[144]

Notably, compared to China—where surveillance technology filters information before it reaches citizens—the Russian government depends on "a repressive legal regime coupled with tightening information control and intimidation of internet service providers (ISPs), telecom providers, private companies, and civil society groups."[145] Further, the so-called Yarovaya amendments, which came into existence in 2016, started requiring telecom providers, social media platforms, and messaging services to "store user data for three years and allow the FSB (Federal Security Service) access to users' metadata and encrypted communications."[146] Subsequently, the Russian government upgraded its surveillance efforts with more sophisticated, real time CCTV cameras; implementing a more advanced video surveillance

[140] *See* Human Rights Law Network, *supra* note 2.

[141] *See* Alina Polyakova & Chris Meserole, *Exporting Digital Authoritarianism: The Russian and Chinese Models*, BROOKINGS INST. 8, https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf (last visited Aug. 15, 2022). SORM works by duplicating all data flows on internet and telecom networks. *Id.* It sends one copy to the government and the other to the originally intended recipient. SORM is the FSB's "backdoor to Russia's internet." *Id.*

[142] *Id*. at 6.

[143] *See* RADIO FREE EUR./RADIO LIBERTY, *Putin Signs 'Sovereign Internet' Law, Expanding Government Control of Internet* (May 1, 2019), https://www.rferl.org/a/putin-signs-sovereign-internet-law-expanding-government-control-of-internet/29915008.html; *see* Federal'nyĭ Zakon RF o Vnesenii Izmeneniĭ v Federal'nyĭ Zakon o Sviazi i Federal'nyĭ Zakon ob Informatsii, Informatsionnykh Tekhnologiiah i o Zashchite Informatsii [Federal Law of the Russian Federation on Introducing Changes to the Federal Law on Connectivity and to Federal Law on Information, Information Technologies, and on Protection of Information] 2019, No. 90-FZ, http://publication.pravo.gov.ru/Document/View/0001201905010025 (Russ.). *See* V Rossii vstupil v silu zakon o "suverennom runete". No rabotat' on poka ne budet [The law on "sovereign Runet" came into force in Russia. But it won't work yet], BBC (Nov. 1, 2019) https://www.bbc.com/russian/news-50259217 (Russ.).

[144] Polyakova & Meserole, *supra* note 141, at 6.

[145] *Id.* at 7.

[146] *Id.* at 9.

system, known as "Safe City," in 2015. The technology behind "Safe City" allowed:

> [T]he automatic transfer of information, including facial/moving objects recognition, to government authorities. This information [became] available to any executive or presidential body. The budget for "Safe City" implementation from 2012 to 2019 was an estimated $2.8 billion to cover all cities hosting the 2018 World Cup. The city of Moscow ha[d installed] approximately 170,000 cameras [for the occasion], at least 105,000 of which ha[d] been outfitted with facial recognition technology developed by . . . NtechLab.147

Such Internet and video surveillance governance decisions are good examples of how the Russian government has and continues to take decisive steps in administrative and law-making processes surrounding the adaptation of novel digital technologies—that of the Internet, and later, of AI technologies, including facial recognition. Unsurprisingly, the Russian government remains directly involved in the financial backing of AI facial recognition's development, as in the case of NtechLab's funding discussed earlier.[148] Likewise, the government has also passed laws making the communications of Internet users more easily identifiable;[149] a clear attempt to thwart signs of political dissent at its root. And much like Morozov's argument that authoritarian regimes tend to control new technology—such as the Internet—the adaptation of facial recognition technology appears to be following in similar footsteps.[150] One of the peculiarities of this new technology—having been created under the auspices of the government—is that it so far has not had the chance to play a role in a free exchange of ideas—as initially was the case with the Internet.

Of the three tendencies of Internet control under authoritarian regimes that Morozov identifies, at least two can be applied to the case of facial recognition technology utilization in Russia. The facial recognition software has been utilized as yet another, more sophisticated, way to censor the Russian citizenry and civil society; serving as an additional, more sophisticated, means of surveillance.[151] Similarly, if we recall Agre's "amplification model,"[152] any new technology may be chronologically novel, but its adaptation will most definitely be molded by the social forces that had

147 *Id.* at 8.

148 BANCAM.RU, *supra* note 95.

149 Polyakova & Meserole, *supra* note 141, at 8 (As in the case of Yarovaya amendments).

150 RADIO FREE EUR./RADIO LIBERTY, *supra* note 25; *see also* Human Rights Law Network, *supra* note 2 (Gainutdinov's talk on nuances of facial recognition adaptation and the Internet shutdowns in Russia).

151 *See* RADIO FREE EUR./RADIO LIBERTY, *supra* note 25 (The transcription of Morozov's interview in which he offers three tendencies of authoritarian regimes in adapting such novel at the time technology as the Internet).

152 *See* Agre, *supra* note 28.

preceded it. For instance, regarding the interrelationship between the Internet and political processes, Agre states:

> [T]he Internet creates little that is qualitatively new; instead, for the most part, it amplifies existing forces (Agre, 1998a). Social forces are nothing but coordinated human will, and institutions channel human will in some directions more than others. To the extent that institutional actors can pursue existing goals by reinterpreting existing action patterns in terms of a newly available technology, the forces that their massed actions create will be amplified.[153]

Despite AI industry leaders' and governmental officials' overly positive portrayal of facial recognition technology as technology that will make life more safe, more secure, and more comfortable, this technology exhibits at least one constant flaw if compared with its less advanced predecessors: it has been created and regulated by human institutions. When applying Agre's formula, it becomes evident that the "existing goals" of Russian political elites, or "institutions" and "institutional actors" have been "channeled" in the "direction" of increasing state control over political behavior of the citizenry, and over its collective will.[154] The adaptation of the technology is not as simple and optimistic as the agents regulating it would like the citizenry to believe. True, there is a multitude of beneficial uses of any novel technology, but there are also negative consequences that must be heeded to be avoided, and so that many possible abuses by those actors who regulate and use it do not become customary.

Just as easily as one's words and political beliefs had been de-anonymized during the advent of the Internet in the late 1980s,[155] Russia, among other nations, is stepping into a new world where every citizen's face can too be easily identified and de-anonymized. Further, since about 2015, the ubiquitous deanonymization of one's faceprint[156] has started to complement one's digital, Internet-based, trace in Moscow.[157] This phenomenon of instant de-anonymization with the help of computer recognition of one's face, gait, or voice recording, is what is being "amplified" under Agre's theory and utilized by high tech industrial actors and State governments.

---

153 *Id*.

154 *Id.*

155 William Craig, *The History of the Internet in a Nutshell*, WEBFX (Aug. 12, 2022), https://www.webfx.com/blog/web-design/the-history-of-the-internet-in-a-nutshell/.

156 *See* Adam Schwartz, Nathan Sheard, & Bennett Cyphers, *Face Recognition Technology: Commonly Used Terms*, ELEC. FRONTIER FOUND. (Oct. 7, 2021) https://www.eff.org/deeplinks/2021/10/face-recognition-technology-commonly-n. Faceprint is defined as "[a] fundamental step in the process of face recognition. [It] is the automated analysis and translation of visible characteristics of a face into a unique mathematical representation of that face. Both collection and storage of this information raise privacy and safety concerns." *Id.*

157 Novaya Gazeta, *supra* note 54.

Damir Gainutdinov, an attorney at Agora, stated that this technology was utilized by the government—and particularly by law enforcement—prior to the 2018 FIFA World Cup, which was previously claimed to be the official implementation of the mass installation of CCTV cameras in Russia.[158] In their report, Gainutdinov and Koroteev point to administrative cases that began appearing in Moscow's courts in which government plaintiffs (for instance, during court proceedings connected to mass protests) use video-recordings as their evidence to prove that a certain person had, in fact, participated in a certain demonstration.[159] Moscow's city website states explicitly that "[t]he video from [CCTV cameras can] be uploaded to the General Centre for Data Storage and Processing ("GCDSP"), and the recordings can be used as evidence in court."[160] Also, specifically to cameras equipped with facial recognition, the Mayor's Office reported that "already in September [2017], more than three thousand city surveillance cameras were connected to the facial recognition system."[161]

Even though video recordings were utilized to identify protest participants in 2021,[162] notably, police usage of facial recognition technology for detaining protesters was not evident. The OVD-Info attorneys have deduced technology's uses from "the large scale [*post factum*] detentions," involving prosecution of non-public figures, and from statements the police made to detainees[163] while arresting them, or in former's reports.[164] Moreover, even though the Russian press began discussing novel facial recognition technology after January 2021 protests, the official documents rarely mentioned it.[165] The OVD-Info experts concluded that "[t]he paucity of direct evidence of the use of facial recognition technology in police reports, case files and court rulings may indicate that the police and courts prefer not to officially document this information."[166]

Gainutdinov further finds uses of the facial recognition by the law enforcement worrisome as there are no laws that efficiently address and regulate these technologies. He describes the Russian government's data collection strategies in his 2021 YouTube talk on facial recognition, Russia's Internet-based censorship, and surveillance in general:

---

158 *See* Human Rights Law Network, *supra* note 2.

159 OVD-Info attorneys, whose work will be discussed in Part III assist defendants in such cases. A singular case, exemplary of many others, is discussed at the start of OVD-Info's Report. *See* OVD-INFO REPORT, *supra* note 49.

160 *See* MOSCOW CITY, https://www.mos.ru/ (last visited: March 25, 2023).

161 *See* OVD-INFO REPORT, *supra* note 49.

162 *Id.*

163 *Id.*

164 *Id.*

165 *Id.*

166 *Id.*

> The Russian legislation didn't regulate the use of FR at all. We are now only preparing laws for this. They've been using [CCTV cameras] for years, but they had no laws to regulate the technology. . . . The technology wasn't politically neutral, and was definitely used for political opponents. They collected DNA samples, finger[prints]. FR use is proved by thousands of case files. Now we are only at the beginning.[167]

The Russian government claims that its position is noble, asserting that:

> [All the data collected is] to be used to protect the protestors, and to . . . find criminals not connected to protests. And [government] published papers about catching these criminals. [We] suspect that this program collects data from all social accounts. The [protest] participants were questioned weeks after the protest. They were identified by city cameras and police ones. 360 degree recordings. Now we see mass evidence of these recordings because they are used in court proceedings.168

At the same time, the Russian public remains largely uninformed due to the lack of transparency from municipal agencies that install and regulate uses of CCTV cameras in urban centers. This is an especially grave concern if an individual, who might have been a mere passerby, gets detained by the police.[169] For example, Dmitrii Serebrennikov presented in the Helsinki University conference his study of CCTV cameras' uses (from 2018 to 2020) for urban security purposes in seven municipalities in the St. Petersburg region. According to Serebrennikov's qualitative interviews and participant observation-based project,[170] CCTV cameras are mostly installed by local emergency services, such as police and firefighter departments, as well as by various utilities agencies.[171] These agencies are the ones who decide locally how to "position the cameras" within a given urban landscape.[172] Importantly, Serebrennikov could not locate any data on law enforcement uses of these cameras.[173] In highlighting his study methodology,

---

167 Human Rights Law Network, *supra* note 2.

168 *Id.*

169 *See* OVD-INFO REPORT, *supra* note 49 ("A particular problem is that a person whose biometric data is illegally processed using a facial recognition system may not find out about the violation, since the fact of using the technology is not disclosed in the case file. Consequently, it will be difficult to appeal it.").

170 Serebrennikov conducted twenty interviews with twenty-two informants from three cities in St. Petersburg region, and twelve interviews with thirteen informants from three other regions for validation purposes. He also analyzed the municipal CCTV location decision making process through governmental purchase contracts, local legislative and regulatory documents, and participant observation in monitoring centers. Dmitrii Serebrennikov, *Parallel Session III.2 - Security and Public Control*, UNITTUBE (October, 19, 2021) https://www.helsinki.fi/fi/unitube/video/990d827e-2f39-471a-99cd-2e101c985a3f.

171 *Program and Schedule EET (Helsinki) Time Zone*, UNIV. HELSINKI, https://www2.helsinki.fi/en/conferences/development-of-russian-law-xiii/program-and-schedule-eet-helsinki-time-zone (last updated Nov. 1, 2021); Serebrennikov, *supra* note 170.

172 Serebrennikov, *supra* note 170.

173 *Id.*

Serebrennikov noted that "in terms of practice, [he] only analyzed online monitoring in real time by municipal monitoring center operators."[174]

According to OVD-Info civil society advocates, facial recognition plays an integral role in an increased suppression of freedom of assembly throughout Moscow and Russia as a whole.[175] About 213,000 CCTV cameras for 12.6 million people were present in Moscow in 2021.[176] The CCTV cameras are installed on the streets and other public spaces as well as at the entryways to apartment buildings.[177] Almost 4.5 million such cameras operate in schools ("Orwell" facial recognition system), kindergartens, hospitals, and government institutions.[178] The largest investment, approximately $19 million, was spent on Moscow Metro.[179] Information from these CCTV cameras is transmitted to the GCDSP, and from there it can be requested by the city's departments, including the Ministry of Internal Affairs. The DIT has emphasized on numerous occasions that "reports of illegal access to the system were rare and sent for investigation." [180]

Yet, it is already possible to buy the CCTV information about a person's whereabouts within Moscow on the black market, for a nominal price. In fact, such violations of Moscovites' privacy rights have already taken place due to the capital's CCTV cameras being poorly protected, as they can potentially be accessed by virtually any person, including "[a]ny crazy guy can stalk you using this technology]; criminals can check when and where you go and steal from your apartment or hurt you."[181] But this data is also in rare instances legally reclaimable, as exemplified by the case of Anna Kuznetsova and her lawyer Yekaterina Abashina of Roskomsvoboda,[182] who were able to sue the city and purchase her personal

---

174 *Id.*

175 OVD-INFO REPORT, *supra* note 49.

176 Paul Bischoff, *Surveillance Camera Statistics: Which Cities Have the Most CCTV Cameras?*, COMPARITECH (July 11, 2022), https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/.

177 Kristyna Foltynova, *We See You! How Russia Has Expanded Its Video-Surveillance System*, RADIO FREE EUR./RADIO LIBERTY (Jan. 19, 2021), https://www.rferl.org/a/russia-video-surveillance/31052482.html.

178 *Id.*

179 *Id.*

180 Umberto Bacchi, *Face for Sale: Leaks and Lawsuits Blight Russia Facial Recognition*, REUTERS (Nov. 9, 2020), https://www.reuters.com/article/us-russia-privacy-lawsuit-feature-trfn/face-for-sale-leaks-and-lawsuits-blight-russia-facial-recognition-idUSKBN27P10U.

181 *Id.*

182 *Id. See also* Reshenie Tverskogo Raĭonnogo Suda Rossiĭskoĭ Federatsii "O Priznanii Nezakonnymi Deĭstviĭ po Primeneniiu Tekhnologii Raspoznavaniia Lits, Obiazanii Vozderzhat'sia ot Primeneniĭ Tekhnologii Raspoznavaniia Lits, Udalit' Personal'nye Dannye iz Bazy Dannykh, Priniat' Akt o Poriadke Ispol'zovaniia Tekhnologii, Vzyskanii Kompensatsii Moral'nogo Vreda" ot 4 dekabria 2020, No. 2a-798/2020 [Decision of Tverskoy District Court of Russian Federation "On Finding Actions Involving Uses of Facial Recognition To Be Unlawful, On Duty to Limit Uses of Facial Recognition and

data—specifically, highly detailed information about her movements within the capital over the span of a few days—for a nominal sum of 16,000 rubles ($254.00 USD).[183]

Gainutdinov highlights that there are three operational levels of video-surveillance in Moscow: first, cameras at the entrance doors of residential buildings that can recognize faces and whether passersby live in a building in question; second, cameras installed on municipal buildings, such as schools and government offices (as a rule, there are four cameras on each corner of the building); and, third, high-resolution cameras in public spaces, which the government claims can recognize hundreds of faces at any moment in time.[184] The government started to use this video-surveillance even before the 2018 FIFA World Cup, during rallies and political protest demonstrations. The rallies were "surrounded by [] fence[s] . . . with twenty metal detectors you had to pass to join the rally."[185] The Russian government described the growing omnipresence of CCTV cameras as a tool of noble pursuit. Gainutdinov stated that according to the officials:

> [T]he data are used to provide the safety and security of the participants, as well as to detect wanted persons . . . on criminal charges, not connected to [a specific] protest. As to me, it seems they launched some kind of PR project. . . . Now we see the mass evidence of using these technologies in the case files of the protestors in courts. [186]

A. Facial Recognition and the Lack of Adequate Law-Making and Impartial Oversight

In their Net Freedoms Report, "Facial Recognition: The Foreboding of Dystopia," summarizing conditions under which facial recognition has been adapted in Russia, attorneys Damir Gainutdinov and Kirill Koroteev note that:

> Facial recognition in Russia can be subdivided into three main stages: preparation (from 2001 to 2015, when cameras were installed and first programming complexes emerged), testing (from 2016 to 2018, when technology started being actively utilized in city's programs targeting safety and readiness for international sports competition), and mass

to Delete Personal Data From the Database, to Pass an Act Regulating Uses of the Technology, and Establishing Compensation For Moral Injury" of Dec. 4, 2020, No. 2a-798/2020], https://www.mos-gorsud.ru/rs/tverskoj/services/cases/kas/details/151b3db1-0400-11eb-a7b5-d914ac4c1d0c#tabs-3 (Russ.).

183 Bacchi, *supra* note 180.

184 Human Rights Law Network, *supra* note 2.

185 *Id.*

186 *Id.*

> implementation (from 2019 till present, as continuation of unification of protocol and integration of various networks into a single unified space).[187]

The very first CCTV cameras entered the daily lives of Moscovites' almost unnoticed, as far back as in 2001.[188] These cameras were installed at the entrances of residential buildings (approximately 80,000 cameras) and in public spaces (120,000 cameras).[189] These were the very first, low-tech, black and white cameras. They could not yet identify faces and they were not connected to a centralized system (as CCTV cameras are now).[190] Instead, data collected from those cameras would be transferred to 125 local monitoring centers.[191] This surveillance system was modernized in 2007 for the first time under the guise of the "Safe City" project.[192] In 2014, the "Safe City" project was officially established throughout Russia in the Komi Republic, Astrakhan, Sverdlov, and Tomsk regions, as well as in St. Petersburg.[193]

On February 18, 2016, the then-unknown company NtechLab, founded by Moscow University graduate, Artem Kukharenko, released the application FindFace, which would later use the photos posted by about forty-six million of *VKontakte* users to develop their facial recognition neuro-network.[194] Consequently, NtechLab started working with the DIT, and about 3,000 new cameras with NtechLab's facial recognition algorithm were promptly installed in Moscow.[195] Soon, the company closed FindFace to the Russian public and started working with the government and private sectors exclusively.[196] NtechLab claimed that its algorithm is one of the best facial recognition algorithms in the world, with a ninety-nine percent rate of accuracy, scanning 1.5 billion facial images in less than one second.[197] In March 2020, the video surveillance system that had been used during the 2018 World Cup was utilized to monitor the spread of COVID among Moscovites and their contacts.[198] By this time, the "Safe City" video-surveillance network spread into forty regions of the country, including:

187 Gainutdinov & Koroteev, *supra* note 45.

188 *Id.*

189 *Id.*

190 *Id.*

191 *Id.*

192 *Id.*

193 *Id.*

194 *Id.*

195 *Id.*

196 *Id.*

197 *Id.*

198 *Id.*

Moscow, St. Petersburg, Ryazan', Saratov, Nizhegorodsk, Cheliabinsk, Tiumen', Kemerov, Kamchatka, and Primorskiĭ Kraĭ.[199]

The use of facial recognition in Russia gained the attention of the international legal community when in July 2020, Vladimir Milov, opposition politician representing the Solidarnost' or "Solidarity" party, and activist Alena Popova, filed a lawsuit in the European Court of Human Rights ("ECHR") against the Russian government.[200] The attorney for the petitioners, Agora's Kirill Koroteev, stated in their lawsuit that the petitioners would challenge the Russian government for violating several articles of the Convention on Human Rights: Article 8 (right to respect private life); Article 11 (freedom of assembly and association); Article 14 (protection from discrimination); and Article 15 (derogation in time of emergency).[201] Koroteev noted in his interviews that this was the first case challenging uses of "facial recognition technology during protests" brought to the ECHR.[202] Specifically, Popova and Milov referred to the mass use of facial recognition surveillance during a rally in Moscow on September 29, 2019.[203] According to the petitioners, this was "the first case of the Moscow authorities using facial recognition technology to gather data about protestors."[204]

Initially, Popova filed an independent lawsuit, asking the court to find the actions of the Russian government—namely, using a facial recognition system on the streets of Moscow in the City Video Surveillance System[205]—to be unlawful.[206] Popova further asked for the deletion of all her stored personal data that was previously collected.[207] In fall 2019, the Moscow Savyolovsky District Court "had already tried that lawsuit, but the

---

[199] *Id.*

[200] *Activists Asking ECHR to Find Use of Facial Identification System in Moscow Unlawful,* INTERFAX (July 6, 2020), https://interfax.com/newsroom/top-stories/69211/.

[201] *Id.*

[202] Anastasiia Kruope, *Moscow's Use of Facial Recognition Technology Challenged*, HUM. RTS. WATCH (Jul. 8, 2020), https://www.hrw.org/news/2020/07/08/moscows-use-facial-recognition-technology-challenged.

[203] *Id.* At least 20,000 people "took part in an authorized rally in Moscow in solidarity with those arrested and charged for their participation in peaceful protests." *Id.*

[204] *Id.*

[205] NETRIS, *Moscow Video Surveillance System* (last visited March 25, 2023), https://www.netris.ru/en/projects/moscow/. (City Video Surveillance System is a Single Moscow CCTV system that consolidates all city cameras. "The system video core is based on Netris high-efficiency video servers. Most cameras are connected by the operators in accordance with the service model. Simultaneous integration of analytical algorithms of different developers has been performed. All city lobby cameras are connected to face recognition analytical system.").

[206] *Id.*; *see also Activists Asking ECHR to Find Use of Facial Identification System in Moscow Unlawful, supra* note 200.

[207] *Russia: Intrusive facial recognition technology must not be used to crackdown on protests*, AMNESTY INT'L (Jan. 31, 2020), https://www.amnesty.org/en/latest/news/2020/01/russia-intrusive-facial-recognition-technology-must-not-be-used-to-crackdown-on-protests/.

defendant was then only activist Popova. On November 6, [2019] the court declined Popova's claim. The decision was later upheld by the Moscow City Court."[208] On March 3, 2020, the Moscow Tverskoy District Court dismissed the case.[209] Those administrative defendants were the Russian Interior Ministry's Directorate for Moscow and the Moscow DIT.[210] On June 18, 2020, the Moscow City Court "ordered a retrial of the claim filed by . . . Popova against the authorities and the police on the illegality of the use of facial identification technology in Moscow."[211]

The *Popova* case can be viewed as an example of the kinds of legal challenges, involving facial recognition technology and individuals' privacy rights, that Russian society faces. The study of cases similar to the *Popova* case also reveals more subtle political and social undercurrents taking place

[208] *Id.*; *see also Activists Asking ECHR to Find Use of Facial Identification System in Moscow Unlawful*, *supra* note 200. *See also* Reshenie Saviolovskogo Raĭonnogo Suda Rossiĭskoĭ Federatsii "O Priznanii Nezakonnymi Deĭstviia, Obiazanii ne Primeniat' Tekhnologii Raspoznavaniia Lits na Territorii . . . Udalit' Biometricheskie Personal'nye Dannye iz Bazy Dannykh Izobrazheniĭ Grazhdanina, Opredostavit' Dokazatel'stva" ot 6 noiabria 2019 g., No. 2a-577/19 [Decision of Savyolovsky District Court of Russian Federation "On Invalidating Acts, Duty Not To Use Facial Recognition on the Territory of . . . to Delete Biometric Personal Data From the Database of Citizen's Images, to Provide Evidence" Nov. 6, 2019, No. 2a-577/19, https://www.mos-gorsud.ru/rs/savyolovskij/services/cases/kas/details/988f386e-be51-47b0-b48f-e871043ef1fc#tabs-3 (Russ.). To learn more about Popova's appeal, *see also* Apelliatsionnoe Opredelenie Sudebnoĭ Kollegii po Administrativnym Delam Moskovskogo Gosudarstvennogo Gorodskogo Suda po Apelliatsionnoĭ Zhalobe Popovoĭ A.V. na Reshenie Saviolovskogo Raĭonnogo Suda g. Moskvy ot 6 noiabria 2019 goda" ot 30 ianvaria 2020 g., N 33a-707/2020 [Appeals Ruling of Judiciary Collegium Regarding Administrative Cases of Moscow City Court as to Appellate Complaint of Popova A. V. Following the Decision of Savyolovsky District Court of City of Moscow Dated Nov. 6, 2019" Dated Jan. 30, 2020, No. 33a-707/2020], https://www.mos-gorsud.ru/mgs/services/cases/appeal-admin/details/6c9dfe4c-ecc7-4626-90f4-dea208d54b5f#tabs-3 (Russ.).

[209] *Activists Asking ECHR to Find Use of Facial Identification System in Moscow Unlawful*, *supra* note 200. *See also* Opredelenie Tverskogo Raĭonnogo Suda g. Moskvy "Po Administrativnomu Iskovomu Zaiavleniiu Popovoĭ A.V., Milova V.S. k Departmentu Informatsionnykh Tekhnologiĭ g. Moskvy, GU MVD Rossii po g. Moskve O Priznanii Nezakonnymi Deĭstviĭ Po Sboru i Obrabotke Personal'nykh Dannykh, Primeneniia Tekhnologiĭ (Algoritma) Raspoznavaniia Lits Pri Poseshchenii Publichnogo Meropriiatiia; Po Neudaleniiu Personal'nykh Dannykh i Inoĭ Informatsii, Poluchennoĭ Vo Vremia Provedeniia Publichnogo Meropriiatiia, Iz Baz Dannykh; Obyazanii Udalit' Liubye Personal'nye Dannye i Inuiu Informatsiiu, Poluchennuiu Vo Vremia Provedeniia Publichnogo Meropriiatiia, Iz Bazy Dannykh" ot 3 marta 2020 g. [Ruling of Tverskoy District Court of City of Moscow "On Administrative Claim by Popova A.V., Milov V. S. Addressing Department of Information Technologies of City of Moscow, GU MVD of Russia in City of Moscow, On Finding Actions Involving Collection and Processing of Personal Data and Usages of Technologies (Algorithm) of Facial Recognition During Attendance of a Public Event To Be Unlawful; On Refusing to Delete Personal Data and Other Information Obtained During a Public Event From Database; On Duty to Delete Any Personal Data and Other Information Obtained During a Public Event From Database" Dated Mar. 3, 2020], https://www.mos-gorsud.ru/mgs/services/cases/appeal-admin/details/19d4a1a6-531e-494a-938b-b14837eeadd8#tabs-3 (Russ.).

[210] *Activists Asking ECHR to Find Use of Facial Identification System in Moscow Unlawful*, *supra* note 200.

[211] *Id.*

in Russia's capital and the country at large. In Russia, the government, assisted by such latest technologies as facial recognition, is demanding increasingly less anonymity from the citizens, while its actions are becoming more secretive and drastic *vis-a-vis* civil society and the public at large.[212] Growing in numbers and becoming technologically more sophisticated, surveillance tools are coupled with legal processes that are mostly supportive of government's actions, but questionable when compared to European standards.[213] This is why Russian activists, among them Popova and Milov, chose to bring their lawsuits to the ECHR.[214]

There are certain pervasive principles that have been emerging consistently throughout the adaptation of novel technologies, including that of facial recognition, in Russia: "the [faulty] proportionality and lack of legal framework,"[215] as well as no impartial official agency whose main task would be to oversee the usages of such technologies by the law enforcement or other governmental agencies.[216] The Ministry of Interior can perform a search of the database, having "specific branches" collect personal data from profiles of "hooligans, human rights activists, . . . anarchists, extremists, etc."[217] Oftentimes, the activities of civil society organizations, such as ones founded by political opposition leader Aleksei Navalny, are labeled as "extremist" which means the government equates their acts with "serious crime[s], placing tens of thousands of Navalny's supporters at risk of prosecution."[218] Privacy rights advocates from Agora, Amnesty International, and Roskomsvoboda have stated on numerous occasions that the use of CCTV cameras might have started as an innocent experiment, but it has progressed into what it has become in more recent years: i.e., an instrument helping the government eradicate political opposition.[219] Russian legal experts have also

---

[212] Many Russian civil society attorneys, such as those of Agora and OVD-Info, point to this tendency in their talks and reports. *See* Human Rights Law Network*, supra* note 2; *see also* OVD-INFO REPORT, *supra* note 49.

[213] *See* OVD-INFO REPORT, *supra* note 49. The Summary section of OVD-Info Report, "How the Russian state uses cameras against protesters," describes numerous detentions of peaceful assembly participants, and stressing that although "police officers often inform detainees that they were 'found through the cameras', the use of facial recognition technology is not mentioned in official documents—case files and court rulings." *Id*.

[214] As an example, Popova and Milov brought their lawsuit to the ECHR, once they had exhausted all the venues offered to them by the Russian court system, where their claims had been constantly denied and dismissed, as seen from the earlier discussion. *See also* OVD-INFO REPORT, *supra* note 49.

[215] OVD-INFO REPORT, *supra* note 49.

[216] Novaya Gazeta, *supra* note 54 (Darbinian's comments).

[217] *Id.*; *see also* Human Rights Law Network, *supra* note 2.

[218] *Russia: Aleksei Navalny's NGOs banned as "extremist", depriving thousands of their rights*, AMNESTY INT'L (Jun. 10, 2021), https://www.amnesty.org/en/latest/press-release/2021/06/russia-aleksei-navalnys-ngos-banned-as-extremist-depriving-thousands-of-their-rights/.

[219] *Id.*; *see also* Human Rights Law Network *supra* note 2. *See also* Roskomsvoboda's petition in their "Campaign against facial recognition", in which they write: "Facial recognition system is justified

commented that the use of these technologies dampens citizens' will to voice their opinions freely, in their rightful peaceful protests.[220] As such, the official uses of these technologies are creating a political and cultural reality, where, eventually, there will be no place for a free forum of public opinion. The authors of OVD-Info Report note that "the collection of data on the participants of the protests by the state creates the risk of politically motivated prosecution."[221]

Importantly, although the installation of facial recognition cameras can be traced as far back as 2001, the Russian legislature is not in a hurry to develop laws that would efficiently regulate biometric and personal data collection and storage, or protect individuals from personal and biometric data-related abuses, as was evidenced in Kuznetsova's case discussed earlier.[222] Darbinian of Roskomsvoboda stressed that there are no legal protections against hacking or undesirable uses of [personal] data. There is no understanding of "who, for what reason and at which moment can become a subject [of surveillance] with the help of facial recognition."[223]

Moreover, an increasing number of new laws are being implemented that make the actions of government bodies regarding these technologies increasingly clandestine, while there remains a lack of oversight by impartial non-governmental parties.[224] Additionally, the judiciary's definitions of what qualifies as "personal data," and "biometric data"—and how law enforcement has the ability to surveil whomever they please with the help of facial recognition technologies—ultimately produced a disturbing precedent that has been critiqued by civil society advocates.[225] These advocates are left

by the legitimate goals like searching for missing children and combating crime, including terrorism. But experience suggests that the system is already being used for illegal control of people much more actively than for a real fight against crime." BANCAM.RU, https://bancam.ru/en#:~:text=It%20can%20make%20power%20all,identifying%2C%20we%20change%20our%20behavior.

220 *Russia: Aleksei Navalny's NGOs banned as "extremist", depriving thousands of their rights*, *supra* note 218; *see also* Human Rights Law Network, *supra* note 2.

221 OVD-INFO REPORT, *supra* note 49.

222 Mariia Starikova, Portret uchastnika v iunosti: pravozashchitniki izuchili opyt politsii po raspoznavaniiu lits mitinguiushchikh [The Portrait of a Participant in Youth: Rule of Law Community Leaders Studied Police Experience of Facial Recognition Uses Against Those Who Protest], KOMMERSANT (Jan. 17, 2022), https://www.kommersant.ru/doc/5171027.

223 *Id.*

224 Novaya Gazeta, *supra* note 54.

225 Irina A. Shashkova, Konstitutsionnye osnovaniia zashchity prava na neprekosnovennost' chastnoĭ zhizni v protsesse ispol'zovaniia tekhnologii raspoznavaniia lits [Constitutional Basis for Protecting Privacy Rights in Light of Facial Recognition Technology Uses], Materials From XVIII International Conference for Young Scholars and Students in Ekaterinburg, at 251 (2020), http://www.spsl.nsc.ru/FullText/konfe/%D0%AD%D0%B2%D0%BE%D0%BB%D0%A0%D0%BE%D1%81%D0%9F%D1%802020.pdf#page=251 (Russ.). Shahshkova quotes Darbinian of Roskomsvoboda who stresses that "we see that whoever has access to this [facial recognition] system can use [it] as they please, violating privacy rights . . . without citizens' consent."

with no other option but to look for justice outside Russia. For instance, after Popova had failed to obtain a fair treatment of her lawsuit in domestic courts, she was joined by Milov, and the activists sought judgments from the ECHR to protect their right to private life, freedom of assembly and association, as well as protection from discrimination.[226] However, theirs and similar undertakings will no longer be as influential because Russia ceased to be a party to the European Convention on Human Rights, the treaty interpreted by the ECHR, on September 16, 2022.[227] Thereafter, the State Duma[228] introduced a new law which President Putin signed on June 11, 2022.[229] According to this new law, decisions of the ECHR "will no longer be bases for appealing decisions that had been made by Russian courts. In other words, decisions of Russian courts will take precedence over those coming from Strasburg."[230] This development has been a powerful blow to Russia's civil society and the rule of law organizations as they rely heavily on precedents established in ECHR decisions in their human rights-related work.[231]

Koroteev highlights the peculiarities of the facial recognition adaptation in Russia during his talk entitled "You Are Being Surveilled?"[232] According to Koroteev, "what is interesting about Russia is that there is quite good regulation of [facial recognition technology] in banking sector," where

---

226 *Activists Asking ECHR to Find Use of Facial Identification System in Moscow Unlawful, supra* note 200.

227 *Russian Law Talks 8: Understanding Russia's Exit from Strasbourg*, HELSINKI UNIV. (last visited Aug. 15, 2022) https://www2.helsinki.fi/fi/unitube/video/e87ab2e2-148d-4683-ac94-6db42b4f5e3d; *see also Newsroom: Russia ceases to be a party to the European Convention on Human Rights*, COUNCIL EUR. (Sept. 16, 2022) https://www.coe.int/en/web/portal/-/russia-ceases-to-be-party-to-the-european-convention-on-human-rights#:~:text=Six%20months%20after%20its%20exclusion,Rights%20on%2016%20September%202022.

228 The principal legislative assembly in Russia from 1906 to 1917 and since 1993. Russian Duma "performs the same functions as legislatures in other countries. It debates and votes on bills, whose projects are usually prepared by the government (the latter is headed by the president and prime minister)." *See* MERRIAM WEBSTER, *Duma,* https://www.merriam-webster.com/dictionary/duma (last visited Apr. 22, 2023).

229 Federal'nyĭ Zakon RF o Vnesenii Izmeneniĭ v Otdel'nye Zakonodatel'nye Akty RF v Priznanii Utrativshimi Silu Otdel'nykh Polozheniĭ Zakonodatel'nykh Aktov RF [Federal Law of the RF "On Introducing Changes into Certain Legislative Acts of the RF Due to Their Losing Force in Certain Legislative Acts of the RF," Jun. 11, 2022, No. 183-FZ], PUBLICATIONPRAVO.GOV.RU, http://publication.pravo.gov.ru/Document/View/0001202206110028?index=0&rangeSize=1 (Russ.).

230 Gosduma priniala zakony o neispolnenii Rossieĭ reshenieĭ ESPCH [State Duma has made laws about disregarding ECHR decisions], ROKOMSVOBODA (June 7, 2022), https://roskomsvoboda.org/post/espch-ne-ispolnyat/?fbclid=IwAR1i-PCdWddUByI6uqw-ien64Zhp67u7kmM1f23r5wVxOg-dhsbkG_erFd0 (Russ.).

231 Complaint from OVD-Info Attorneys, to Human Rights Council under the President of the Russian Federation, *supra* note 50.

232 Novaya Gazeta, *supra* note 54.

"informed consent" is "required" from a bank customer.[233] He added: "[b]ut when you are being watched by the government, there is no such regulation."[234] Informed consent is not required in Russia, nor are there obvious traces of facial recognition use by the police in administrative court case materials—even though media coverage points to such uses.[235] Agora experts propose three viable motives behind this anomaly:

> (1) [T]he technologies currently possessed by the [Russian] government agencies are not at the level to be used constantly and automatically, and the labor of the policemen is still much cheaper than the use of these cameras; (2) those in power want to implement the technologies as broadly as possible without having to make new laws addressing and limiting them; [and] (3) the evidence of their use is not broadly discussed so as not to create foundation for case law, and not to vent these technologies in a public forum.[236]

A colleague of Koroteev, Roskomsvoboda attorney Sarkis Darbinian added to this discussion, underscoring that the current regulations do not clearly define how and when police can access the cameras, nor establish mechanisms for impartial oversight by a non-government party.[237] He stressed that what Russians currently have is "a system that doesn't have any kind of control. . . . [T]hose in power deny that they are using facial recognition technology, and they say that they need [it] to watch over the streets. Unfortunately, [there is] no legal regulation that controls the use of these technologies."[238] According to Darbinian, the DIT and the MVD[239]

---

[233] *Id.*; *see also* Anastasiia Kruope, *The Government's Advance on Biometric Data: Kremlin Orders Banks to Hand Over Data without Individuals' Consent*, HUM. RTS. WATCH (Jul. 23, 2022), https://www.hrw.org/news/2022/07/23/russian-governments-advance-biometric-data#:~:text=Last%20week%2C%20Russian%20legislators%20adopted,into%20a%20central%20biometrics%20database. However, it must be noted that even in banking, the biometric data is no longer untouchable. *See* Federal'nyĭ Zakon RF o Vnesenii Izmeneniĭ v Stat'iu 14 i 14-1 Federal'nogo Zakona ob Informatsii, Informatsionnykh Tekhnologiiakh i o Zashschite Informatsii' i stat'iu 5 Federal'nogo Zakona o Vnesenii Izmeneniĭ v Otdel'nye Zakonodatel'nye Akty RF, Jul. 14, 2022, No. 325-FZ, [Federal Law No. 325-FZ of 14.07.2022 on Amendments to Articles 14 and 14-1 of the Federal Law on Information, Information Technologies and Protection of Information and Article 5 of the Federal Law on Amendments to Certain Legislative Acts of the Russian Federation], PUBLICATIONPRAVO.GOV.RU, http://publication.pravo.gov.ru/Document/View/0001202207140096?index=0&rangeSize=1 ("obligating banks and state agencies to enter their clients' biometrics, including facial images and voice samples, into a central biometrics database").

[234] Novaya Gazeta, *supra* note 54.

[235] *Id.*; *see also* OVD-INFO REPORT, *supra* note 49.

[236] Novaya Gazeta, *supra* note 54; Gainutdinov & Koroteev, *supra* note 45, at 10-11.

[237] Novaya Gazeta, *supra* note 54.

[238] *Id.*

[239] In Russian, Ministerstvo Vnutrennikh Del, is the "federal executive body responsible for drafting and implementing government policy and legal regulation in the sphere of internal affairs, and drafting government policy in the sphere of migration." GOVERNMENT.RU, http://government.ru/en/department/86/events/.

have an agreement about the uses of facial recognition, but no one has ever seen this document.[240] It is a sign that those in power do not want to be transparent, and do not want to show the processes connected to the uses of [facial recognition on the Russian citizenry]."[241] In contrast, in nearby Georgia, there is an Office of Data Protection that is not connected to other governmental structures and, therefore, does not purportedly have ulterior motives underlying its administrative decisions.[242] Darbinian pointed to this example in Georgia, noting that in Russia, the Roskomnadzor[243] regulates personal data-related processes and is not an independent regulatory body.[244]

In writing "Facial Recognition: The Foreboding of Dystopia," Gainutdinov and Koroteev analyzed judicial treatment of three legal cases[245] challenging facial recognition uses by law enforcement agencies.[246] The authors concluded that in all three instances, Moscow government officials "insisted (and the courts agreed with them), that not only laws about personal data are not to be applied when using facial recognition, but that such cases do not belong to the category of personal data ones."[247] The courts supported the government officials when opponents argued that "cameras recorded open spaces, such as streets and residential buildings' backyards, and that citizens were not targeted subjects in those recordings."[248] Therefore, the courts concluded, it was lawful to use data collected according to Article 152.2 of Civil Code of the RF.[249] The officials also cited the legislation of Moscow government dated February 7, 2012 #24-PP, about the Single Center

240 Novaya Gazeta, *supra* note 54.

241 *Id.*

242 *Id.*

243 Starikova, *supra* note 222. *See also* Alexander Gurkov, *Personal Data Protection in Russia*, *in* PALGRAVE HANDBOOK DIGIT. RUSSIAN STUD., 97 (Daria Gritsenko, Marielle Wijemars, Mikhail Kopotev eds., 2021). Administratively, Roskomnadzor plays an important role in data flows within Russia, and even vis-à-vis companies that are founded outside of the country but operate with data of Russian citizens. The agency has power to investigate and initiate control and supervision of data operators in Russia. Such proceedings do not require claims related to violation of personal rights of individuals. In other words, the agency acts without regard to whether those individuals whose data is being processed have any claims to data operators. "As a result, the activity of Roskomnadzor is directed toward the protection of data as such and not toward the protection of individual rights affected by data processing."

244 Novaya Gazeta, *supra* note 54.

245 Gainutdinov & Koroteev, *supra* note 45. The authors refer to the three following cases: (1) solo protest by Alena Popova near the building of State Duma; (2) the demonstration on Sakharov Avenue on September 29, 2019, against repressions connected to the election campaign for Moscow City Duma; (3) the petitioner obtained recordings from cameras with facial recognition with her personal data on "black market." *Id.* In the first two cases, the DIT did not deny uses of facial recognition technologies. *Id.* Moreover, in the second case, on September 29, 2019, the DIT even offered an MVD document about uses of the technology. *Id.*

246 *Id.*

247 *Id.*

248 *Id.*

249 *Id.*

for Storage of Personal Data, which made such data collection lawful according to government officials and the courts.[250] Agora attorneys concluded in their report that it can be predicted with utmost certainty that Russian courts will continue to support the government's claim that data collected by the CCTV cameras on streets and during public gatherings is not to be classified as "personal data" collection in legal proceedings in Russia.[251] This is the crux of the current legal practices paradox in Russia regarding facial recognition adaptation. Multiple Moscow district and city courts have deemed that when banking services collect biometric data through CCTV cameras, this data is personal data. But when street CCTV cameras equipped with facial recognition collect data during routine surveillance and protests, this data is somehow not personal data.[252]

It is not only judicial interpretations and decision-making that codify this understanding of personal data law as it relates to AI-facial recognition technology. Roskomnadzor[253] and its official statements and interpretations regarding the existing laws have influence on how such novel technology as facial recognition is being used by other governmental agencies. According to the relevant article of Russian Civil Code,[254] entitled "Protection of [Russian] citizen's image," collecting information about an individual (including one's image) in public spaces does not require consent of an individual in question. In other words, information collected about an individual in public spaces is not considered to be information about private life of the individual.[255] Andreeva and her co-authors argue in their article on uses of AI in criminal proceedings that such "principle" of separation between what is private and what is public was just "before the advent of facial recognition and [advanced technological] surveillance."[256] Yet, according to Roskomnadzor's interpretation of the above mentioned law in 2013, data collected from videorecording in public spaces does not qualify

250 *Id*.

251 *Id.*

252 *Id.*

253 *See* Gurkov, *supra* note 243 for the description of official duties delegated to Roskomnadzor by the Russian government.

254 Grazhdanskiĭ Kodeks Rossijskoĭ Federatsii [GK RF] [Civil Code of the Russian Federation Article 152.1. Protection of the Image of a Citizen], CONSULTANT.RU (April 16, 2022), http://www.consultant.ru/document/cons_doc_LAW_5142/14c6c3902cffa17ab26d330b2fd4fae28e5cd059/ (Russ.) (Art. 1, Part 2).

255 Andreeva Olga Ivanovna, Ivanov Viacheslav Vasil'evich, Nesterov Alexandr Iur'evich, & Trubnikova Tat'iana Vladimirovna, Tekhnologii raspoznavaniia lits v ugolovnom sudoproizvodstve: problema osnovaniĭ pravovogo regulirovaniia ispol'zovaniia iskusstvennogo intellekta [Facial Recognition Technologies in Criminal Proceedings: Problems of Grounds for the Legal Regulation of Using Artificial Intelligence], 449 BULL. TOMSK ST. UNIV. 201, 206 (2019) https://cyberleninka.ru/article/n/tehnologii-raspoznavaniya-lits-v-ugolovnom-sudoproizvodstve-problema-osnovaniy-pravovogo-regulirovaniya-ispolzovaniya (Russ.).

256 *Id.*

as biometric personal data before the actual moment an individual is identified in a given videorecording.[257] According to Roskomnadzor, it is sufficient that the individuals be notified in advance by an appropriate administrator about the possibility of photo or videorecording.[258] Further, consent of those being photographed or recorded is not required.[259]

Notably, even though there is a lack of clear, coherent regulations addressing the uses of facial recognition technology[260] by the Russian police, and lack of transparency as to DIT's and MVD's cooperation with regard to personal data transfers,[261] the State Duma was proactive in passing laws regulating governmental powers and banking industry in this regard.[262] For instance, the Russian government is developing a federal bank of biometric data, with the cooperation of the Central Bank of Russia[263] and Rostelekom. This single biometric system was given the status of state information system, according to the Federal Law of the RF "On Introducing Changes in Certain Lawmaking Acts of the RF" No. 479-FZ, signed by President Putin on December 29, 2020.[264] The collected personal data must be integrated within the Single System of Identification and Authorization ("SSIA").[265]

Additionally, Federal Law of the Russian Federation No. 123-FZ "On Carrying out Experiment on Establishment of Special Regulation for the Purpose of Creation of Necessary Conditions for Development and Deployment of Technologies of [AI] in the Subject of the [RF]—the Federal City of Moscow and Introduction of Amendments to Articles 6 and 10 of the

---

257 *Id.*

258 *Id.*

259 *Id.*

260 *See* Borak, *supra* note 16. Sergey Ross, the founder of the Collective Action Center think tank and a former Moscow politician, stresses that

> A key concern is that Moscow's surveillance system was designed to conceal its data collection from Moscow's 12 million residents. . . . Although the system is run by the Moscow government, elected members of the Moscow City Duma say they are excluded from regulating face recognition systems and have little insight into how it is being used. "It's a complete black box," says Ross.

Id.

261 *See* Novaya Gazeta, *supra* note 54. Darbinian underlines in his interview that there is an agreement between the DIT and the MVD which prescribes how collection of biometric and personal data on the streets of Moscow should take place, but no one has ever seen it as it is "classified." *Id.*

262 Gainutdinov & Koroteev, *supra* note 45.

263 The Central Bank of the Russian Federation is "the main issuing bank and monetary regulator of the country." *History of the Bank of Russia,* BANK RUSS., https://www.cbr.ru/eng/about_br/history/.

264 Federal'nyĭ Zakon RF o Vnesenii Izmeneniĭ v Otdel'nye Zakonodatel'nye Akty Rossiĭskoĭ Federatsii [Federal Law of the Russian Federation on Introducing Changes in Certain Lawmaking Acts of the RF] 2020, No. 479-FZ, ALTA.RU, https://www.alta.ru/tamdoc/20fz0479/ (Russ.).

265 In Russian, Edinaia Sistema Identifikatsii i Avtorizatsii ("ESIA").

Federal Law 'About Personal Data'"[266]—enacted in April, 2020 and having come into effect on July 1, 2020—allows city officials not to adhere to laws relating to personal data.[267] This experimental scheme also allows companies to work on innovative AI technologies that are not regulated under existing legislation, which creates opportunities for observing how AI functions in real-life scenarios.[268] This law attempts to create a regulatory body (the "Council") to "control" the experiment's development, while, at the same time allowing the Moscow Mayor's Office to regulate personal data collection as it sees fit.[269] Once again, the law is quite unclear as to the Council's powers. Even though the idea of the Council was officially discussed back in December 2020, the agency has yet to be, in fact, created.[270] The law is the first step towards regulation of AI technology in Russia.[271] The duration of this legal experimental scheme will last five years starting from July 2020.[272] It is the Moscow municipality's right hand in developing Moscow "Smart City" as per Sobyanin's official strategy.[273] To the great chagrin of human rights activists and rule of law professionals, the law does not address where the data of digital identities will be stored and for how long, how the citizens' privacy will be protected, and who will be liable in cases of security and data breaches.[274]

As to other administrative developments, 2011 marked the founding of the Single Center for Storage and Processing of Data ("Single Center"),[275]

---

266 Federal'nyĭ Zakon RF o Provedenii Eksperimenta po Ustanovleniiu Spetsial'nogo Regulirovaniia v Tseliakh Sozdaniia Neobkhodimykh Usloviĭ dlia Razrabotki i Vnedreniia Tekhnologii Iskusstvennogo Intellekta v Sub"ekte RF – Gorode Federal'nogo Znacheniia Moskve i Vnesenii Izmeneniĭ v Stat'i 6 i 10 Federal'nogo Zakona o Personal'nykh Dannykh [Federal Law of the Russian Federation Dated Apr. 24, 2020, No. 123-FZ], CIS LEGISLATION, https://cis-legislation.com/document.fwx?rgn=124089 (last visited March 25, 2023).

267 *Id.*; *see* Gainutdinov & Koroteev, *supra* note 45.

268 *A new experimental legal framework in Russia shows the perils and promise of future AI regulation,* GOWLING WLG (Sep. 14, 2020), https://gowlingwlg.com/fr/insights-resources/articles/2020/future-ai-regulation-in-russia/.

269 Gainutdinov & Koroteev, *supra* note 45.

270 *Id.*

271 *Id.; see* GOWLING WLG, *supra* note 268.

272 Gainutdinov & Koroteev, *supra* note 45*; see* GOWLING WLG, *supra* note 268.

273 Moscow Smart City Report 2030, *supra* note 18; *see also* GOWLING WLG, *supra* note 268.

274 *See* GOWLING WLG, *supra* note 268.

275 Gorodskaia sistema videonabliudeniia [City Video Surveillance System] and Edinyĭ tsentr khraneniia i obrabotki dannykh ("EZHOD") [Single Center for Storage and Processing of Data ("SCSPD"), BUDGETARY INST. CITY MOSCOW, http://gbuchc.ru/poleznaya-informatsiya/pozharnaya-bezopasnost/174-gorodskaya-sistema-videonablyudeniya.9T (last visited March 25, 2023) (Russ.). This regulation was part of a Moscow-based program called "Information City," and was enforced by the Moscow municipal government. *Id.* The regulation covered the following areas of video-surveillance: entries to residential buildings, backyards of residential buildings, mass gatherings, educational facilities, weekend mall spaces, as well as those of various trading and service posts, medical facilities, construction sites. *Id. See also* Postanovlenie Pravitel'stva Moskvy ot 9 avgusta 2011 g. No. 349-PP ob Utverzhdenii

a technological center (building housing servers),[276] that processes data received from CCTV cameras.[277] Agora attorneys note that, concurrently, anti-government protest activity increased in Moscow.[278] In 2012, approximately 60,000 new cameras were installed on city's streets.[279] Further, protest participants were ordered not to cover their faces and not to use masks.[280] The "Single Center" grew to include data collected by eighteen different state agencies.[281] The official explanation behind the Center's expansion was to use AI capabilities for purported socially desirable purposes, such as predicting and reacting to possible emergencies, including "deluges, pandemic, car accidents, organized crime, earthquakes, [and] illegal mass gatherings."[282]

Federal Law of December 31, 2017, No. 482-FZ,[283] established bases for creation and implementation of "single informational system of personal data, targeting processing of such data (including the collection and storage of biometric personal data), data's authentication, and transfer of information about how well the above processes correspond with biometric personal data of a given citizen of the [RF]."[284] The existence of this unified system was established by Article 14.1 FZ of the Federal Law of the RF "On the Information, Information Technologies and Protection of Information"[285] which discusses the collection of data for preservation in a single biometric

Gosudarstvennoĭ Programmy Goroda Moskvy 'Razvitie Tsifrovoĭ Sredy i Innovatsiĭ (s Izmeneniiami i Dopolneniiami)" [Regulation by City of Moscow Government "On Establishment of Governmental Program of the City of Moscow 'Development of Digital Space and Innovation (with Changes and Additions)" Dated Aug. 9, 2011, No. 349-PP], BASEGARANT.RU, https://base.garant.ru/397438/ (Russ.) (last visited March 25, 2023).

276 *See* Postanovlenie Pravitel'stva Moskvy ot 9 avgusta 2011 g. No. 349-PP ob Utverzhdenii Gosudarstvennoĭ Programmy Goroda Moskvy 'Razvitie Tsifrovoĭ Sredy i Innovatsiĭ (s Izmeneniiami i Dopolneniiami), *supra* note 275. It is impossible to access the "Single Center" as it is "technological center" (a building housing multiple servers). *Id.*

277 Gainutdinov & Koroteev, *supra* note 45.

278 *Id.*

279 *Id.*

280 *Id.*

281 *Id.* at 5.

282 *Id.*

283 Federal'nyĭ Zakon RF o Vnesenii Izmeneniĭ v Otdel'nye Zakonodatel'nye Akty Rossiiskoĭ Federatsii, 2017, No. 482-FZ [Federal Law of the RF on Introducing Changes in Certain Lawmaking Acts of the RF, 2017, No. 482-FZ], PUBLICATION.PRAVO.GOV.RU, http://publication.pravo.gov.ru/Document/View/0001201712310004 (Russ.) (last visited March 25, 2023).

284 Gainutdinov & Koroteev, *supra* note 45, at 19.

285 Federal'nyĭ Zakon RF ob Informatsii, Informatsionnykh Tekhnologiiakh i o Zashchite Informatsii ot 27 iiulia 2006, No. 149-FZ [Federal Law on Information, Information Technologies and Information Protection Dated Jul. 27, 2006. No. 149-FZ], ALTA.RU, https://www.alta.ru/tamdoc/06fz0149/?print (Russ.) (last visited March 25, 2023).

system and its uses for the identification of citizens.[286] The collection of facial photos is mentioned at the very start of the Ruling No. 772 of the RF, dated June 30, 2018.[287] Agora experts conclude in their report that, eventually, a balance will emerge between the harms and advantages of facial recognition technology usages in democratically inclined countries.[288] On the other hand, in countries that lean towards authoritarian political regimes, and that can afford to buy or build these technologies, facial recognition software will eventually become more affordable. The tech industry will continue to routinely portray these innovations as necessary for public safety and convenience, making them desirable for those parties who can afford to purchase them.[289] Lawmakers will adhere, *post-factum*, to these realities. In the case of Moscow, and subsequently that of Russia, the courts—mostly driven by the political agendas and interests of the state[290]—will solidify the position of those in power in their interpretation of current laws.[291] It is

[286] The above Article 14.1 FZ from the Federal Law of the RF on the Information, Information Technologies and Information Protection was superseded by Federal'nyĭ Zakon RF ob Osushchestvlenii Identifikatsii i (ili) Autentifikatsii Fizicheskikh Lits s Ispol'zovaniem Biometricheskikh Personal'nykh Dannykh, o Vnesenii Izmeneniĭ v Otdel'nye Zakonodatel'nye Akty RF i Priznanii Utrativshimi Silu Otdel'nykh Polozheniĭ Zakonodatel'nykh Aktov [Federal Law of the RF on Undertaking Identification and (or) Authentication of Physical Persons Using Biometric Personal Data, on Introducing Changes into Certain Lawmaking Acts of the RF and Acknowledging that Certain Lawmaking Acts Are Outdated] 2022, No. 572-FZ, PUBLICATION.PRAVO.GOV.RU, http://publication.pravo.gov.ru/Document/View/0001202212290024 (Russ.) (last visited March 25, 2023).

[287] Gainutdinov & Koroteev, *supra* note 45, at 19; *see also* Postanovlenie Pravitel'stva RF ot 30 iiunia 2018 g. No. 772 ob Opredelenii Sostava Svedeniĭ, Razmeshchennykh v Edinoĭ Informatsionnoĭ Sisteme Personal'nykh Dannykh, Obespechivayushcheĭ Obrabotku, Vklyuchaia Sbor i Khranenie, Biometricheskikh Personal'nykh Dannykh, Ikh Proverku i Peredachu Informatsii o Stepeni Ikh Sootvetstviia Predostavlennym Biometricheskim Personal'nym Dannym Fizicheskogo Litsa, Vklyuchaia Vid Biometricheskikh Personal'nykh Dannykh, a Takzhe o Vnesenii Izmeneniĭ v Nekotorye Akty Pravitel'stva RF" (s Izmeneniiami i Dopolneniiami) 2018, No. 772 [Ruling of Government of the RF on Identification of Information, Found in the Single Information System of Personal Data, Guaranteeing Processing, and Including Collection and Storage of Biometric Data, Checking and Transfer of the Information About How Well [the Data] Corresponds With Given Personal Data of a Certain Physical Person, Including the Variety of Personal Data, and Also on Introducing Changes to Certain Acts of Government of the RF (with Changes and Additions)] 2018, No. 772, BASE.GARANT.RU, https://base.garant.ru/71979312/#friends (Russ.) (last visited March 25, 2023).

[288] Gainutdinov & Koroteev, *supra* note 45, at 23-24.

[289] *Id.*

[290] Kommersant, *As long as the judicial system of the Russian Federation does not become more independent, doubts about its effectiveness remain*, COUNCIL EUR. (Feb. 25, 2016), https://www.coe.int/en/web/commissioner/-/as-long-as-the-judicial-system-of-the-russian-federation-does-not-become-more-independent-doubts-about-its-effectiveness-remain. The authors, who have studied Russian judicial system for seventeen years, identified four main challenges existing in the country: "issues related to non-enforcement of court decisions, obstacles to the international system of human rights protection, insufficient judicial independence and excessive prosecutorial powers." *Id.* The authors stressed that Russian judges "remain exposed to pressure from powerful political and economic interests." *Id.*

[291] *Id.*

evident that emerging legislation and its practical applications benefit the government and the industry, supplying the former with the latest technologies. Individuals' privacy rights remain underrepresented thus far—Moscow courts do not believe they must address these rights in cases dealing with the surveillance of public spaces, evidenced by the judicial treatment of the Popova case.

B. Personal Data Laws and the Roles of the Legislature and the Judiciary

The Russian State Duma enacted data protection laws in 2006,[292] before which the Russian Constitution of 1993—specifically Articles 23 and 24[293]—were used as a foundation for data rights protections:[294]

> According to Article 23 of the RF Constitution, every person has a right to a private life and personal and family secret. According to Article 24, collection, storage, usages and dissemination of information about private life of a person without their consent is not allowed. Article 137 of Criminal Code of the RF discusses criminal culpability for violating private life. According to Paragraph 1 Article 3 of Federal Law from July 27, 2006 No. 153 "About personal data," personal data is seen as any information related directly or implicitly to a certain identified or identifiable physical person (subject of personal data). Paragraph 1 of Article 9 of a given law finds that it is subject of personal data who makes a decision about revealing his or her personal data and gives consent to their processing, freely, of his or her own will, and in his or her interests.[295]

In July 2007, the State Duma passed two laws dedicated to data protection: (1) Federal Law No. 149-FZ ("On Information, Information Technologies and Protection of Data");[296] and (2) Federal Law No. 152-FZ, the "Law on

---

[292] Gurkov, *supra* note 243.

[293] Konstitutsiia Rossiĭskoĭ Federatsii [Constitution of the Russian Federation], PRESIDENT RUSS., http://kremlin.ru/acts/constitution/item (Russ.) (art. 23 and art. 24).

[294] *See* Gurkov, *supra* note 243.

[295] Bukaev Nikolaĭ Mikhaĭlovich & Ismagilov Rinat Al'bertovich, K voprosu sobliudeniia konstitutsyonnykh prav grazhdan v ugolovnom sudoproizvodstve pri ispol'zovanii v dokazyvanii kamer s funktsyeĭ raspoznavaniia lits [On the Issue of Observing the Constitutional Rights of Citizens in Criminal Proceedings When Using Face Recognition Cameras in Evidence], CYBERLENINKA, https://cyberleninka.ru/article/n/k-voprosu-soblyudeniya-konstitutsionnyh-prav-grazhdan-v-ugolovnom-sudoproizvodstve-pri-ispolzovanii-v-dokazyvanii-kamer-s-funktsiey (Russ.) (last visited Aug. 6, 2022).

[296] Federal'nyĭ Zakon No. 149-FZ 27 iiulia 2006 g. ob Zashchite Informatsii, Informatsionnykh Tekhnologiiakh i o Zashchite Informatsii (s Izmeneniiami i Dopolneniiami) [Federal Law "On Information, Information Technologies and the Information Protection" No. 149-FZ Dated Jul. 27, 2006], WORLD TRADE ORG., https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus58_leg_369.pdf (last visited March 25, 2023).

Personal Data."[297] The second law defines biometric personal data as information of an "individual's biological and physiological characteristics that enables the individual's identification and is used by the controller for identification" purposes.[298] Some legal experts—among them Agora attorneys and advocates representing Russian citizens in numerous administrative hearings following political protests—insist that CCTV cameras with facial recognition capabilities violate the above-mentioned constitutional and federal rights.[299] These legal experts view such violations as grave intrusions on privacy rights of Russian citizens in the context of these constitutional and federal protections. This legal position conflicts with how governmental bodies, including Moscow courts, interpret these laws and the facts of specific cases, as evidenced by their treatment of the *Popova* proceedings.[300]

As discussed, federal personal data protection laws requiring the data subject's consent do exist in Russia; what makes these laws difficult to comprehend is their interpretation by the judicial bodies. The prevalent tendency of judges, thus far, has been to support the actions of law enforcement agencies and to treat specific legal cases,[301] in which data collected from CCTV cameras by the police is used as evidence, as belonging to the category of non-personal data cases.[302] Procedurally, this approach allows courts to practically bypass the existing personal and biometric-related laws altogether, for judges do not apply personal data laws to cases involving the police and its uses of facial recognition-based evidence. Moreover, they stress in their decisions that no collection of personal data took place.[303] Therefore, not only does the "reaction of the government 'lag[]' behind rapid technological innovations,"[304] but the judiciary's treatment of cases involving facial recognition technology also sets damaging precedent, making it increasingly difficult for Russian individuals to have

297 Gurkov, *supra* note 243, at 96; *see also* Federal'nyĭ Zakon o Personal'nykh Dannykh, 2006 g., No. 152-FZ [Federal Law on Personal Data, Dated 2006, No. 152-FZ], BASE.GARANT.RU, https://base.garant.ru/12148567/ (Russ.) (last visited Mar. 25, 2023).

298 Ksenia Andreeva & Dmitry Simbirtsev, *Russia: Basics of Biometric Data Processing and Protection*, MORGAN, LEWIS & BOCKIUS LLP, https://www.morganlewis.com/-/media/files/publication/outside-publication/article/2022/russia-basics-of-biometric-data-processing-and-protection-dataguidance.pdf (last visited Aug. 10, 2022).

299 *See* Complaint from OVD-Info Attorneys, to Human Rights Council under the President of the Russian Federation, *supra* note 50 discussed *infra* Part III.

300 Roskomsvoboda trebuet vvesti moratoriĭ na sistemy raspoznavaniia lits [RosKomSvoboda Demands a Moratorium on Facial Recognition Systems], ROSKOMSVOBODA (Oct. 7, 2019), https://roskomsvoboda.org/50441/ (Russ.).

301 *See* Gainutdinov & Koroteev, *supra* note 45.

302 *Id.* at 21.

303 *Id.* Both Moscow government and Moscow courts accentuate that the CCTV cameras "record open spaces," and Russian citizens are not subjects of such video recordings. *Id.*

304 Andreeva, Ivanov, Nesterov & Trubnikova, *supra* note 255, at 206.

their day in court for biometric privacy-related litigation. In practice, there are no legal guarantees of protection from data leakages or data abuses by those who use facial recognition.[305]

Recent changes proposed by the State Duma complicate the application and understanding of existing data privacy laws.[306] A number of Russian attorneys, among them Sarkis Darbinian and Stanislav Seleznev, commented on inconsistencies within the modifications proposed to Federal Law No. 149-FZ in July 2006,[307] that took place at the end of 2021.[308] According to these attorneys, the final proposed changes had gone through approximately three rounds of readings, and have eventually included multiple corrections by different legislators.[309] The attorneys commented on the lack of clarity in the proposed changes and the possibility of future procedural challenges, writing that:

> By the time proposed changes were to be read for the third time, the legislative project turned into a curious nesting doll, because besides proposals about justification for extremism, there emerged norms about biometrics. . . . In other words, for whatever reason, with the help of a given document, someone decided to work on biometric legislation as well. There is no logic of juridic technique in this. One law will regulate two absolutely different spheres: Internet censure on one hand and surveillance based on biometric data on the other hand.[310]

The attorneys explained that it is not a rare practice for a proposed legislation to go through multiple readings in the Duma.[311] However, it is troubling that the document increased five times in length since its first draft and had a chunk of text added that was not in the original proposal.[312] Such a practice is an aberration from the standard legislative process.[313] The attorneys warned that: "[c]onsidering that the ruling about biometric identification is included in anti-extremist proposed law, maybe, legislators are implying that anyone who is suspected of participating in extremism will be found with the help of a biometric system? Only such logic comes to one's mind."[314] Darbinian deciphers even more existential agenda at work:

---

305 Starikova, *supra* note 222.

306 Prinyat zakon o biometricheskoĭ identifikatsii i rasshirenii vnesudebnykh blokirovok [Law on Biometric Identification and Expansion of Extrajudicial Lock Downs Passed], ROSKOMSVOBODA (Dec. 22, 2021), https://roskomsvoboda.org/post/prednovogodni-extrem-i-biometr-trash/ (Russ.).

307 *Id*.

308 *Id*.

309 *Id.*

310 *Id.*

311 *Id.*

312 *Id.*

313 *Id.*

314 *Id.*

> It appears that proposed corrections do not have any relation to system of [Internet] blockages and filtration. But if one looks deeper, it is possible to understand plans of our legislators for the next few years. The government is sending a signal that biometrics is becoming a state monopoly. Any work with biometrics through online services will be built through Single Biometric System, which from now on will be a government-controlled information system. It is evident that the government is progressing into the next stage: identification of all citizens with the help of biometric data. The idea of Internet passport is becoming increasingly real. The government will do as it pleases.[315]

Darbinian's vision of the more subtle motives of those in power serves as a rather realistic prediction of what to expect in years to come. Governmental centralization of personal and biometric data will steadily lead to one most certain outcome: surveillance over all Russian citizens. A sort of legal "grey zone" is thus created in how governmental agencies and the judiciary interpret claims dealing with CCTV cameras and biometric data collection: with less or no regard for individuals' rights, inevitably producing a multitude of possible abuses by those in power (i.e., by law enforcement, the mayor's office, bank officials, to name a few possible scenarios).[316]

In 2021, law enforcement detained at least "454 persons in seventeen cities" throughout Russia, in what Russian attorneys refer to as "*post factum* detention,"[317] or detentions related to demonstrations and political protests.[318] A highly centralized and standardized biometric system, while controlled by the government and unchallenged by civil society or external legal bodies—such as the ECHR[319]—will most certainly lead to the normalization of individuals' privacy rights violations, thus establishing them as a customary occurrence. The state monopoly over biometric data in Russia can be viewed as possibly the government's most important investment in increased surveillance and diminishment of any possibility of meaningful political dissent, now with the assistance of the most sophisticated technological means.

C. Trends in Facial Recognition-Related Case Law: A Closer Look at the Popova Decision

An analysis of the *Popova* and *Popova & Milov cases*, eventually submitted by the petitioners to the ECHR, serves as an example of how such

---

315 *Id.*

316 Starikova, *supra* note 222.

317 *Id.*; *see also* OVD-INFO REPORT, *supra* note 49.

318 Starikova, *supra* note 222.

319 *See Russia Ceases to be a Party to the European Convention on Human Rights on September 16 2022, supra* note 133. This support coming from an important European institution is no longer possible as Russia has been recently expelled from the European Convention on Human Rights.

Moscow judicial bodies as Savyolovsky[320] and Tverskoy District Courts[321] categorize administrative cases where facial recognition technologies are involved. In these cases, where the opposing parties were the Russian Interior Ministry's Directorate for Moscow ("MVD") and the DIT[322] the main complaint was that the MVD and the DIT processed a Russian citizen's biometric data without her written consent.[323] Specifically:

> [Alena Popova] claimed that her biometric data had been collected and used by law enforcement agents during her detainment after her solo protest in April, 2018. At the time, the court administered a fee to be paid by her in the amount of 20 thousand rubles [US$324]. During the proceeding the

[320] *See* Savyolovsky District Court of the city of Moscow, PRAVO.RU, https://pravo.ru/arbitr_practice/courts/144/ (Russ.). The district courts were founded by Article 4 of the Federal Constitutional Law of December 31, 199, No. 1-FKZ on the Judicial System of the Russian Federation. *Id.* According to this law, district courts belong "to courts of common jurisdiction, being courts of lowest level." *Id.* These courts preside over civil, criminal and administrative cases. *Id. See also*, Andreeva, Ivanov, Nesterov & Trubnikova *supra* note 255. Andreeva and her co-authors accentuate that both district courts agreed with the MVD and the DIT that there was no violation of personal data laws as there was no identification taking place. *Id.*

[321] *See* Tverskoy District Court of the city of Moscow, MOS-GORSUD.RU, https://mos-gorsud.ru/rs/tverskoj; Alena Popova podala vtoroĭ isk protiv sistemy raspoznavaniia lits v Moskve [Alena Popova filed a second lawsuit against a facial recognition system in Moscow], MEDUZA (Jan. 23, 2020), https://meduza.io/news/2020/01/23/alena-popova-podala-vtoroy-isk-protiv-sistemy-raspoznavaniya-lits-v-moskve (Russ.). *See* Opredelenie Tverskogo Raĭonnogo Suda Goroda Moskvy "Prekratit' Proizvodstvo po Administativnomu Delu No. 2a-72/2020 po Adminstrativnomu Iskovomu Zaiavleniiu Popovoĭ A.V., Milova V.S. k Departmentu Informatsionnykh Tekhnologiĭ Goroda Moskvy, GU MVD Rossii po Gorodu Moskve o Priznanii Nezakonnymi Deĭstviĭ po Sboru I Obrabotke Personal'nykh Dannykh . . . .", ot 3 marta 2020 g., No. 2a-72/2020 [Ruling of Tverskoy District Court of the City of Moscow "To Terminate Complaint in Administrative Case N 2a-72/2020 in Administrative Proceeding Filed by Popova A.V., Milov V.S. Against the Department of Information Technologies of the City of Moscow, GU MVD of Russia in the City of Moscow Asking To Find Their Actions of Collecting and Processing of Personal Data to Be Unlawful . . . .", Dated Mar. 3, 2020, No. 2a-72/2020, https://www.mos-gorsud.ru/mgs/services/cases/appeal-admin/details/19d4a1a6-531e-494a-938b-b14837eeadd8. (Russ.).

[322] *Activists Asking ECHR to Find Use of Facial Identification System in Moscow Unlawful, supra* note 200.

[323] Sud otkazalsia zapreshchat' sistemu raspoznavaniia lits na ulitsakh Moskvy [The court refused to prohibit system of facial recognition on the streets of Moscow], MEDUZA, (Nov. 6, 2019), https://meduza.io/news/2019/11/06/sud-otkazalsya-zapreschat-sistemu-raspoznavaniya-lits-na-ulitsah-moskvy (Russ.). *See* Reshenie Saviolovskogo Raĭonnogo Suda Rossiĭskoĭ Federatsii "O Priznanii Nezakonnymi Deĭstviia, Obiazanii ne Primeniat' Tekhnologii Raspoznavaniia Lits na Territorii . . . ., Udalit' Biometricheskie Personal'nye Dannye iz Bazy Dannykh Izobrazheniĭ Grazhdanina, Opredostavit' Dokazatel'stva . . . . Otkazat'" ot 6 noiabria 2019 g., No. 2a-577/19 [Decision of Savyolovsky District Court of Russian Federation "On Invalidating Acts, Duty Not To Use Facial Recognition on the Territory of . . ., to Delete Biometric Personal Data From the Database of Citizen's Images, to Provide Evidence . . . . Motion Denied" Dated Nov. 6, 2019, No. 2a-577/19, https://www.mos-gorsud.ru/rs/savyolovskij/services/cases/kas/details/988f386e-be51-47b0-b48f-e871043ef1fc#tabs-3 (Russ.).

> printouts from video-recordings were used on which [Popova's] face was magnified thirty two times.[324]

In November 2019, the Moscow Savyolovsky District Court "denied [Popova's] lawsuit containing the same claims."[325] In this case, Popova was a plaintiff, asking the court to find the uses of facial recognition in city-wide surveillance system illegal.[326] The Savyolovsky District Court judge, Marina Ivanova, found the evidence provided by Popova to be insufficient.[327] Consequently, Popova challenged the decision of the Savyolovsky District Court and appe.aled in January, 2020.[328] The appeals court, the Moscow City

[324] Sud prekratil proizvodstvo po isku o zaprete tekhnologiĭ raspoznavaniia lits [The court has terminated law suit regarding prohibition of facial recognition], RAPSINEWS (Mar. 4, 2020), https://rapsinews.ru/judicial_news/20200304/305534387.html (Russ.). Alena Popova was a defendant in a court case concerning the violation of rules for conducting public events and demonstration. She was fined by the Tverskoy District Court in 2018. The Moscow City Court confirmed the validity of Tverskoy court ruling in a case No. 4a-6688/2018. *See* Moskovskiĭ Gorodskoĭ Sud Postanovil "Postanovlenie Sud'i Tverskogo Raĭonnogo Suda g. Moskvy ot 13 Aprelia 2018 g., Reshenie Sud'i Moskovskogo Gorodskogo Suda ot 4 Iiulia 2018 g., v Redaktsii Opredeleniia ob Ispravlenii Opiski ot 16 Oktiabria 2018 g. po Delu ob Administrativnom Pravonarushenii, Predusmotrennom ch. 2 st. 20.2 KoAP RF, v Otnoshenii Popovoĭ *** Ostavit' bez Izmeneniia, Zhalobu Zashchitnika Krupskogo M.A. – bez Udovletvoreniia" 16 noiabria 2018 g., No. 4a-6688/18 [Moscow City Court Decided "Ruling by the Judge of Tverskoy District Court of the City of Moscow Dated Apr. 13, 2018, To Leave the Decision of Moscow City Court's Judge Dated Jul. 4, 2018 Editing Ruling on Correcting Case Dated Oct. 16, 2018 in Case Regarding Administrative Violation, Regulated by Part 2 Article 20.2 KoAP, Regarding Popova *** To Leave Without Changes, and Complaint by Attorney Krupskiĭ M. A. – Without Satisfying" Nov. 16, 2018, No. 4a-6688/18], MOS-GORSUD.RU, https://www.mos-gorsud.ru/fastsearch?q=%D0%90%D0%BB%D1%91%D0%BD%D0%B0+%D0%9F%D0%BE%D0%BF%D0%BE%D0%B2%D0%B0&page=1 (Russ.).

[325] In this lawsuit, Popova filed her administrative proceeding complaint with the assistance of Roskomsvoboda attorneys. *See* Sud ne priznal sistemu raspoznavaniia lits nezakonnoĭ. Kommentariĭ RosKomSvobody [The court did not recognize the facial recognition system as illegal. Comment by RosKomSvoboda, ROSKOMSVOBODA (Nov. 6, 2019), https://roskomsvoboda.org/51831/ (Russ.); *see also* Reshenie Savelovskogo Raĭonnogo Suda g. Moskvy po Delu No. 02A-0577/19 ot 6 noiabria 2019 g. [Decision of Savyolovsky District Court of Moscow case No. 02A-0577/19, Dated Nov. 6, 2019], MOS-GORSUD.RU, https://www.mos-gorsud.ru/rs/savyolovskij/services/cases/kas/details/988f386e-be51-47b0-b48f-e871043ef1fc (Russ.).

[326] On November 6, 2019, the Justice of Savyolovsky District Court of city of Moscow denied Popova's administrative claim against the MVD and the DIT. *See* Reshenie Savelovskogo Raĭonnogo Suda Goroda Moskvy po Delu No. 02A-0577/19 ot 6 noiabria 2019 g. [Decision of Savyolovsky District Court of Moscow case No. 02A-0577/19, Dated Nov. 6, 2019], MOS-GORSUD.RU, https://www.mos-gorsud.ru/rs/savyolovskij/services/cases/kas/details/988f386e-be51-47b0-b48f-e871043ef1fc (Russ.).

[327] Sud ne priznal sistemu raspoznavaniia lits nezakonnoĭ. Kommentariĭ RosKomSvobody, *supra* note 325.

[328] Vasiliĭ Vasil'evich Iarovenko, Galina Mikhaĭlovna Shapovalova, & Rinat Al'bertovich Ismagilov, *Selected Application Problems Face Recognition Systems for Law Enforcement*, 61 LEGAL STATE: THEORY & PRAC.189, 194-95 (2021). To learn about appeals ruling *see* Apelliatsionnoe Opredelenie Sudebnoĭ Kollegii po Administrativnym Delam Moskovskogo Gosudarstvennogo Gorodskogo Suda po Apelliatsionnoĭ Zhalobe Popovoĭ A.V. na Reshenie Saviolovskogo Raĭonnogo Suda Goroda Moskvy ot 6 Noiabria 2019 g." ot 30 ianvaria 2020 g., No. 33a-707/2020 [Appeals Ruling of Judiciary Collegium Regarding Administrative Cases of Moscow City Court as to Appellate Complaint of Popova A. V. Following the Decision of Savyolovsky District Court of City of Moscow Dated Nov. 6, 2019" of Jan. 30,

Court, agreed with the Savyolovsky District Court, and left the matter without changes[329] based on:

> [N]orms of material law and given facts. The receipt of video-recording of an administrative petitioner [Popova] during period that one is surveyed by a specific camera, which is located there to oversee what is going on near the building of the State Duma of the RF, does not qualify as collection of personal (biometric) data of the petitioner because it was not used to identify the petitioner.[330]

Notably, Roskomsvoboda's attorneys in Popova's case strongly believed that they had enough evidence to prove that such governmental agencies as the DIT, the MVD, and city police used "unconstitutional illegal [facial recognition] technology, which was not allowed by 'Personal Data Law'" to collect and process citizens' images.[331] According to Roskomsvoboda attorneys' interpretation of "Personal Data Law" Popova's consent was required.[332] On the other hand, governmental agencies' main counter-argument was that "facial recognition is needed not only for 'watching over' people, but to make sure the roads are clean . . . [and that] citizens are not subjects of surveillance."[333] Further, DIT's position was that they only store images of citizens, and not their personal data; therefore, they are unable to delete anything as had been requested by Popova in her motion.[334] According to the DIT, it is algorithms that translate images into a special code, and citizens' "consent is only required if a given image is accompanied by the personal data."[335] The important outcome of the proceeding was that the DIT and the MVD refused to acknowledge that the facial recognition system was already functioning in Moscow.[336] Moreover, despite the evidence provided by Popova and Roskomsvoboda, the courts (first Tverskoy District Court, then Moscow City Court, and later Savyolovsky District Court) supported the position of governmental agencies—namely, that facial recognition algorithms can expose similarities in codes and mathematical vectors in the original and analyzed video, with some certainty; therefore, no identification

2020, No. 33a-707/2020], https://www.mos-gorsud.ru/mgs/services/cases/appeal-admin/details/6c9dfe4c-ecc7-4626-90f4-dea208d54b5f#tabs-3 (Russ.).

329 *Id*. Moscow City Court was the highest judicial body to review this case.

330 *See* Iarovenko, Shapovalova, & Ismagilov, *supra* note 328.

331 *Id.*; *see* Sud ne priznal sistemu raspoznavaniia lits nezakonnoĭ. Kommentariĭ RosKomSvobody, *supra* note 325 (signaling that the court did not recognize the facial recognition system as illegal under Russian law).

332 Iarovenko, Shapovalova, & Ismagilov, *supra* note 328; *see* Sud ne priznal sistemu raspoznavaniia lits nezakonnoĭ. Kommentariĭ RosKomSvobody, *supra* note 325.

333 Iarovenko, Shapovalova, & Ismagilov, *supra* note 328.

334 *Id.*

335 *Id.*

336 *Id*.

is taking place.[337] The judges agreed with the DIT and the MVD that these processes could not be categorized as those making personal identification possible,[338] and because there is an absence of individuals' identification, videos of citizens cannot be treated as biometric personal data.[339] "Hence, there's no need to obtain a written consent for retention and storage of biometric personal data."[340]

The courts took a highly technical approach, interpreting the facts of the case in such a way as to stress the *technicality* of the process. They did not explore broader ethical and social implications of facial recognition as used by law enforcement. The judiciary does not appear to be seriously concerned with what the societal implication of their current approach will be—anybody can be surveilled at any point in time if strolling on the streets of Moscow. Thankfully in light of the precedent the courts are setting now, such practice will not be viewed as the collection of personal and biometric data *a priori*, no matter the numbers of the CCTV cameras around. Rather, it will be interpreted by the judicial bodies as solely an "exposure [of] similarities in codes and mathematical vectors in the original and analyzed video."[341] This sounds like a rather formulaic and predictable outcome.

There are, however, Russian scholars who support the courts' decisions. They cite to Part 1 of Civil Code Article 152,[342] according to which:

> Publicizing and future usage of citizen's image (including one's photo, or video recording, or art image) is allowed only with the consent of such citizen, but such consent is not required, when: 1) a given image is being used in governmental, societal, or other public interests; 2) image of a citizen is obtained during recording taking place in spaces open for free attendance, or in public events (such as public gatherings, conferences, concerts, shows, sports competitions, and similar events).[343]

In other words, if a petitioner was in the public space next to the State Duma building, which is always surveyed by CCTV cameras, the petitioner can expect that their face would have been recorded. Therefore, their consent

---

337 Irina A. Shashkova, Konstitutsionnye osnovaniia zashchity prava na neprekosnovennost' chastnoĭ zhizni v protsesse ispol'zovaniia tekhnologiĭ raspoznavaniia lits [Constitutional Basis for Protecting Privacy Rights in Light of Facial Recognition Technology Uses], *in* XVIII INT'L CONF. FOR YOUNG SCHOLARS & STUDENTS IN EKATERINBURG at 251 (2020) (Russ.).

338 *Id.*

339 *Id.*

340 *Id.*

341 *Id.*

342 Grazhdanskiĭ Kodeks Rossiĭskoĭ Federatsii Chast' 1 Stat'ia 152 [Civil Code of the Russian Federation Part 1, Art. 152], RULAWS.RU, https://rulaws.ru/gk-rf-chast-1/Razdel-I/Glava-8/Statya-152.1/#:~:text=В%20пункте%201%20статьи%20152.1,только%20с%20согласия%20этого%20гражданина.

343 Iarovenko, Shapovalova, & Ismagilov, *supra* note 328, at 196.

was *not* needed. What is notable in Popova's case is that the recordings of one's face are not categorized as "biometric data."[344] At the same time, this exception to the above-referenced law is overly broad: no consent before collection of personal data is required when one is in pretty much *any* public space in Moscow, a city surveilled by over 200,000 CCTV cameras.[345] Therefore, the possible claims for invasion of individuals' private life or unlawful collection of personal data, once again, are denied by Moscow's judicial system.[346]

III. BYPASSING THE RULE OF LAW IN ADMINISTRATIVE PROCEEDINGS OF POST FACTUM DETENTIONS AIDED BY FACIAL RECOGNITION

One of the parties with decision-making power over personal and biometric law-making in Russia is the President, i.e., President Putin.[347] Official documents and reports addressed to President Putin shed some light on how governmental bodies and civil society leaders envision the nature of challenges, and what they see as a prerogative in the preservation of privacy rights of Russian citizens during the adaptation of facial recognition technologies. This article considers two such communications—one verbal and one written—that took place in 2021. Both communications described concerns from two agencies about the state of human rights within Russia, and especially in connection with the expansion of digital technologies.

In December 2021, the head of Human Rights Counsel of Russia, Valeriĭ A. Fadeev, addressed President Putin during an annual video conference.[348] Fadeev and his colleagues presented a project which conceptualized a "provision of protections of rights and freedoms of persons

---

344 *Id.*

345 *Id.*; Kamphorst*, supra* note 5.

346 Another notable development has emerged in cases dealing with evidence based on video recordings. The Supreme Court of the RF ruled in its recent decisions that it is not necessary to provide expert testimony and special investigation in order to establish the fee amounts punishing administrative violations. The presence of video recording constitutes sufficient evidence for objective resolution of any given case. An attorney Kaloĭ Akhil'gov explains that such Supreme Court decision-making supports a doctrine of "lesser force" evidence in administrative cases, as opposed to criminal ones. For instance, in analogous situation, but in a criminal case, the video recording alone would not be sufficient. Akhil'gov stresses that it means that "administrative violation can be fixated with the help of any technology, and [such technological evidence] alone will be enough." Verkhovnym sudom razresheno nakazyvat' za otsutstvie maski na osnovanii fotomaterialov [*The Supreme Court allowed to punish for not wearing a mask based on photographic materials*], ROSKOMSVOBODA (Dec. 8, 2021), https://roskomsvoboda.org/post/vsrf-razreshil-shtrafovat-po-foto/ (Russ.).

347 *See* Gurkov, *supra* note 243, at 106.

348 Glava SPCH rasskazal Putinu o doklade pro zashchitu prav cheloveka v seti [*Head of Human Rights Counsel Told Putin about the Report Describing Protection of Human Rights Within Digital Space*], RAPSINEWS.RU (Dec. 9, 2021), https://rapsinews.ru/human_rights_protection_news/20211209/307589657.html (Russ.).

and citizens within digital space as well as plans on how to realize them."[349] Fadeev stressed his hope that Putin would enact their project with a Presidential order.[350] Fadeev listed surveillance by social media websites, private companies, banks, mobile operators, as some of the most flagrant human rights violations in digital space.[351] As to procedure, the Counsel informed the President that it had created a specialized working group to address enumerated challenges.[352] Among the listed members of this group were representatives of MinDigits, MinIust, and Roskomnadzor.[353] Igor Ashmanov, a well-regarded specialist in information technologies, was called to lead these prospective projects.[354] Notably, Fadeev referred to the surveillance undertaken by the private sector, stressing its general disregard for the privacy rights of individuals.[355] There was no explicit mention, however, of law enforcement's misuse of personal and biometric data.[356] Yet, the Head of the Counsel alluded to the wording of Russian personal data laws, specifically to protecting "private life, the right to personal and family secret,"[357] while talking about the violations by private companies, social networks, etc.[358]

Another important communication to the President, in writing this time, and relating to law enforcement's uses of facial recognition, was the *Complaint*[359] compiled under the auspices of the OVD-Info attorneys in June of 2021.[360] Understanding of this relatively short, nine-page legal document requires greater scrutiny than that of Fadeev's presentation. It must be noted from the outset that, contrary to the above-mentioned speech presented by Fadeev, this document does not mention the private sector's abuses of personal and biometric data, but rather speaks in great detail about law

[349] *Id.*

[350] *Id.*

[351] *Id.*

[352] *Id.*

[353] *Id.* Ironically, most of these state agencies would be considered by the civil society attorneys as the ones who directly participate in the ways of facial adaptation in Russia as it is now. It is highly unlikely that the latter would see these organs as "impartial bodies." Being closely connected to the Russian government they have been in the position to oversee and affect what's been happening in the realm of personal data collection in Moscow and the country.

[354] *Id.*

[355] *Id.*

[356] *Id.*

[357] *Id.* In Russian: "Pravo na neprikosnovennost' chastnoĭ zhizni, lichnuiu i semeĭnuiu taĭny."

[358] *Id.*

[359] A detailed letter titled "*Complaint*," signed by the OVD-Info attorneys, and addressed to President Putin. The document describes what the attorneys see as violations of law by the police in *post factum* detention cases, and the unjust uses of the facial recognition technology by the police. *See* Complaint from OVD-Info Attorneys, to Human Rights Council under the President of the Russian Federation, *supra* note 50.

[360] *Id.*

enforcement's mismanagement. The document also discusses the subsequent judicial handling of the administrative cases in which the defendants were detained *post factum* with the help of facial recognition.[361] As a whole, the *Complaint* serves as a succinct legal account of the facial recognition usages by law enforcement, and of the subsequent adjudication process by the courts.[362] The document describes what has been taking place in Russia in the area of facial recognition uses by the country's law enforcement agencies.[363]

Some, or possibly all, of the authors of the *Complaint* have professional ties to the OVD-Info, an organization that defines itself and its work as:

> [A]n an independent media human rights project. It is aimed at the ultimate extinction of political persecution in Russia. At the moment, OVD-Info is focused on enforcing particular human rights (freedom of speech and freedom of assembly) and inspecting political repression as well as abuse of the aforementioned rights taking place all over Russia.[364]

The *Complaint* is subdivided into the following three sub-parts, each consisting of a few paragraphs: "Factual circumstances," "Legal foundation," and "WE ARE ASKING."[365] The "Factual circumstances" sub-part lists the names of nineteen defendants, who were accused of administrative violations and were all detained by Russian law enforcement organizations aided by facial recognition cameras.[366] According to the attorneys, these detentions became more widespread, resulting in at least three-hundred forty-seven *post factum* detentions around the country.[367] These detentions happened a few days, weeks, or even months after the public gatherings or demonstrations at hand had taken place.[368]

The "Legal foundation" sub-part introduces the following claims, backed by arguments: (1) facial recognition violates personal data laws; (2) the data in question is being used illegally as the foundation for cases alleging administrative violations; (3) there is no regulation behind facial-recognition-based proceedings; and (4) mass facial recognition violates Article 23 of Constitution, Art. 8 of Convention, and the UN International Pact on Civil and Political Rights.[369] The crux of this sub-part is to highlight

---

361 *Id.*

362 *Id.*

363 *Id.*

364 OVD-INFO, https://ovdinfo.org/ (last visited Nov. 17, 2022).

365 Complaint from OVD-Info Attorneys, to Human Rights Council under the President of the Russian Federation, *supra* note 50.

366 *Id.*

367 *Id.* at 2.

368 *Id.*

369 *Id.* at 3-7.

inconsistencies in how cited laws are being applied and interpreted by the Russian courts, and the lack of transparency in these judicial proceedings.

For instance, the attorneys allude to the earlier-cited law "On Personal Data,"[370] stating that personal and biometric data can only be collected with the person's written consent.[371] No such consent had been obtained in any of the given cases.[372] Further, according to the attorneys, "[s]earch and seizure cannot take place due to signs of administrative offense, but only when there are signs of a severe violation."[373] The authors of the *Complaint* provide three examples of how biometric data of administrative defendants can be used unlawfully as evidence, in violation of Definition of Constitutional Court of the RF, 1998, No. 86-O[374] and Definition, 2005, No. 327-O,[375] in the given administrative proceedings.[376] For instance, in one of the examples, it was reported that photos or videos were obtained by a policeman who had supposedly recognized a certain citizen about whom they provided an official report.[377] In this instance, it is evident that photos or videos might have been obtained from the DIT office or from social media, but the law enforcement agency provides no explanation as to how people in

[370] Federal Law on Personal Data, 2006, No. 152-FZ, *supra note* 297.

[371] Complaint from OVD-Info Attorneys, to Human Rights Council under the President of the Russian Federation, *supra* note 50, at 3.

[372] *Id*.

[373] *Id*.

[374] Opredelenie Konstitutsionnogo Suda RF ot 14 iiulia 1998 g. No. 86-O "Po Delu o Proverke Konstitutsionnykh Otdel'nykh Polozheniĭ Federal'nogo Zakona ob Operativno-rozysknoĭ Deiatel'nosti' po Zhalobe Grazhdanki I. G. Chernovoĭ" [Decision of Constitutional Court of the RF Dated Jul. 14, 1998, No. 86-O "Considering Case of Checking Certain Constitutional Principles of Federal Law on Operational-Search Activity as to Complaint Filed by Citizen I. G. Chernova"] 1998, No. 86-O, CONSULTANT.RU. The given case of journalist Chernova serves as an example of what form violations by the police during their operative work can take place. *Id.* The Judge agreed that Chernova's constitutional rights were violated during search and seizure (operative activities by the law enforcement agents). *Id.* According to the facts of the case, Chernova was to write a critical article about the work of the local law enforcement agency. *Id.* As a result, the local (Volgograd) police black mailed her, by threatening her to publicize details of her private life that they had obtained during search and seizure. *Id.* The Judge has agreed with Chernova that the justice system, and specifically because of how Federal Law "On Operational-Search Activity" was applied to her case, had failed to protect her rights during the span of about three years. *Id.*

[375] Opredelenie Konstitutsionnogo Suda RF ot 6 sentiabria, 2005 g. No. 327-O "Po Zhalobe Grazhdanina Chukova Aznaura Nikolaevicha na Narushenie Ego Konstitutsionnykh Prav Polozheniiami Punktov 1 i 3 Chasti Pervoĭ Stat'i 6 i Podpunkta 1 Punkta 2 Chasti Pervoĭ Stat'i 7 Federal'nogo Zakona "Ob Operativno-Rozysknoĭ Deiatel'nosti" [Decision of Constitutional Court of the RF Dated Sep. 6, 2005, No. 327-O "Considering Complaint by Citizen Chukov Aznaur Nikolaevitch as to Violation of His Constitutional Rights According to Paragraphs 1 and 3 of Part 1 Article 6 and sub-Paragraph 1 of Paragraph 2 of Part 1 of Article 7 of Federal Law "On Operational-Search Activity"], BASE.GARANT.RU.

[376] According to these decisions of what can constitute a violation of operational-search activity preceding detention, if during operational-search activity it is established that the violation is not severe, than according to Article 2 and Part 4 of Article 10, operational-search activity must be stopped.

[377] Complaint from OVD-Info Attorneys, to Human Rights Council under the President of the Russian Federation, *supra* note 50, at 4.

question had been identified.[378] In the *Complaint*, the attorneys underscore that the courts did not investigate this inconsistency, and there was no proof that the evidence presented by the police had been collected lawfully.[379] In all listed administrative cases, the search for detainees-to-be, according to the authors, took place *unlawfully*.[380] Moreover, the search had not been terminated, as per above-referenced laws, once these policemen had the time and ability to understand that the violation did not meet the law's requirement of severity.[381]

Notably, the attorneys quote two influential ECHR decisions in support of their arguments.[382] In *Shimovolos v. Russia*,[383] the ECHR found that surveillance over citizens and collection of their personal data is an intrusion into the right to private life.[384] The *Complaint* highlights in *Shimovolos* that, first, surveillance due to undocumented peaceful protest did not have legitimate backing.[385] Second, government could not invade citizens' private life and collect their personal data even for the purposes of keeping public order.[386] Ultimately, there must be guarantees that there will be no abuses of such powers in cases where surveillance needs to take place.[387] The attorneys stress that there is no legislation in the Russian

[378] *Id.* at 4-5

[379] *Id.* at 5.

[380] *Id.*

[381] *Id.* at 3.

[382] *See* Complaint from OVD-Info Attorneys, to Human Rights Council under the President of the Russian Federation, *supra* note 50, at 6; *see also* Shimovolos v. Russia, App. No. 30194/09, Eur. Ct. Of H.R (2011), HUDOC.ECHR.COE.INT, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-105217.

[383] *Shimovolos v. Russia*, App. No. 30194/09, Eur. Ct. Of H.R. para 64 (2011), http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-105217 ("The Court reiterates that private life is a broad term not susceptible to exhaustive definition. Article 8 is not limited to the protection of an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. It also protects the right to establish and develop relationships with other human beings and the outside world. Private life may even include activities of a professional or business nature. . . . There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life."') (citing relevant case law).

[384] *Id.* at para. 66.

[385] *See* Complaint from OVD-Info Attorneys, to Human Rights Council under the President of the Russian Federation, *supra* note 50, at 6; *see also* Shimovolos, App. No. 30194/09, at ¶ 6 .

[386] *See* Complaint from OVD-Info Attorneys, to Human Rights Council under the President of the Russian Federation, *supra* note 50, at 6; *see also* Shimovolos, App. No. 30194/09, at ¶ 7.

[387] *See* Complaint from OVD-Info Attorneys, to Human Rights Council under the President of the Russian Federation, *supra* note 50, at 6; *see also* Shimovolos, App. No. 30194/09, ¶ 7; *see also* Gaughran v. U.K., App. No. 45245/15, ¶ 97-98 (Feb. 13, 2020), https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-200817%22]}.

Federation to date addressing these concerns.[388] Third, state officials engaged in surveillance must justify the reason for the latter and their intrusion into private life, balancing public and private interests.[389] It is evident that, thus far, Russian courts do not engage in a balancing test of public and private interests, and the guarantee of the former has been mostly played out at the expense of the latter.

The "WE ARE ASKING" sub-chapter summarizes the solutions that the *Complaint* suggests in order to resolve enumerated inconsistencies and guarantee administrative defendants, who are clients of OVD-Info, their rights of due process.[390] The OVD-Info attorneys view impartial oversight of governmental bodies whose officials have access to stored biometric and personal data and making adjudication processes transparent to the public and Russian society at large as the priority. Judging by President Putin's speeches and the administrative law making, such as President's Order "On Development of AI in Russian Federation,"[391] targeting regulation of AI development, the expansion of AI appears to be of the utmost interest to the Russian political elites. The Order established an official National Strategy that would develop:

> [P]urposes and main tasks connected to the development of artificial intelligence in Russian Federation, and also ways in which [AI] can be used for purposes of supporting national interests and realization of strategic national priorities, including in a sphere of scientific and technological development.[392]

In reality, there is a lack of official interest in protecting individuals' privacy rights and other freedoms associated with the advent of AI technologies, specifically when considering the law enforcement and judiciary agencies' treatment of *post factum* detentions. In addition, proactive legislative steps that extend powers of the government and those of the tech industry—as well as judicial backing of the law enforcement facial recognition usages—make survival of the rule of law and that of civil society especially difficult in light

---

388 *See* Complaint from OVD-Info Attorneys, to Human Rights Council under the President of the Russian Federation, *supra* note 50, at 6; *see also* Shimovolos, App. No. 30194/09, ¶ 7.

389 *See* Complaint from OVD-Info Attorneys, to Human Rights Council under the President of the Russian Federation, *supra* note 50, at 6; *see also* Shimovolos, App. No. 30194/09, ¶ 7; *see also* Gaughran, App. No. 45245/15, ¶ 97-98.

390 *See* Complaint from OVD-Info Attorneys, to Human Rights Council under the President of the Russian Federation, *supra* note 50; *see also* Shimovolos, App. No. 30194/09, ¶ 7.

391 Ukaz Prezidenta RF ot 10 oktiabria 2019 g. No. 490 "O razvitii iskusstvennogo itellekta v Rossiĭskoĭ Federatsii" [Order of the President of the RF "On the Development of Artificial Intelligence in the Russian Federation" Dated Oct. 10, 2019, No. 490], GARANT.RU, https://www.garant.ru/products/ipo/prime/doc/72738946/#1000 (Russ.) (last visited Nov. 17, 2022).

392 *See* Tsifrovaia Energetica [Digital Energy], DIGITAL-ENERGY.RU, https://www.digital-energy.ru/trends/analytics/projects/strategy-development-of-artificial-intelligence-until-2030/ (Russ.).

of advancing technologies. The blog authors of the Netherlands-based legal-tech organization, PrivacyPerfect, wrote:

> The more computers can interpret what is happening on the streets, the more meaningful observations can be produced; and the more meaningful observations are made, the larger the inclination will be to attach consequences to those observations. Mass surveillance will turn into mass enforcement. A dangerous road to go down on.[393]

This existential concern, expressed by contemporary European thinkers,[394] can be summarized in the context of countries with lesser pro-individual rights protections and tendencies: the more cameras there are that survey public spaces, the more there are urgent predictions of society's political behavior, and the less likely these behaviors are to be tolerated by the ruling class. In countries like Russia, the government had already taken crucial steps in accumulating and centralizing personal and biometric data. In its massive—or, at least, Moscow-wide—AI experiment, the Russian government started codifying rules involving administrative organizations, an act that is also part of the process of codifying the nature of administrative proceedings dealing with political opposition and civil society at large. The only question to be asked is that by Sergey Sobyanin: "What do[es] the data say?"[395] Or, more specifically, for instance, in case of political demonstrations: when and where will the demonstration take place,[396] and who are the organizers? The contemporary Russian government has sufficient technologies to stifle the opposition even before it takes physical form.

Arguably, due to its authoritarian leanings, and following Agre's and Morozov's arguments discussed earlier, Russia is ahead in the "surveillance capitalism" led game.[397] To follow author and Harvard University Professor

---

393 *Facial Recognition and Data Protection: Will You Collect Happy Points for Good Citizenship in 2025?,* PRIV. PERFECT (July 5, 2019), https://blog.privacyperfect.com/the-privacyperfect-blog/facial-recognition-and-data-protection.

394 *Id.*

395 Zakharov, *supra* note 114.

396 *Id*. For example, this can be deduced from social media posts, publicly uploaded faces of people, or statements made in social media chats and direct messages.

397 *See Shoshana Zuboff: Surveillance Capitalism and Democracy*, *supra* note 13; *see also* SHOSHANA ZUBOFF, *About,* https://shoshanazuboff.com/book/shoshana/ (last visited March 27, 2023). Professor Zuboff is Charles Edward Wilson Professor Emerita at Harvard Business School and a former Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard Law School. *Id.* She has published numerous articles and books on mechanization of human society with an advent of new digital technologies. *Id.* In her most recent work and research Professor Zuboff "synthesizes years of research and thinking in order to reveal a world in which technology users are neither customers, employees, nor products." *Id.* "Instead they are the raw material for new procedures of manufacturing and sales that define an entirely new economic order: a surveillance economy." *Id.*

Shoshana Zuboff's formula:[398] Moscow's personal data-based "experimentation" involving facial recognition surveillance started, unhindered by laws, as early as 2001.[399] Russia's civil society and rule of law activists are the only parties who have seriously questioned both the uses of facial recognition surveillance by law enforcement and the nature of legal procedures in administrative cases involving the novel technology. Relevant judicial interpretation in Russia are at the beginning stages, for the capital's courts do not view individuals' personal and biometric data—if collected in public spaces—as personal and biometric data that warrants protections under Russian law.[400] Some Russian lawyers and experts, such as Darbinian, Koroteev, and Gainutdinov, have demonstrated that the Russian government is building a state monopoly over biometrics, mainly by centralizing and unifying citizens' personal data and making it accessible to various governmental agencies, which, in turn, are becoming less transparent and fundamentally lack any meaningful oversight from non-government parties.

A. Future Governmental Predictions and Current Governance Made Possible by Personal Data Collection

Andrew Ferguson, a Professor of Law at American University Washington College of Law, says that governments that utilize new facial recognition technologies, including China and the U.S., "now have the capability to identify people and patterns, and . . . [to] show the association about where you go and why you are going there."[401] He argues that this "really change[s] the relationship between citizens and [their] governments."[402] Similarly, in Professor Zuboff's theory of "surveillance capitalism," data is equivalent to knowledge, and knowledge is directly connected to power.[403] Professor Zuboff argues that, "extreme

[398] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (1st ed. 2019). On a more pragmatic note, Professor Zuboff argues "that knowledge about individual behavior—derived from personal and biometric data—itself is power." *Id.* According to Zuboff, the balance of power in citizens v. tech, including big tech and AI industries, as well as the governments, has shifted in directions that are detrimental for individual rights, particularly, privacy rights. *Id.* Average citizens' knowledge about meta data derived from their personal data is limited or non-existent. *Id.*; *see also Shoshana Zuboff: Surveillance Capitalism and Democracy*, *supra* note 13 (Zuboff's talk on "surveillance capitalism" and its derivatives).

[399] Gainutdinov & Koroteev, *supra* note 45.

[400] *Id*.

[401] VICE News, *How China Tracks Everyone*, YOUTUBE (Dec. 23, 2019), https://www.youtube.com/watch?v=CLo3e1Pak-Y.

[402] *Id.*

[403] *See* Fortune Magazine, *Surveillance Capitalism In Today's Digital Age*, YOUTUBE (Nov. 18, 2019), https://www.youtube.com/watch?v=2WYjZo9kNYI.

concentrations of knowledge produce extreme concentrations of power; that what we can do is now no match for what can be done *to us*."[404]

The Moscow municipal government only appears to be transparent in its communications with the public about the importance of aggregate personal data collection, preceding the establishment of a "smart city."[405] As expected, according to city officials' descriptions of smart city planning, everything is being done for the improvement of everyday lives of regular Moscovites. As Moscow Government Chief Information Officer, Artem Ermolaev, notes: "We weren't fighting for an improved place in the rankings, but we were fighting for the people's perception of Moscow by the citizens."[406] Ermolaev and his colleagues also want to "move all government services to AI."[407] For instance, such is Moscow's official framing, which states:

> In about 2015, the [Moscow] Mayor Office had decided that it was time to create more inclusive systems that would use data from different sources. The task of such systems is not to store one kind of [personal] data, such as permissions to build housing or record marriage certificates. They, like AI from science fiction movies, must answer complex questions and be able to predict the future.[408]

City officials appear to be transparent *vis-à-vis* public about their plans to incorporate capabilities of AI in governance decision-making having to do not only with the present, but also with what can take place in the future.[409] For instance, in 2015-2016, the Department of Territorial Development of Moscow[410] was delegated powers by the Mayor's Office to oversee the "emergence, monitoring, prediction, planning of actions and making decisions in situations, connected to realization of governmental politics in the sphere of territorial governance."[411] Zakharov compares such powers of Moscow's Department of Territorial Development, rooted in vast collections

---

404 *Id.*

405 We can deduce that the Moscow government is far from transparent in its uses of novel technologies judging how in Popova's proceedings the DIT and the MVD avoided acknowledging that they were using facial recognition technologies to identify protesters. *See* Sud ne priznal sistemu raspoznavaniia lits nezakonnoĭ. Kommentariĭ RosKomSvobody, *supra* note 325.

406 Jonathan Andrews, *Moscow embraces digitization to improve the standard of living,* AI FOR GOOD, https://aiforgood.itu.int/moscow-embraces-digitization-to-improve-the-standard-of-living/.

407 *Id.* (stating that "[s]eventy percent of crimes are investigated using CCTV"); *see also* Novaya Gazeta, *supra* note 54 (Roskomsvoboda attorney, Darbinian, voices his skepticism about such statistics, implying that average citizens do not know what crimes the government refers to, and how valid these numbers are).

408 Zakharov, *supra* note 114.

409 *Id.*

410 *See* Departament Razvitiia Novykh Territoriĭ Goroda Moskvy, MOS.RU, https://www.mos.ru/drnt/contacts/ (Russ.).

411 Zakharov, *supra* note 114.

of data, to those possessed by the U.S. company Palantir,[412] which serves American law enforcement while collecting "vast amounts of data from different sources in order to find in them signs of possible crimes or terrorist acts."[413]

On a societal level, Moscow's Department of Territorial Development will use collected data and AI science to predict future realities based on "publications in internet-based media, statements on social media, street surveillance and other types of data."[414] Given the extent of control wielded by Russian authorities over the domestic Internet, it becomes evident that the government is starting to utilize science, or predictions of AI algorithms derived from large data sets, to set its governance agenda for the future as well.

The quality and veracity of contemporary AI science, on which such predictions of the future are based,[415] is rooted in the facial recognition data continually harvested by the Moscow city government.[416] It is fortuitous that the government now has access to a variety of citizens' data, coming from the multitude of state-sponsored websites with different operational objectives and, therefore, collecting different categories of Moscovites' personal information:

> [T]he contractor must develop and implement on mos.ru [Moscow city portal] a procedure for saving "a reference photo from a user profile to an additional gallery for the automatic registration of video indexing scenarios (PARSIV) of the Single Data Storage Center (SCDC) of the Main Directorate of the Ministry of Internal Affairs in Moscow. [417]

And:

> PARSIV, in fact, is a channel through which police can connect to city's network, in order to look for criminals. Mos.ru itself is integrated with the "System of distance-based education," "Unified mobile platform of

412 *See* Frances, *Palantir Technologies*', SOFTWARE ANALYST NEWSL. (Dec. 17, 2020), https://investianalystnewsletter.substack.com/p/palantir-technologies-americas-most. Palantir counts among its clients the CIA, FBI and NSA. *Id.* The company, by "build[ing], and successfully integret[ing] large-scale, disparate data in a cohesive and coherent manner . . . give[s] insight and drive[s] actions" helping with "counterterrorism, human trafficking, disaster response and high-profile criminal cases." *Id.*

413 Zakharov, *supra* note 114.

414 "Rostekh" razrabatyvaet neĭroset' dlia predskazyvaniia massovykh besporiadkov ["Rostekh" is Developing Neuro-network to Predict Mass Protests], ROSKOMSVOBODA (Nov. 30, 2021), https://roskomsvoboda.org/post/rosteh-predskazhet-besporyadky/ (Russ.).

415 *Id.* (where Roskomsvoboda's article describes anti-religious protests and "antipolice behaviors," as well as analysis of the behavior of those participating in demonstrations, and directions in which crowds move during demonstrations).

416 TIME NEWS, *Moscow Mayor's Office Will Hand Over Photos of Mos.ru Users to the Police* (Oct. 13, 2021), https://time.news/moscow-mayors-office-will-hand-over-photos-of-mos-ru-users-to-the-police/.

417 *Id.*

> Moscow," portal "Active citizen," Single Medico-Informational and Analytical System of Moscow (SMIAS) . . . and others.[418]

As such, Moscow's city government and political elites appear to know that, if we view their administrative techniques in light of Professor Zuboff's "surveillance capitalism" model, it is not only the quantities of data that matter, but also their variety.[419] The more expansive variation of the data, the better; because the "[s]cale is not enough," what is needed is also the "scope—varieties of data."[420]

Considering the metro area population size in Moscow—over twelve million according to recent estimates[421]—and legal, bureaucratic, and high-tech systems working in tandem to achieve common goals of data collection, analysis, and centralization, Moscow is becoming a well-programmed "experimentation" ground. This is exactly what Mayor Sobyanin wants to achieve administratively with the help of Moscovites' data collection, evident in his statement: "Give me [Moscow] in an online mode."[422] Moscow "Smart City" will eventually become as technologically advanced as Singapore, for this is what is desired by those who are orchestrating the "smart chapter" of its existence. Yet, it will also resemble a highly controlled society, rooted in AI science.

B. Administrative Detentions and their Post Factum Nature

> *"Someone must have slandered Josef K., for one morning, without having done anything truly wrong, he was arrested."*
> - Franz Kafka, The Trial, 1925

In addition to future endevours, the Russian government also seeks control over the present via AI-based applications by law enforcement agencies.[423] Some experts have noted that "[a]fter demonstrations to release [Alexei A.] Navalny,[424] [facial recognition technologies] started being used

---

418 *Id.*

419 *See* Fortune Magazine, *Surveillance Capitalism In Today's Digital Age*, *supra* note 403.

420 *Id.* Prof. Zuboff's comments on the nature of "surveillance capitalism" economies.

421 *Moscow, Russia Metro Area Population 1950-2022,* MACROTRENDS, https://www.macrotrends.net/cities/22299/moscow/population#:~:text=The%20current%20metro%20area%20population,a%200.5%25%20increase%20from%202019 (last visited Nov. 28, 2022).

422 Moskva pod kolpakom "bol'shikh dannykh" "Umnyĭ gorod" mera Sergeya Sobyanina sledit za moskvichami i gostiami stolitsy cherez seti, WiFi, videokamery [Moscow and big data "Smart City" of Mayor Sergey Sobyanin watches over Moscovites and guests of the capital with the help of networks, WiFi, video cameras], COMPROMAT.RU, https://www.compromat.ru/page_41190.htm (Russ.).

423 Andreĭ Zakharov & Vladimir Dergachev, Protestuyushchikh nakhodit moskovskiĭ "Starshyĭ brat." Pridut li ko vsem? ["Big Brother" Finds Those Who Protest. Will They Come To Everyone?], BBC (Feb. 9, 2021), https://www.bbc.com/russian/features-56000110 (Russ.).

424 *See* Pjotr Sauer, *Alexei Navalny in 'critical' situation after possible poisoning, says ally*, GUARDIAN (Apr. 14, 2023), https://www.theguardian.com/world/2023/apr/14/alexei-navalny-in-critical-situation-after-possible-poisoning-says-ally ("Alexei Navalny, Russia's most prominent opposition

for the first time to make participants accountable in administrative proceedings."[425] Notably, Russians rallied in support of the jailed Navalny in more than one hundred cities in January of 2021, culminating in the "biggest protests in the nation since at least 2017."[426]

Russian attorneys assisting demonstrators who were detained days, weeks, and sometimes months, after certain protests had taken place, refer to such detentions as "*post factum.*"[427] These detentions have been described as *post factum* not only because they can happen much later after the protest, but also because they can take place at a person's domicile, where they work or study, or while an individual enters or exists a subway station.[428] The authors of the OVD-Info Report describe such practices by the police in "Summoning or bringing in [the defendants] to a police station."[429] Likewise, these detentions are highly arbitrary in regard to the time and place of their occurrence.[430] "I consider it to be a form of psychological pressure," said Oleg Ovcharenko, a journalist with the independent *Echo of Moscow* radio station,[431] when police showed up at his home six days after his involvement with a protest.[432] Attorneys from the OVD-Info highlighted the arbitrary nature of these detentions in the aforementioned *Complaint* to the President:

> 1) Policemen can prepare protocol at any point in time, according to their desires, which allows for manipulation of legal process; it makes [such process] arbitrary; 2) the context is not considered during facial recognition recordings, as a result, passers-by get detained, as well as journalists who are there because of their professional duties; 3) there is no judicial oversight and no possibility to appeal.433

The uses of facial recognition software by the police to control the opposition are as haphazard as arrests policemen make during the protests themselves.[434]

politician, has been grappling with severe stomach pain in jail that could be the result of slow-acting poison, a close ally said on Friday.").

425 Zakharov & Dergachev, *supra* note 423.

426 Anton Troianovski, *Pro-Navalny Protest Photos: Wave of Anger Rolls Across Russia*, N.Y. TIMES (Jan. 25, 2021), https://www.nytimes.com/2021/01/24/world/europe/photos-russia-navalny-protest.html?action=click&module=RelatedLinks&pgtype=Article.

427 *See* OVD-INFO REPORT, *supra* note 49 ("OVD-Info is aware of the prosecution both after two days and after more than five months after an event.").

428 *Id.*

429 *Id.*

430 Complaint from OVD-Info Attorneys, to Human Rights Council under the President of the Russian Federation, *supra* note 50.

431 Amy Mackinnon, *Russia's Surveillance State Struggles to Wean Itself Off the West*, FOREIGN POL'Y (May 24, 2021), https://foreignpolicy.com/2021/05/24/Russia-surveillance-technology-western-companies-facial-recognition/.

432 Complaint from OVD-Info Attorneys, to Human Rights Council under the President of the Russian Federation, *supra* note 50.

433 *Id*. at 5.

434 *Id.*

For instance, during the January 2021 protests on Pushkin's Square in central Moscow, police arrested some protestors while letting most go—arrests executed in a seemingly arbitrary manner.[435] Such actions have an effect of applying psychological pressure on the public, and further produce a sort of dampening effect on civil society in general: one never knows whether one will be arrested, or when and where—a truly Kafkaesque scenario.

The arbitrary nature of the above-referenced arrests is an important characteristic of a larger dynamic at work. Once again, these circumstances are directly related to the idea of knowledge examined by Professor Zuboff in "The Age of Surveillance Capitalism."[436] Police, the DIT, the MVD, and scores of other governmental agencies are the ones who "know," or have resources to "know" where the protest will take place—thanks to the AI's analysis of social media, cell phone communications, etc.—how many people can attend, how to best approach the desired outcome in preventing the political opposition. This knowledge is powerful even if it is not based on concrete facts (i.e., how many people to arrest right at the action versus how many *post factum* detentions to undertake). The fact remains that the arbitrary nature of such decisions cause individuals—those who have the will to protest the prevailing political order—to live in a perpetual state of precarity and uncertainty.

The constant supply of information from Moscow's array of CCTV cameras makes law enforcement's observation of those who oppose it, and everyone else who happen to be in the vicinity of a protest, also bear the frightening possibility of being punished by the government, regardless of whether such punishment ever takes place in a physical form. The presence of the many CCTV cameras throughout Moscow is *essential*. It is analogous to the presence of one well-positioned guard in Jeremy Bentham's highly utilitarian Panopticon prison.[437] The effect of a government's "all-seeing" eye, accomplished by the surveillance system of 200,000 CCTV cameras, achieves the same goal as had been desired in the construction of the Panopticon: to make citizens behave as they are expected to behave, with the least resistance to the prevailing order.[438] The uncertain nature of arrests,

[435] *See* Troianovski, *supra* note 426.

[436] *See Shoshana Zuboff: Surveillance Capitalism and Democracy*, *supra* note 13.

[437] Philip Steadman, *Samuel Bentham's Panopticon*, 14 J. BENTHAM STUD. 1 (2012). In Bentham's Panopticon, only the prison inspector could see and observe prisoners at any point in time—prisoners did not know whether they were being watched. *Id.* Hence, the essence of the Panopticon's architecture served the role of a highly utilitarian structure to allow the guards to watch while being invisible, and to enact discipline with the minimum possibility of opposition. *Id.* On a larger, more philosophical scale, the Panopticon was first of all a structure that served as a succinct visual metaphor of power relations within a given social unit—the prison. *Id.* The guards would be at the apogee of their power, while the prisoners never knew whether they were being watched (i.e., surveilled); therefore, they had to assume that they always were, and had to behave accordingly. *Id.*

[438] *Id*.

occurring arbitrarily in time and space, also possesses features of a public performance. Such public displays of the state's power take place unbeknownst to the detained, and at the same time, show to the onlookers the grave repercussions of opposing the regime—i.e., that all onlookers themselves are potential detainees.

IV. CONCLUSION

"Face recognition is too powerful to be secret."
- The Perpetual Line-Up Project[439]

Alan Westin defined privacy in his 1967 book, "Privacy And Freedom," as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated."[440] Westin's definition of such a complex and philosophically multi-layered concept as privacy is built on at least these three essential pillars: (1) the existence of individuals who possess the choice and will to claim privacy rights or to point to their violations; (2) these individuals possess powers and faculties to decide the timeliness of when their personal information is to be "communicated"; and (3) the individuals can decide the manner in which their personal information is to be "communicated," as well as the quantity of the information.[441] As such, privacy provides individuals and groups with a preservation of their autonomy, a release from role-playing, a time for self-evaluation, and for protected communications.[442]

Westin's meaning of privacy, however, loses its viability in a world where human experience and such a personal and easily identifiable part of the human body as one's face no longer belong to their biological owners (i.e., the individuals). In countries such as Russia—where the power exerted by governmental agencies is felt especially acutely—Westin's definition of privacy loses its meaning in Internet and media regulation, in AI rapid utilization, in infrastructure of smart cities being built, and therefore, in the reality of everyday Russian life. For example, Russian individuals' claims for protection of their biometric data in administrative proceedings have not been honored thus far.[443] In other words, Russian citizens are unable to raise a privacy violation claim in these situations. For the most part, citizens are also unable to control when, how, and in what quantities the information

[439] Clare Garvie, Alvaro Bedoya, & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEORGETOWN L. CTR. ON PRIV. & TECH. at 65 (Oct. 18, 2016), https://www.perpetuallineup.org/.

[440] Alan F. Westin, *Privacy and Freedom*, 25 WASH. & LEE L. REV. 166 (1968).

[441] *Id*.

[442] *Id*.

[443] Complaint from OVD-Info Attorneys, to Human Rights Council under the President of the Russian Federation, *supra* note 50.

about them is being collected, as well as in what manner it is being analyzed and utilized by other parties, such as the government and market entities. According to the Russian judiciary, no protections are needed because surveillance takes place in public spaces, and hence, one's face is not one's biometric data.[444] Further, current decisions by Russian legislature and judiciary affecting adaptation of facial recognition technology will also define citizens' quality of life for generations to come. If we consider a more metaphysical realm of the political power dynamics in Russia, the expectations of roles of various actors that are being established now will mold individuals' privacy rights *vis-à-vis* the state, market entities, and the AI industry.

Importantly, Russian civil society and its legal advocates are not hesitating to strongly question the negative consequences of such novel technology and its impacts on individual liberties. On the contrary, their familiarity with and critical assessment of the authoritarian leanings of Russia's political elites provide advocates with undeniable advantages for forming educated, professionally based projections of some of the worst-case scenarios in adaptations of AI-based technologies in Russia, and the world. It is true that the spread of facial recognition technologies appears to be taking an accelerated route in Russia due to an absence of impartial oversight and the inability of the country's civil society to protest its negative consequences on individual freedoms. However, Russian civil liberty advocates can play an important role in educating the broader Russian public—as well as the global community—as it relates to the serious concerns and potential negative impacts of AI technologies' imminent expansion.

Elena Shakhova,[445] Chairperson of Citizens Watch, noted in her interview a curious linguistic nuance of the Russian "police laws," stating that "the language we use affects our consciousness."[446] Shakhova pointed out that the Russian police are oftentimes referred to as "the police forces"[447] in legal texts,[448] strengthening the idea that the agency stands separate from the society, and, in fact, protects *itself* and the State from the society. "This is quite ironic," Shakhova continued, "because the police is supposed to

---

444 *Id.*

445 Elena Shakhova is Chairperson of Citizens Watch, "a human rights organization in St. Petersburg that was established in 1992 with the aim to assist in instituting parliamentary and civic control over the police, the security service, and armed forces, and to help prevent violations of the constitutional rights of people living in Russia by these governmental agencies." *See Case History: Elena Shakhova*, FRONTLINE DEFENDERS, https://www.frontlinedefenders.org/en/case/case-history-elena-shakhova (last visited March 27, 2023).

446 In Russian: "Iazyk vliiaet na soznanie." Interview with Elena Shakhova, Chairwoman, Citizens Watch, in St. Petersburg, Russia (Feb. 2014) (on file with author).

447 *Id.* In Russian: "politseĭskie sily."

448 *Id.*

safeguard rights and laws in the interests of civilians."[449] This observation paralleled that of Lyudmila Alekseyeva[450] of Moscow Helsinki Group[451] ("MHG") who stressed in her "Practice of Freedom" Talk at Sakharov Center in February of 2014, that in Russia "the power not so much protects the civilians, as it protects itself against those civilians."[452] In other words, political power dynamics are such that those who govern do not do so with citizens' interests in mind. Therefore, Russian citizens exhibit distrust *vis-à-vis* those in power. Namely, both Shakhova and Alekseyeva, being well-regarded Russian civil society leaders, worked with and spoke of violations against citizens' human rights, committed by the law enforcement agencies, and disregarded by the domestic judiciary.

As much as Agre's "amplification"[453] model is coming to fruition in Russia, and facial recognition technologies are becoming some of the most sophisticated surveillance tools in the hands of the political elite intending to control the opposition and Russia's civil society—human rights and privacy advocates are aware of what has been taking place, and how these novel technologies have been utilized. It may be that presence of such civil society advocates as Agora, OVD-Info, Roskomsvoboda, and independent media channels, is what provokes the political regime to introduce and implement facial recognition technology in Russia as quickly as they have done in the absence of adequate lawmaking thus far. And, as this article has demonstrated, this regime has not done so in the interests of individuals and those of the civil society.

Within the current legal landscape, there is a heightened urgency around concerns regarding the use of facial recognition, as this novel technology will be a precursor to many other, more complex AI-based technologies that can exist, improve, and proliferate based on collection of

449 *Id.* In Russian: "zashchita prav i zakonov v ineteresakh grazhdan."

450 Lyudmila Alexeyeva, *"Grandmother" of Russia's Human Rights Movement, Dies at 91*, N.Y. TIMES (Jan. 9, 2018), https://www.nytimes.com/2018/12/09/world/europe/lyudmila-alexeyeva-dead.html. Lyudmila Alexeyeva is an important Russian human rights activist. *Id.* She saw herself as the "grandmother" of the Russia's human rights. Alexeyeva was the co-founder of the Moscow Helsinki Group (MHG), an influential NGO. *Id.*

451 *See* Moskovskaia Helsinskaia Gruppa [Moscow Helsinki Group], https://www.mhg.ru/index.php (last visited Feb. 19, 2023).

452 Lyudmila Alexeyeva, "Practice of Freedom" Talk, Sakharov Center, Moscow, Russia (Feb., 2014) (on file with author).

453 If we apply Agre's "amplification" model to the adaptation of facial recognition technologies in Russia, it is evident that the social forces that had existed prior to the advent of these novel technologies continue in the same direction as before: i.e., a strong authoritarian crack-down on political dissent, civil society, and autonomy of individuals in general. According to the model, just as with the Internet, nothing qualitatively new emerged with the advent of facial recognition technologies, but the institutions possessing agency to develop such technologies (i.e., the AI industry) and to implement and control them (i.e., the government in case of Russia) utilize these novel technologies in their own interests, while presenting them as a panacea to all kinds of societal wrongs.

personal and biometric data. It is crucial to remain aware that the first intended uses of novel technologies are not the only uses. Justices, lawyers, civil liberties advocates and other professionals participating in the creation and interpretation of laws, arguably, must face more grave challenges than those encountered by the peers of Samuel Warren and Louis Brandeis when the two protested proliferation of instantaneous cameras and the widespread circulation of newspapers in the United States.[454] Such protest resulted in a seminal 1890 article "The Right to Privacy."[455]

Thankfully, some important decision-makers in proceedings related to facial recognition in the U.S. have recognized that the capture of biometric identifiers—such as face prints—permanently belong to a human body and unlike other personal identifiers (e.g., name or address) cannot be changed.[456] Rather, they are as unique as is possible, and this uniqueness is one of the main reasons that the growing collection of biometric data poses "greater risks to an individual's security, privacy, and safety"[457] than had been the case when such precise technologies did not yet exist. Members of Russian civil society—such as the OVD-Info, Agora, and Roskomsvoboda—have accomplished a great deal by identifying the nature of what is happening in terms of AI-based facial recognition technology, and by questioning the approaches to facial recognition of law enforcement and the judiciary. Their vision and expertise can be instrumental in scenarios where the adaptation of these technologies has yet to progress so quickly. Ironically, as hastily as the Russian political elites begin to utilize AI to predict possible opposition, simultaneously, civil society is becoming better equipped at predicting the behavior and tactics of the authorities too. Possibly, more than ever before, with Russia's exit from the ECHR and the closure of Memorial International, Russian civil society needs support from its international colleagues involved in similar work with a common mission: protecting people from wrongful government intrusion by use of modern technology.

---

454 Leah Burrows, *To be Let Alone: Brandeis Foresaw Privacy Problems*, BRANDEISNOW (Jul. 24, 2013), https://www.brandeis.edu/now/2013/july/privacy.html.

455 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193-220 (1890); *see* Burrows, *supra* note 454.

456 ACLU, *Illinois Court Rejects Clearview's Attempt to Halt Lawsuit Against Privacy-Destroying Surveillance* (Aug. 27, 2021), https://www.aclu.org/press-releases/illinois-court-rejects-clearviews-attempt-halt-lawsuit-against-privacy-destroying.

457 *Id.*