Data (De)colonization:
Case of the "Safe City" Project in Belgrade

LUND
UNIVERSITY

Petar Korać

August 2021

Master of Science Programme in Development Studies

Department of Sociology

Supervisor: Carl-Göran Heidegren

Abstract

In my thesis, I follow the argument of the authors belonging to the school of decoloniality, who explore the phenomena of coloniality of power outside of historical colonialism. This gives me the freedom to look through decolonial lances into phenomena of undergoing colonization through data. By following the idea that data colonialism is a reality, not just a metaphor, I examined how data colonialism occurs in the "Safe City" project in Belgrade. Furthermore, I analyzed how different actors are influenced by data colonialism and how a group of activists challenges the ongoing top-down process of datafication. I used a single case study research design, using documents and articles on the internet as secondary data sources. Primary sources were semi-structured interviews with experts and advocates for digital rights who are challenging datafication. Results indicate that colonization can happen if and when datafication begins through the centralized infrastructure for biometric data extraction and that beneficiaries of this process are most likely to be found in the political elite and private companies. At the same time, decolonization is practiced by activists through research and data collection, raising awareness, and community mobilization.

Keywords: *decoloniality, data colonization, datafication, big data, biometric surveillance, Safe City*

Word count: 20 651

Acknowledgment

Two people deserve special acknowledgment. First of all, I have to thank my partner in life 李俊杰 (Junjie Li) for the incredible emotional and psychological support last eight months. Second, Nela, thank you for your patience and support, from the initial idea to the last hours of work on this thesis. This work would not be the same without you.

In the last writing stage, comments and help regarding language stylization received from Asja and Michalis will forever be part of this document and our friendship. Carl-Göran Heidegren, thank you for your understanding and last comments, which made my submission decision definite.

I must acknowledge the enormous importance of the activists of the *Hiljade kamera* initiative and *Share Foundation* in Belgrade. Their work and dedication to digital rights and freedoms inspired me to write this thesis and made conducting interviews easier than I expected, thanks to their patience and understanding.

Thanks to *The Swedish Institute* (Si) and *The Foundation for Young Talents – Dositeja*, I have been able to study at *Lund University*, learn the Swedish language, meet incredible people, and finally, deliver this thesis in front of you.

Because I know that my sister and brother will not read these pages, there is no point in thanking them in this way. Instead, I want to mention my niece and nephew, Helena and Kosta, who should know I had them and their generation in mind when writing this thesis.

Finally, I would like to dedicate this work to my mum. Her departure during the work on my thesis caused a lot of pain, but her beautiful voice that will stay with me forever, made me finish it. Just as all other good things I did and will continue to do.

Table of Contents

Abbreviations

AI – Artificial Intelligence

BRI – the Belt and Road Initiative

CCP – the Chinese Communist Party

CCTV – Closed-Circuit Television

CDS – Critical Data Studies

CEEC – Central and Eastern European Countries

Commissioner – Commissioner For Information Of Public Importance And Personal Data Protection

DPIA – Data Protection Impact Assessment

EDRi – European Digital Rights

EU – The European Union

FR – Facial Recognition Technology

GDPR – General Data Protection Regulation

GPRC – The Peoples Republic of China

GRS – The Government of the Republic of Serbia

Huawei – Huawei Technologies Co., Ltd.

ICT – Information and Communication Technologies

IoT – Internet of Things

LPDP – Law on Personal Data Protection

MIARS – Ministry of Internal Affairs of Republic of Serbia

NIT – Nations in Transit

PRC – People's Republic of China

SNS – Serbian Progressive Party

UID – Unique Identifier

1. Introduction

Big data truly is the buzzword. We see and hear different interpretations and discourses of its importance for economic growth and development (The Economist, 2017; Schwab, 2016). This optimistic narrative is often characterized by the expression "data is the new oil" first used by Clive Humby in 2006 (Arthur, 2013). The importance of big data for contemporary society is also often analyzed in light of the emergence of massive surveillance (Ferguson, 2019) and the expansion of new technology such as artificial intelligence (from now on: AI) (Hydén, 2020; Giacaglia, 2019). Massive changes in society due to the emergence of big data and digital technology are often referred to as revolutionary (Kitchin, 2014). Big data, along with the industry of the fourth industrial revolution, are growing at a never-seen speed. AI grows 300 times on the Industrial Revolution scale (The World Wide Web Foundation, 2017: 4), while the amount of data in the world doubles every two years (Gallagher, 2020).

However, big data is not just a neutral phenomenon. It is a socio-technical phenomenon that mediates almost all indirect interpersonal relations in today's world. It is one through which new forms of sociability emerge, in the form of "data relations" (Couldry & Mejias, 2019a). Also, big data is the main element of emerging surveillance capitalism in which "behavior surplus" is gained through the extraction and accumulation of "behavioral data" through surveillance of our everyday life and "behavioral modification" (Zuboff, 2019a, 2019b). For Couldry & Mejias (2019a), big data is a crucial resource for emerging social relations in the form of data colonialism, announcing a new form of capitalism and social totality. In this new form of social order, everything is part of the system and susceptible to scrutiny and surveillance by the state and corporations (Couldry & Mejias, 2019b: 346).

For Yuval Noah Harari (2018), big data is becoming the most crucial asset that results in a power struggle for its control. The concentration of data in one place and positioning its control and analysis in the hands of the few might lead to the situation in which democracy becomes a "puppet show" ending up in fascism (Harari, 2018). According to Harari (2018), the most significant handicap of the authoritarian regimes of the twentieth century was that they tried to make all the decisions on the central level while not having technology that would allow an analysis of information on the mid-level. Today, with big data and technology for its analysis, more data in one place means more accurate predictions and more efficient analysis. Therefore, Harari (2018) calls for improvements in distributed data processing to be as efficient as the centralized. Couldry and Mejias (2019a: 157) perceive data's role in connecting all parts of the social system, which is a complete realization of the modern ideal of rationalization of society and totalization of social order. A new phase of modernity, which is manifested through digital and big data revolution phenomena, is based on data epistemology as the central point of knowledge and connection.

The socio-technical system behind the personal data collection and processing is often untransparent to the public and often conceptualized as the "black box" (Pasquale, 2015). We usually get an insight about the depths and scales of intrusion in our lives, based on data misuse, through the whistleblowers and insiders. For example, revelations made by Edward Snowden about the PRISM program gave us an insight into the capabilities of the National Security Agency (NSA) to spy on almost anyone with access to the internet through the metadata gathered by the convergence of state and corporations (Price, 2014).

However, the disruptive effects of big data and discussion about it are framed according to Western criteria. These discussions are only partly accustomed to the social context of the South. "Big Data from the South" initiative is advocating for the creation of more contextualized knowledge about the negative implications of big data

epistemology in the South, before all its implications on freedom and rights of the people.

The central question of the politics of data is who controls the process of datafication and who benefits from it. Although today, there are fronts that aim to control these processes, such as narrative around privacy and antitrust, the difference between those who can manage these processes varies across populations (Zuboff, 2019a; Couldry & Mejias, 2019a). That is why we should pay attention to those regions and countries shaped by unequal relations, economic marginalization, and fragile democracy (Milan and Treré, 2019).

Thus, my focus on specific processes in the Global South will allow me to analyze how big data is transforming the relations between state and citizens and the consequences of this "colonization of the lifeworld" through data (Thatcher et al., 2016: 991). In this thesis, I will examine the relationship between power and data, focusing on how the specific form of epistemology is used for extracting information from people for power and control (Ricaurte, 2019). Through data, we are becoming susceptible to the matrix of power/knowledge relations which are a particular form of the colonial way of governing through the categorizing, classifying, and correlating emanating in the form of data colonialism (Couldry & Mejias, 2019a; Quijano, 2007). Coloniality is thus a consequence of modern knowledge, which is in the contemporary world made possible through data. I will present how big data is not a neutral process of knowledge creation (Kitchin, 2014) but rather phenomena shaped by power and profit, in the case of the "Safe City" project in Belgrade. Also, I will demonstrate how datafication, as a specific regime of knowledge through data, is imposed, legitimized, but also contested by social activists.

1.1. Aim and Research Questions

The aim of this thesis is twofold. Firstly, I will apply theoretical insight from decolonial theory and Critical Data Studies (from now on: CDS) on the case of "Safe City" project in Belgrade to provide new contextual insights and perspectives that can potentially enrich the concept of data colonialism. The second aim is to join a broader scholar and activist attempt of "rethinking relations to ongoing coloniality" (Couldry & Mejias, 2019a: 80) in the era of big data to end colonization through data.

Couldry and Mejias (2019a) extensively discussed the concept of data colonialism and laid the foundation for its further use in academic writing. However, my impression is that it is almost strictly linked to the discussion regarding the online "platform" economy and society. At the same time, some other empirical phenomena, whose primary purpose is not capital gain, are left behind in their analysis and not subsumed under the phenomena of data colonialism. Therefore, this thesis is an attempt to extend the use of the theoretical concept of data colonialism to the case of "Safe City" project in Belgrade to extend conclusions to other similar projects. Furthermore, my intention is not just to demonstrate how the process of data colonization unfolds in the mentioned project in Belgrade but also to provide insights about how it is challenged and contested by the digital rights activist of the "Hiljade kamera"[1] initiative.

I will try to provide answers to the following research questions:

> **RQ1:** How can colonization through data potentially occur in the case of the "Safe City" project in Belgrade?

[1] In literal translation, "Hiljade kamera" means" Thousands of cameras". Initiative and its members also use other names and ways to represent themselves in public and social media, such as "#hiljadekamera" and "hiljade.kamera". However, I have decided to use "Hiljade kamera" when referring to them and their work in my thesis.

RQ1.1: How might the extraction of data influence different social actors?

RQ2: How the "Hiljade kamera" initiative opposes the process of colonization through data in the case of the "Safe City" project in Belgrade?

I will use literature review and single case research design applied to the "Safe City" project in Belgrade to answer the research questions. Data used for my case study comes from both primary and secondary sources. Primary data are collected through semi-structured interviews with the experts and activists in the field of digital rights which are part of the initiative "Hiljade kamera" whose goal is to terminate the "Safe City" project in Belgrade. Other sources of data and information represent documents, web pages, news articles, and presentations available on the internet.

1.2. Thesis Structure

My thesis contains in total ten chapters, here I will mention the most important. In the next chapter, called *Background*, I will briefly present the concept of big data and its social relevance in the contemporary world. Since data has become an essential part of working and private life, it represents one of the most important goods in the twenty-first century and an essential ingredient of capital creation and corporate and state surveillance.

I will present a literature review in chapter three by outlining the most important authors and literature pieces relevant to my thesis. This section will heavily rely on critical approaches and theories often designated as CDS which try to link datafication (a process of data creation) with the social context, most essentially power and capital.

In the fourth chapter, named *Theory*, I will present the essential concepts and theories relevant to analyzing Belgrade's "Safe City" project. In this section, I will primarily focus on data assemblage, coloniality/decoloniality, and data colonialism.

The fifth section will be dedicated to the Methodology of my approach, presenting primary sources of my data and research design.

I will answer the research questions using empirical data interpreted by theories in the Analysis and Interpretation part. Finally, In the Sixth chapter, conclusions and the summery of the analysis will be presented along with the recommendations for the further research in the field.

2. Background

2.1. Data in the Twenty-First Century and Fourth Industrial Revolution

The etymology of word data implies a naturally given phenomenon since it comes from the Latin word *dare*, meaning 'to give*'* (Kitchin, 2014: 29) *or* 'given' as the fact (Mayer-Schönberger & Cukier, 2013: 71). This kind of etymology frames data as something objective, true, and an intrinsic quality of phenomena rather than socially shaped and constructed knowledge production. Kitchin (2014) suggests a more reflexive term that adequately refers to data as the knowledge derived/extracted from the process and not provided by it. A more proper term for the phenomena to which data refers would be *capta*, derived from the Latin word *capare*, which means "to take" (ibid.). Data today means something that can be recorded, analyzed, and reorganized (to *datafy* phenomena). The process of datafication implies abstraction and transformation of phenomena to quantified format to be tabulated and analyzed (Mayer-Schönberger & Cukier, 2013: 75). Kitchin (2014: 1) defines data as "raw material produced by abstracting the world into categories, measures, and other representational forms – numbers, characters, symbols, images, sounds, electromagnetic waves, bits – that constitute the building blocks from which information and knowledge are created."

Data is not a new thing and phenomenon. However, the series of "disruptive innovations" (Christensen, 1997 according to Kitchin, 2014: i) changed the *status quo* regarding how data is produced, analyzed, stored, managed, and utilized. The cumulative effect of "disruptive innovations" under the influence of data is often framed under the term "Data revolution" (Milan and Treré, 2019; Kitchin, 2014). This revolution is inseparable from the technological innovations in the field of information

and communication technologies (from now on: ICT) such as digital Closed-circuit television (from now on: CCTV), smartphones, online transactions, the Internet of Things (from now on: IoT), social media platforms, cloud computing, and other technology often referred to as the technology of fourth industrial revolution (Kitchin, 2014: 3).

Every new period of science has new technology for data generation, which also triggered the new ways of producing, storing, analyzing, and interpreting it. Around fifty years ago the world entered the era of big data (Kitchin, 2014: 25; Kitchin & Lauriault, 2018: 4). Big data is often referred to as the qualitative and quantitative change of data generated in terms of the increased amount of data (volume), out and in the speed of data and range (velocity) of data types and sources (variety) often referred to as "three Vs of big data" (Thatcher et al., 2016: 992). In addition, Kitchin and Lauriault (2018: 4) add a few more characteristics of big data, which are: *exhaustive* in scope, intending to capture the whole population or system and reach the sample of n=all; *relational*, which means that its common fields are enabling joining other data sets; flexible, extensional and scalable which means that its new fields can be added easily and size can be expanded rapidly.

The fourth industrial revolution technology provided new data analysis techniques and made data generation an essential part of almost all digital devices, leading to a huge increase in unstructured data. Unstructured data is growing fifteen times faster than structured (Kitchin, 2014: 33). While structured data has the defined model (numbers or text set in the table or database) and format (name, address, gender), which makes the analysis, storing, and transfer easy, unstructured data does not have the defined data model or identifiable structure (Kitchin, 2014: 33). Data "analytics 3.0" based on the AI technology can find patterns in unstructured data, something that has no patterns at all, which makes most of the data on social media platforms such as Facebook, Twitter, etc. (Couldry & Mejias, 2019a: 9; Kitchin, 2014; Hydén, 2020). The AI technology covers a wide range of technologies and analytical methods, which

in different ways imitate and perform the tasks that were previously limited to humans and animals: natural language processing, image recognition, neural networks, machine learning, deep learning, neural networks (Larsson, 2019: 575). The relationship between AI and big data is two-sided: big data represents the material for training the AI algorithms, which is then further used to find and validate patterns in the data (Hydén, 2020: 10).

2.2. Facial Recognition and Big Data

In my thesis, I will consider facial recognition technology (from now on: FR) as the process of reducing the physicality of the human face into a measurable object in a machine-readable format, which is then stored and compared with the existing data (Smith, 2020). Facial recognition is a growing realm of body measurement, biometrics, which is being conducted through CCTV, which are digital carriers of this type of technology (Gray, 2003: 317). The massive growth of the FR market and usage in recent years could be explained by developing AI and cloud computing technology, making it easier and more efficient (Thales, 2021). The datafication process through FR is conducted through the use of machine learning algorithms, which are transforming body measurements into the data through digital pictures. That data is biometric and unique to every individual. It is the most personal data, like fingerprint or DNA. Data extraction is happening by converting facial geometry ratios into numbers (Gray, 2003: 315). Data extracted from the photos and videos are then paired with those stored in the database, usually collected by the police to create biometric documents. When data extracted from the CCTV is matched with existing data, a person could be identified or not.

2.3. Everything Can Be Data

Datafication is making things into data, increasingly being the central concept of today's world's transformations. According to van Dijck (2014), datafication is normalized and accepted as the new paradigm for understanding social behavior and sociality. At the same time, *dataism* is its ideological ground, an uncritical belief in the quantification and tracking of human life marked with the trust in the institutional actors who collect, share, and interpret the data obtained through the communication technologies (van Dijck, 2014: 198).

According to Ricaurte (2019: 350-351), big data epistemology is *the* epistemology of our historical moment, which is based on the three crucial assumptions derived from the positivist paradigm: (1) data reflects reality; (2) data analysis generated the most valuable and accurate knowledge and (3) the results of data processing can be used to make better decisions about the world. This new epistemology of knowledge production regime requires specific resources which can enable data extraction, storage, processing, and analyzing (ibid.). Furthermore, this new form of social knowledge requires advanced computing capacity, human capital in the form of data science, vast amounts of data which will inform our actions, relations, and decisions in all fields of our social life: transport, commerce, labor, public administration, security (ibid.).

Datafication is a manifestation of the idea that everything, regardless of it being a process or a thing, can be made into data (face, brain function, heart beating, location, or trading) through the use of ICT (Mejias & Couldry, 2019: 2; Mayer-Schönberger & Cukier, 2013: 91). However, as this thesis is in the field of social science, I am going to demonstrate the way of making personal and social life into the data, in other words, how life and its elements can be derived into continuous, seamless flows of data (Couldry & Mejias, 2019a: 159).

Process of datafication in the era of big data could hardly be understood outside of the context of the fourth industrial revolution in which data is often interpreted as the "new oil" or natural resource which should guide the development of new technology and value creation (Couldry & Mejias, 2019a: 89). Founder and executive chairman of the World Economic Forum describes the fourth industrial revolution as "(…) a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres" where data could be understood as a universal and connecting element between these spheres (Schwab, 2016). Technologies of the fourth industrial revolution are based on collecting, processing, or/and analyzing data such as autonomous vehicles, 3-D printing, quantum computing, IoT, and AI (ibid.).

Datafication, according to Mejias and Couldry (2019: 3), has two dimensions. First is "the external infrastructure" through which data is being "collected, processed and stored (…)" while the second is consisted of the "(…) processes of value generation, which include monetization but also means of state control, cultural production, civic empowerment, etc." (ibid.). For Mejias and Couldry (2019), datafication represents a historically new method of quantifying social life, since never before has social life been exposed to this level and form of quantification process.

It is important to note that the big companies and the states hold infrastructure for the datafication while the citizens and their lives are the ones from which the big data is being extracted. Datafication, as Mejias and Couldry (2019: 4-5) emphasize, is inevitable from the question of the relation of power and who is conducting datafication and for what purpose.

2.4. Big data: Corporate and State Surveillance

Most of the discussion around the role of big data today is related to the platform economy, in which big data plays an essential role. However, it is very hard to distinguish between big data for-profit and the role of big data for surveillance, just as it is hard to make a clear separation between state and corporate surveillance. Therefore, there is the emergence of concepts reflecting this complex reality, such as "surveillance assemblage" (Haggerty & Ericson, 2000), "surveillance capitalism" (Zuboff, 2019b), "private-public surveillance partnership" (Mejias & Couldry 2019: 123) which are manifesting the problems of analytical separation between actors, process and entities involved in data creation and analysis.

Big data plays an essential role in today's world economy. Although the higher proportion of big data is "harvested" from business, extraction of personal data from individuals' personal lives and connections is much more relevant for the social sciences approach to which this thesis belongs (Mejias & Couldry 2019: 4). Datafication has become the essential process for governing global supply chains and became the main commodity traded in return for the free services on digital platforms (ibid.; van Dijck et al., 2018: 33). Collecting, analyzing, and circulating data to third parties is an essential part of the business model of digital platforms profiting from the datafication of our online life in different ways, but mainly through advertising (van Dijck et al., 2018: 33). In my thesis, I will not deal with big data in general, but rather big data as the personal data, which could be defined as "any data that is related to or resulting from the actions of a person" (Lehtiniemi & Ruckenstein, 2019: 2) or according to Couldry and Mejias (2019b: 339) the "data of actual or potential relevance to persons, whether collected from them from other persons or things."

In contemporary capitalism, personal information in form of metadata is collected as a currency for the "free services" we are using online (van Dijck, 2014: 197-198).

Manokha (2018a), discussing the contemporary changes in surveillance under the influence of digital technology, notes that two developments characterize the current phase of capitalism: first is the increasing importance of data as the new command, the second one is the rise of platform capitalism. According to Manokha (2018a), data could be added to Karl Polanyi's list of three "fictitious commodities": land, labor, and money, which are not inherently produced for sale but became commodified under capitalism.

> *Surveillance and ever-expanding privacy invasions (the constant collection of data and its processing) in more and more sophisticated ways, are intrinsic to the operation of platform capital as well as other entities whose business models also depend on this new fictitious commodity (e.g., data brokers or consultancies).*
>
> *(*Monokha, 2018a: 227*).*

Shoshana Zuboff (2019a), famous for her concept of "Surveillance capitalism", claims that surveillance became an inherent part of our life, massive and unavoidable, due to the transformation of the accumulation logic of capitalism. According to her, surveillance is everywhere today, and unlike in the Panopticon model, we cannot escape the gaze of the "Big Other" (Zuboff, 2019b: 441). Furthermore, this new accumulation logic of behavior surplus through data produces huge asymmetries in knowledge and power. Companies such as Google and Facebook can survey our behavior through data for prediction and its modification for profit (Zuboff, 2019a: 12; Zuboff, 2019b: 87-95).

Continued surveillance through metadata is often referred to as dataveillance (van Dijck, 2014: 198). For van Dijck (2014: 205), the difference between surveillance and dataveillance is that the former is limited to monitoring for specific purposes, while the latter presumes continuous collection and tracking of metadata for the unstated present

purposes. Regardless of whether we are addressing surveillance in the contemporary world as dataveillance or mass surveillance, the point is that surveillance is intensified and extended throughout the whole society while in the earlier periods was limited to the specific persons and places (Haggerty & Ericson, 2000: 606). As a result, tracking our personal data online and offline became normalized (Manokha, 2018b).

In light of the big data revolution and digitalization, Haggerty & Ericson (2000) conceptualize changes in surveillance in the form of the concept of surveillance assemblage, implying that surveillance is being conducted by the process of surveillance, the integration and conversation mediated by the digital technology. Our bodies are increasingly becoming the object of surveillance and being abstracted to in the series of discrete data flows, which are being integrated into the "data doubles" (Haggerty & Ericson, 2000: 606). Our body is, according to them, increasingly being made in cyborgs, "decorporealized" and being the object of government and corporate control and action (ibid. 611-613).

The concept of privacy and its protection through laws is often perceived as protecting human autonomy and integrity from manipulation, surveillance, and data extraction from corporate and state actors (Couldry & Mejias, 2019a: 155; Zuboff, 2019a: 19). Also, discourse about big players' monopolistic/monopsonist position in the data economy is often intended to lower their influence over society by lowering their market share (Couldry & Mejias, 2019a: 189).

2.5. Safe City: Surveillance Through Seamless Data Flow

Corporations are not the only actors engaged in the collection and processing of personal data. A Safe City is just one of the socio-technological assemblages which are using personal data for surveillance. This idea of a Safe City integrates the technology of the fourth industrial revolution and big data with urban governance and surveillance to lower the crime rate and increase the safety of the citizens in the urban areas (Cao, 2016). Chinese companies are leading in the global race of developing the platform and public surveillance technology through software and hardware solutions (networked surveillance cameras, programs for facial and plate, software for monitoring social media platforms, etc.) (Arun, 2020; Hillman & McCalpin, 2019a). Huawei Technologies Co., Ltd. (from now on: Huawei) is certainly not the only company that provides Safe City solutions, but it is among the most prominent ones. Until now, Huawei implemented Safe City solutions in more than 100 countries and 700 cities worldwide (Greitens, 2020: 2-3).

The Safe City projects implemented by the Chinese companies are often perceived as "exporting authoritarianism" since they are more often than not implemented in countries with low levels of civil freedoms and democratic procedures (Greitens, 2020: 6; Hillman & McCalpin, 2019a). China is not just "exporting authoritarianism" to the other countries, but it is also often perceived as the country of 'data-driven authoritarianism' or "IT-backed authoritarianism" referring to the growing importance of the ICT in governing the society, surveillance, and social control (Lee, 2019: 955).

2.6. Contesting Datafication

With the penetration of big data epistemology in almost all aspects of our lives, there is a growing number of individuals, groups, and institutions resisting it. To understand social phenomena critically is to understand their conflicting and political elements. There are several assumptions necessary for understanding data politics, and that is 1. That data is the object whose production interests those who are exercising power; 2. Production of data is a social and political practice that mobilizes both objects and subjects of data (Beraldo & Milan, 2019:2). For Beraldo and Milan (2019:4), there are two types of consequences of datafication: institutional and contentious politics of data. Institutional politics of data concerns with the top-down effects of the datafication, such as government surveillance, corporate profiling, and algorithmic violence, while contentious politics of data are bottom-up practices of individuals and civil society organizations which are increasingly aware of the consequence of datafication and its opportunities for democratic empowerment (ibid.).

While Ruppert and colleagues (2017) are claiming that subjects of data politics are yet to be found, Beraldo and Milan (2019) are focusing their attention on the analysis of data activism as the social actors of "contentious politics of data" which are taking a critical stance on massive data collection and datafication.

> *By contentious politics of data, we mean the multiplicity of bottom-up, transformative initiatives interfering with and/or hijacking dominant, top-down processes of datafication, by contesting existing power relations and narratives and/or by re-appropriating data practices and infrastructure for purposes distinct from the intended*
>
> (Beraldo & Milan, 2019: 2).

To practice contentious politics of data is to practice subversion and resistance towards the existing process of datafication, its narrative, or power relations, whether collective or individual (ibid. 3-7). In developing the typology of data activism, Beraldo and Milan (2019: 6) argue that social activism can manifest itself in two distinct ways: contention over control of data and/or through the contention manifested through data practices. So, the data can be seen as the main stake and/or part of the repertoire of actions besides already known forms of civic engagement and protest (ibid.). However, these distinctions are not exclusive, and they can simultaneously exist in the same empirical case (Beraldo & Milan, 2019: 7). Furthermore, Beraldo and Milan (2019) argue that the exclusive existence of the data as the stake and data as part of the repertoire is limiting. Mobilizing around the data without integrating datafile tactics can miss making use of the potential of the data practices for the sake of social empowerment (ibid. 8). At the same time, only relying on the data tools for actions can miss to critically engage with the power relations in which datafication is embedded, which is necessary for the "redirecting" the process of datafication to become a process of emancipation rather than domination (ibid.).

2.7. Civil Society Organizations and Digital Rights

The term "civil society" was defined and redefined many times since the ancient Greek and Roman philosophers; today, it refers to a discreet socio-political sphere outside the realm of state and market forces (Daskal, 2018: 243). In this sphere, citizens and organizations can participate in order to shape different aspects of life in society (ibid.). Daskal (2018) differentiates between two types of civil society organizations: a-political and political. In the former group fall organizations that are not posing a threat to the authorities and which activities are non-conflictual, they carry no explicit political weight, such as ethnic organizations, cultural organizations, professional

associations, etc. Political civil society organizations are those nongovernmental organizations that are able to resist the ruling forces by attempting to shape or challenge existing laws and policies in order to achieve welfare to the whole society, rather than exclusively their own. Political civil society organizations often initiate civic education, citizen education, and mobilization of young people to become involved in civic life (ibid.).

One of these political civil society organizations is also digital rights organizations mainly concentrated on privacy, access to the internet, and freedom of speech (ibid.: 242-245). These organizations protect digital rights in three areas: public, judicial, and political (ibid.: 242). They file lawsuits against government and internet bodies in political and judicial areas and promote legislative initiatives in the mediated public sphere. In addition, these organizations promote their agenda by instructing citizens how to fight for their digital rights and influence public opinion (ibid.: 242).

In my thesis, I analyzed how datafication is becoming the object of battle and contestation between state and civil society organizations in the “Safe City” project in Belgrade. Suppose decoloniality is not just decolonization but rethinking the process of ongoing colonization. In that case, civil society organizations and initiatives challenging datafication can be seen as liberation forces.

3. Literature Review

3.1. Critical Data Studies

There is an emerging field of CDS, sub-filed of broader Critical science (Mohamed, 2020: 662) approach, which focuses on the potential inequality, exclusion, and discrimination by the mechanism of big data (Milan & Treré, 2017: 1; Kitchin & Lauriault, 2018). With my thesis, I want to join the body of scholarly work that critically approaches the optimistic narratives around technological development, which is often portrayed as the driver of knowledge, change, and innovation. CDS authors seek to approach it as "mythology" that needs to be critically examined and uncover how data and datafication processes are used by the companies and states for surveillance and privacy intrusion and identify actors that are challenging these processes (Milan & Treré, 2017).

As Iliadis and Russo (2016) put it, CDS should explore ethical, cultural, and critical challenges posed by big data rather than treating it as a neutral phenomenon. Thus, the CDS subject is suggested to be socio-technical "data assemblages," structures constitutive of big data that exert power (Kitchin, 2014; Kitchin & Lauriault, 2018; Iliadis & Russo, 2016: 3). According to Kitchin and Lauriault (2018: 14), one of the most pressing social issues which need addressing from the CDS perspective is the dataveillance and erosion of privacy, anticipatory governance, profiling, social sorting, and control creep.

There is a wide range of authors who call and argue for the necessity of a decolonial approach in examining the relations between power, data, and technology (Milan and Treré, 2017, 2019; Arora, 2019; Arun, 2020; Couldry & Mejias, 2019a; Mohamed et al., 2020). These authors critically examine the interests behind datafication and

technology while arguing for decolonizing it through activism and alternative knowledge creation. In that sense, decolonial thinking and theory can be situated as critical theory (Mignolo, 2007: 156).

3.2. Big Data from the South

Besides rooting my approach in the scholarly work of CDS, it is also essential to notice and be aware of global inequalities in the processes of datafication and exploitation that come with it. While Dalton and Thatcher (2014), Kitchin and Lauriault (2018), Iliadis and Russo (2016) constituted research subjects and questions for the CDS, there is another stream of authors, such as Milan and Treré (2017, 2019), Arora (2016, 2019). Those authors call for focusing on the effects of big data on the Global South. This broader movement gathered around the initiative "Big Data from the South"[2] tends to bridge the divide between North and South, researchers and activist in the field of big data. Milan and Treré (2017: 2) are claiming that many approaches in the field of the CDS are relying on 'digital universalism' which tends to homogenize and assimilate differences that exist across the cultural and social contexts and, by doing that, fail to recognize the cultural richness of the South, its plurality and diversity.

Also, Milan and Treré (ibid.) openly call for "engaged research" on datafication and mobilize people to fight for their digital rights. They are trying to perceive the process of datafication and big data from the perspective of their relevance for the existing system of inequality, dominance, discrimination, and injustice on all levels and particularly between the South and North (ibid.). They are urging that in finding the answer on how datafication affects the Global South concerning unequal distribution of the resources and power between the South and North and the "political economy of

[2] Launched in 2017 by Stefania Milan and Emiliano Treré (DATACTIVE, n.d.).

knowledge production" (Milan & Treré, 2019: 320). While claiming that western modernity has made colonialism possible, datafication has the same potential to cause marginalization and "epistemicide" (Santos, 2016) of the South (Milan & Treré, 2019: 320-1). Places from the South, underprivileged and silenced, are not just excluded from storytelling generated by the techno-optimists who are celebrating the successes and possibilities of the big data revolution but also by the critics of these developments (Ibid.). This is even clearer when we examine how the dominant discussions and public dialogues about privacy, surveillance, and automation are framed exclusively by the "Western" standards and concerns (ibid.).

So, we must ask how datafication unfolds in the Global South and what is happening in the intersections of the other underprivileged identities and positions that have limited access to education, income, and human rights protection (Milan & Treré, 2019: 321). Datafication is the big data revolution that exacerbates existing divides and inequalities between the wealthy western population, which has established democratic practices and silenced underprivileged subaltern populations with fragile democracies (Milan & Treré, 2019: 320). Using the examples from India and other countries of the Global South, Arora claims that the big data revolution unfolds in "unprecedented ways in these neglected contexts" where 60% of the population is living under the poverty line (Arora, 2016: 1681).

Following Milan's and Treré (2019: 326), the process of datafication data extraction, storage, and processing in the Global South should be situated and analyzed in the context of domination, exploitation, extraction, and oppression. This is precisely what Arun is trying to do when he is analyzing the impacts of AI technology on the Global South, arguing that this technology is interfering with the vulnerabilities of the South causing harmful effects (Arun, 2020: 594-595). The Global South is the place where technology is used in exploitative purposes by both international companies and domestic governing elites (ibid.)

4. Theory

Basing my approach on the assumptions that datafication represents the tool in the power struggle of states and corporations controlling and conducting this process, I will examine the "Safe City" project in Belgrade as the process of data colonization. This approach uses coloniality to claim that knowledge production cannot be perceived independently from the process of domination and power (Quijano, 2007).

4.1. Data Assemblage

Kitchin (2014) is suggesting that big data is always created within the complex of data assemblage. This term implies that data is never neutrally produced as a raw material but rather cooked by the goals and recipes of the chefs who are in the position of power (Kitchin, 2014: 9). Data assemblages are, according to Kitchin (2014: 51): "(…) complex socio-technical systems that are embedded within a larger institutional landscape of researchers, institutions, and corporations, constituting essential tools in the production of knowledge, governance, and capital." Thus, data assemblage provides a tool to think about data critically concerning the wider social relations and structures. Data and analytic processes are kept inside the web of relations, so it is undesirable to study them as isolated phenomena (Carter, 2018: 2). So, in my approach, I use the model of data assemblage to analyze how data is produced, stored, analyzed, and used in a wider social context. In that sense, data assemblage represents the tool to analyze the relations since it includes technological, social, and political apparatus that frame the production, operation, and work of data (Kitchin & Lauriault, 2018: 8). According to Kitchin and Lauriault (2018:9), every apparatus is in the function of production of power since data is never neutral, but in the functions of those in the institutions and who have specific goals and aspirations. Thus, the goal of using the concept of data assemblage is to uncover how data infrastructure works and is

embodied in specific social context producing social consequences and then as the boomerang returns to the society that created it. That being said, uncovering the data assemblages means uncovering the relationship between data generation, storage, analysis, and relations with wider social context, actors, institutions, laws, and protocols. In other words, focus on the three main domains of data assemblage: things (infrastructure), language (algorithm, law), and people (internal and external) (Aragona et al., 2018: 455).

4.2. Contemporary Coloniality from a Decolonial Perspective

Historical colonialism was a specific form of social and economic organization, with countries such as France, Span, Britain, and later the United States in power, with four essential components: appropriation of resources, unequal social and economic relations which enabled resource extraction; unequal distribution of benefits from resources appropriation; and an ideology that justified the unequal power relations (Couldry & Mejias, 2019a: 4).

Although historical colonialism is over, it has left the world with a serious legacy, which we deal with today, such as racism, migration, poverty, debt, and dependency of former colonies to their former metropoles (Couldry & Mejias, 2019a: 74-75). Big data from that position is seen as the phenomenon that facilitates colonial relations and structures new ones.

Coloniality is a broader concept often used to denote colonial characteristics in the present times, and it is used as an analytical tool for understanding society (Mohamed et al., 2020: 663). However, at least three critical theoretical approaches deal with coloniality: neocolonialism, postcolonialism, and decoloniality (Couldry & Mejias, 2019a: 75). It is sometimes hard to make the difference between them. Authors often

acknowledge a need for synergies of these approaches to fully understand the links between big data and new/old forms of coloniality (Couldry & Mejias, 2019a). Here, I will focus on the decolonial approach without entering the discussion about the difference between the three approaches mentioned.

The decolonial approach seeks to survive the postcolonial and neocolonial realities and articulate an alternative worldwide, free from Eurocentric modernity (Couldry & Mejias, 2019a: 80). This approach is intellectually inspired by the grassroots movements and intellectuals from the South. It seeks to establish a universal worldview outside of Western Universalism and acknowledges that the road towards the decolonization of knowledge is through critical thinking (ibid.): “Decoloniality is therefore not simply decolonization, defined as the end of colonial occupation and administration, but a broader rethinking of relations to ongoing coloniality” (Couldry & Mejias, 2019a: 80).

Many authors think about big data from the perspective of the coloniality of power, and that is through the imposition of thinking, knowing which are considered “objective” but are discriminatory and part of a specific “colonial” structure of power (Quijano, 2007: 168). According to Quijano (2007), coloniality is inseparable from modernity. Modernity is an essential part of coloniality. Without modernity, there is no coloniality, and there are no racial, ethnic, and other social classifications and categories that are considered 'scientific' and 'objective' (Quijano, 2007: 168-172). From the decolonial perspective, data is far from neutral, but rather the means in the hands of those in power who use this epistemology to shape the world in their interests. From this perspective, coloniality is a necessary part of modernity, while colonization advances through modern ideas and visions (Hoffmann, 2017). There is specific salvation rhetoric through which modernization is advancing, such as development, progress, and civilization, hiding the logic of coloniality characterized by sexism, injustice, inequalities, destruction, etc. (Hoffmann, 2017).

Today, coloniality can help us analyze how big data epistemologies materializing through the data assemblage produce marginalization, subordination, and discrimination. At the same time, decoloniality would imply liberation from the logic of coloniality. Coloniality exists beyond historical colonialism and helps us explain the continuation of unequal power dynamics between the disadvantaged and those who possess the privileges (Mohamed et al., 2020).

4.3. Data Colonialism

Data colonialism is used in CDS literature as the metaphor for power asymmetries in current forms of data commodification (Thatcher et al. 2016: 992), but also as a literal continuation of the previous historical forms of colonialism, which lasted from the sixteenth to the twentieth century (Couldry & Mejias, 2019a; 2019b: 337-339). Couldry and Mejias (2019a; 2019b) are arguing that data colonialism indeed represents the new form of colonialism which in the end will result in the new phase of capitalism where there will be no space between us and the capitalist system, as our entire lives will be subjected to capital through data.

Couldry and Mejias (2019a: 84) use the concept of coloniality to analyze the current process of commodification and abstraction of social relations through data. Thus, we are witnessing a continuation of historical colonialism in the form of data colonialism, where the center of appropriation is not land and bodies, but social relations through data (ibid.). However, the process of data colonization should be extended so that it does not only refer to the process of the data extraction for the sake of profit (Couldry & Mejias, 2019a: 85), but also for the sake of political elites who can benefit in different ways from data extracting, storage, analysis, and use (Ricaurte, 2019, 356-358).

Colonization by data, every aspect and layer of human experience becoming the target of data extraction for profit, is becoming the key dimension of capitalism today (Couldry & Mejias, 2019a: x). Thus, Couldry and Mejias (ibid.) perceive colonialism and capitalism as two phenomena that are deeply interconnected and dependent, just like colonialism and modernity for Quijano (2007), whose work they base their approach on.

Couldry and Mejias (2019a: xvii) argue that the capital was extending and acquiring new territories from which labor was labor and resources were extracted under the Spanish, British and Portuguese empires. In that way, colonialism provided essential preconditions for the emergence of industrial capitalism, just as they expect that new form of colonialism will contribute to the new stage of capitalism where "the appropriation of human life through data will be central" and complete (Couldry & Mejias, 2019b: 337). Today, we encounter a never-seen convergence of economic and cognitive power; in other words, the ability to know and make value is overlapping like never before (Couldry & Mejias, 2019a: xii). Power and knowledge derived from data are in the direct link since knowledge derived from the personal data might give the higher control and higher precision in targeted ads on a social media platform and thus give higher profit, or it can provide a different aspect of knowledge which can give higher ability of control to the data holder (Couldry & Mejias, 2019a: 128). According to the Couldry & Mejias (2019b: 337) "new types of human relations which enable the extraction of data for commodification" are emerging (called "data relations") through which extraction for capital is happening in both global South and North (Couldry & Mejias, 2019a: 128.). For Couldry and Mejias (2019b), the analogy between neutral resources and data is obvious. Thus, an analysis of how data is acquired through data relations should be perceived through the process of appropriation or extraction (ibid.: 338). The colonial moment of contemporary capitalism lies in its appropriation of social and individual life through data with the final goal of total incorporation of bodies and "everyday life" into the "capitalist production process" (Couldry & Mejias,

2019a: 12; 2019b: 342). However, data is not abstracted from us automatically but through social relations (Couldry & Mejias, 2019b: 343).

Nudging, tracking, and targeting happens based on "data doubles" which are data constructs, arranged in complex categories to target advertising, but effects of this new social knowledge are often discriminatory (ibid.: 345). Constant surveillance and tracking of the spaces that belong to the self can result in, according to Couldry and Mejias (2019b), losing our core, places that allow us to transform freely. In a literary sense, data colonialism "brings extraction to home" through various gadgets and technological means used for data extraction, such as IoT (Couldry & Mejias, 2019a: 136-137). The authors insist on the risk of losing what they call "the minimal integrity of the self" which is "the entity that can make and reflect on choices in a complex world" and which "is essential to all Western liberal notions of freedom" (Couldry & Mejias, 2019b: 345). This minimal integrity could also be perceived outside the Western models of power, beyond its reach, which shows that it is the "natural substantivity of a person" (ibid.: 163). For Couldry and Mejias (2019b: 346), recognizing that our life is dispossessed through tracking is the start of the fight against data colonialism.

The vision of totality that is enforced by data colonialism must be criticized and questioned, just as we, according to Quijano (2007), must abandon the idea of the universality of European modernity and rationality. Datafication denies alternative visions of order and datafied life. It "categorizes subjects and builds societies toward total algorithmic control" (Couldry & Mejias, 2019b: 346). Therefore, the decolonial mission in the fight against data colonialism ideal of totality based on the datafication of life should start with rejecting the idea that continuous collection of data for human beings is normal and rational. However, Couldry and Mejias (ibid.) acknowledge that rejecting data colonialism does not mean rejecting the idea of data usage in all its forms. Instead, it means rejecting the current form of resource extraction and social order in which this appropriation is possible and naming it colonial. Couldry & Mejias (2019b)

argue that data did not change the logic of capitalism. The goal still is maximizing value, which leads to the concentration of power and wealth in the hands of the minority (Couldry & Mejias, 2019a: 32).

4.4. Decolonization

According to the Mohamed (et al. 2020: 664), decolonization has two distinct roles and forms, one being territorial decolonization which can be achieved with the dissolution of the colonial relations, and the other being structural, erasing colonial mechanism of power, language, culture, thinking and economics that shape our life most essentially through understanding and challenging legitimacy of dominant norms, knowledge, assumptions, and values. Therefore, the first step towards decolonization is naming something colonial and understanding something through these lenses while focusing on the cultural and material circumstances surrounding that phenomenon.

To practice decolonization, it is necessary to engage in the epistemic reconstitution and imagine a different way of knowing and thinking (other than totality embodied in the modernity/rationality), which is open to the heterogeneity of reality and other realities nationalities (Quijano, 2007). Liberation from coloniality is linked to the process of social liberation from the expression of power organized through exploitation, domination, discrimination, and inequality (Quijano, 2007: 178). For Quijano (2000) coloniality of power means that life changes, circumstances, and opportunities are structured according to the race and geographical relations, in other words, economic privilege and classification imposed by the knowledge system (Couldry & Mejias, 2019a: 73).

5. Methodology

For the method, I chose a single case research design (Yin, 2018: 97), which would allow me to explore data colonialism in the specific social context through the "Safe City" project in Belgrade. In this project, I will examine both the process of colonization through datafication and the process of decolonization through the actions of activists gathered around the "Hiljade Kamera" initiative. In that way, I can analyze both the top-down process of data extraction through the complex infrastructure of the "Safe City" project in Belgrade and bottom-up resistance.

My research is not centered on the country's case but rather on the project, which I perceive through the model of data assemblage, a specific socio-technical entity of analysis to assess how data is created. Although Serbia does not represent the case for my analysis, it represented a wider context in which the specific case of "Safe City" exists. My research is explorative since it aims to discover new empirical places for applying the concept of data colonization and decolonization.

5.1. Case Study

The case will represent the "Safe City" project in Belgrade, which will be analyzed as a data assemblage and complex socio-technical system in which the center lays its goal of collecting personal data. Yin (2018: 50) notices that case study is probably the most appropriate method when there is a "why" or "how" research question and defines it as an empirical method that seeks to investigate the contemporary phenomena in real-world context when the boundaries between the phenomena and context are not fully evident.

There are several reasons for choosing the "Safe City" project in Belgrade. Until now, Belgrade is, according to the digital rights activists (Krivokapić et al., 2021), the only European capital that is already implementing FR on the whole city level. This implementation phase provides me with a great opportunity to investigate the ongoing process of project constitution and its contestation by digital rights activists. Another reason is that Serbia goes through failing personal rights and freedoms levels according to international organizations such as Freedom House, which allows me to investigate the links between these processes and datafication (Petrović, 2020: 11; Freedom House, 2019). Additionally, the project has defined contestants through whose perspective I will understand the power dynamics in light of anticipated datafication.

5.2. Data Collection

I will base my case study on the data collected through:

1. Primary research: semi-structured interviews with the "Hiljade kamera" initiative representatives who are contesting the establishment of the "Safe City" project in Belgrade;
2. Desk research: documents, secondary literature, and publications on the internet.

5.3. Selection of Interviewees and Conduction of Interviews

To adequately answer the research questions related to the case study, I conducted six interviews with activists and members of the "Hiljade Kamera" initiative, with equal distribution of male and female respondents. This is the core data as part of this

master’s thesis project, which allowed me to understand contextual circumstances and data (de)colonization in Belgrade's “Safe City” project.

I chose to interview the representatives of civil society organizations for at least two reasons. First, they are experts in different fields (ICT, Law, Journalism or Activism) regarding big data, privacy, new technology, and surveillance. The second is that I wanted to give space to the narratives and knowledge, which are located in sphere of resistance to oppression rather than in the position of power. That is the reason why I did not want to interview representatives of the state actors because they avoid providing the information and documents transparently not only to the public but also independent state bodies such as the Commissioner for Information of Public Importance and Personal Data Protection (from now on: Commissioner).

First contact with the representatives of the Initiative I had in October 2020, in the time when I was preparing the Master thesis project. First pilot interview with the key informant of the Initiative “Hiljade Kamera” was conducted in February 2021. Back in that time, the focus of my research was more on the corporate aspects of surveillance. After two months of literature review and articulating the definite focus of my work, I conducted an interview with the same person about the Safe City project in Belgrade.

The selection of other interviewees has been conducted through the “snowball” method of sampling (Mason, 2002: 142). The only criteria for including someone in the sample was that they are recognized as part of this informal initiative. However, all the respondents are employers, founders, or affiliated in different ways with organizations advocating for digital rights and privacy (Share Foundation, Partneri Srbija, Open Society Foundation, etc.).

All six interviews were conducted through video calls. The sample size in my research was shaped by the saturation (Creswell, 2015: 77). I noticed that there was less information useful for my research with every new interview, so I decided to stop conducting interviews after the sixth one. The interviews were 30 to 60 minutes long

and were conducted between the sixteenth and twenty-seventh of April 2021. After conducting the interviews, they were transcribed by using the recorded audio of our conversation, while the saved audio record of our conversation was deleted after the transcription. More detailed information about the interviews conducted and a guide for the semi-structured interview can be found in Appendix A and B.

5.4. Coding and Analysis

The interviews were coded with the help of the NVivo 12.6.0 software for qualitative data analysis. Coding was conducted in two cycles. Initial coding was conducted to notice initial themes and patterns, which could help me answer my research question by reading the transcripts and taking notes (Saldana, 2013: 100). In the second coding cycle, I used pattern coding by developing the categories under which I could subsume similar coded data (Saldana, 2013: 232). Developed categories are in line with the theoretical propositions. The main ones are data referred to activities of the "Hiljade Kamera" initiative, biometric surveillance, social actors, biometric data, data infrastructure, and data capabilities.

Analysis followed the coding of interviews to identify the themes and patterns, which could essentially be subsumed to the brother method of thematic analysis described in depth by Braun & Clarke (2006). This type of data analysis allowed me to recognize themes, patterns, and relationships in the data so that complex reality could be captured to answer the research question (SAGE Publications, 2019).

Since the "Safe City" project in Belgrade is still in the implementation phase and, according to the official documents, not fully operational, I used anticipation as the framework to understand the possible future effects of data extraction. Therefore, the bare fact that the "Safe City" project in Belgrade is not fully operational, its social

consequences and datafication could not be analyzed directly, but only anticipated through the knowledge about the technology, which is its essential part (Alvial-Palavicino, 2016). Adam and Groves (2007, according to Alvial-Palavicino, 2016: 136) claim that the future is knowledgeable since it represents either a continuation of the past or present and could be uncovered through the scientific methods or mapping the possible, preferable, or probable futures.

Because data colonialism represents a social phenomenon that is not directly measurable, I decided to understand it through data assemblage (Kitchin, 2014). In that way I understand the work of infrastructure (hardware and software) through which data can be extracted and analyzed to be converted into knowledge. The other dimension of data colonialism that I analyzed is understanding the impact made on different social actors. I used theoretical insights from decolonial theory, to understand and identify emancipatory characteristics of data contestation practices, which can be defined as activities, narratives, and practices of subversion and resistance to datafication practices (Beraldo & Milan, 2019: 2-7).

5.5. Reflection on Ethics and Process

Ethics in the direct involvement of the other people in the research is never straightforward because it is highly dependent on the concrete situation, people, and context where it is happening. Ethics in the social sciences research is never definite, but rather an open system where decisions must be made for every specific situation. Ethical issues arise even before research starts. During the formulation of questions and choosing the focus, it continues with the direct involvement of people as interviewees and respondents. Ethical issues deal with the issues of the social consequences of the research, which include both negative and positive effects on

respondents and the community about whom research is conducted or could affect (Kvale & Brinkmann, 2014: 95).

For me, of utmost importance was gaining informed consent from interviewees and protecting their confidentiality. However, I had the impression that all respondents are quite ambivalent about that since they are already talking and acting publicly about the issues which were the subject of our conversation. Therefore, informed consent was based on the fact that all interviewees were informed about the purpose of the interview, my research, and using data from the research. Also, I asked for consent for the audio recording of our conversation and it's handling/keeping it until transcription was conducted.

All the interviewees were first contacted by email, where I offered them to choose the time and application through which we will have our conversation. I was expecting that since all of them are privacy advocates and activists will have some preference over the application or program over which we will have our conversation, most of them were indifferent in that regard. I guess that it is because they are conscious that our data is unavoidably shared with the companies and that our complete privacy on the internet is almost impossible.

During the preparation of the interviews, one situation made me think of how vital ownership of data might be for the person. Namely, one of the interviewees asked me if I could share the audio record of our conversation with them for their self-analysis. That made me reflect on importance of data possession because there is direct connection between ownership of personal data and control of it. Their ownership of audio record of our conversation gave me a feeling of limitation of my freedom in terms of interpretation of what they said, making my potential faking of data less likely and very easily proven by them. So, in that interview situation, data control, data ownership, and knowledge creation have got in touch in an obvious way.

6. Case study

6.1. The "Safe City" Project in Belgrade

The beginning of the "Safe city" project could be located in the series of agreements between the Government of the Republic of Serbia (from now on: GRS) and the government of the People's Republic of China (from now on: GPRC). Bilateral agreements followed the strategic partnership and cooperation agreements between The Ministry of Internal Affairs of the Republic of Serbia (from now on: MIARS) and Huawei. The first "Agreement on Economic and Technical Cooperation in the Field of Infrastructure" was signed in 2009 between GRS and GPRC and following that agreement, the Law on Ratification of the Agreement on Economic and Technical Cooperation in the Field of Infrastructure (The Ministry of Internal Affairs of the Republic of Serbia [MIARS], 2019a) was also introduced. Both the agreement and the law provided MIARS basis for the development of the cooperation with Huawei, which started in 2011 by opening talks about the advancement of the ICT system of the MIARS through the project "Safe Society"[3] (ibid.).

A significant event happened in 2014, when a young man died after being hit by a car and the driver escaped (N1, 2014). The case was named "Countryman", after a model of the driven car (Prague Security Studies Institute [PSSI], 2020: 8). The suspect fled to the People's Republic of China (from now on: PRC) to avoid prosecution in Serbia but was located after just three days by the cutting edge FR in China, and was arrested and extradited to Serbia (Stojkovski, 2019). According to Huawei, police

[3] In the official documents provided by the MIARS, two titles are used interchangeably: "Safe City" and "Safe Society". However, it is not clear whether there is any difference between these projects since that difference is not explained by them. Therefore, I decided to refer to all activities planned in Belgrade as the "Safe City" because there is not enough information to make the conceptual and analytical differences between them.

officials in Serbia were “inspired” with the efficiency of the Safe city’s solutions in China and became interested in installing the system of intelligent surveillance in Serbia (Huawei Technologies Co., Ltd. [Huawei], 2018). As a result, Huawei and MIARS signed the Memorandum of Understanding concerning the steps needed to implement the “Safe City” project (MIARS, 2019b: 20).

The “Safe City” project in Belgrade emerged in a specific social context, which I will present in the following pages. Firstly, I will examine the social context concerning the Safe city project by examining relations between China and Serbia in recent years. Secondly, I will examine the digitalization initiative launched by the Serbian government, the phenomena of the captured state, and the ongoing concentration of political power in the hands of president Vučić and his political party. Finally, I will examine the treatment of personal data by the public sector in Serbia.

6.2. Social context

6.2.1. Project in the Context of International relations: Between European Union and China

According to Vuksanović (2019), in recent years, Sino-Serbian relations flourished to an unprecedented extent. Domains where the most important developments occurred, are finance, infrastructure, and increasingly national security. Cooperation in the security sector is most notably observed through the development of Serbia's surveillance system, providing the Serbian military with the equipment and cooperation between police departments through established joint patrols in Serbia (Vuksanović, 2019). According to some reports, there are two reasons why the cooperation between China and Serbia started to develop in an unprecedented way after 2009. One is that

Serbia’s geopolitical location represents the door to Europe's market, which is strategically important for China’s influence in Europe and the Balkans, and the other is the need of the local politicians to attract investment in the infrastructure after the financial crisis in 2008 (PSSI, 2020: 7).

As noted in the report Nations in Transit (from now on: NIT) from 2020, Chinese foreign policy goals of promoting the positive image of China globally and expanding the country's influence abroad are much more easily implemented in the context with the institutional weaknesses and concentrated power (Csaky, 2020). In this situation, China can spread its economic influence by tailoring its approach to the clientelist economic and political structures in countries with a lack of democratic institutions (ibid.: 10). For example, in 10 out of the 29 NIT countries, Chinese company Huawei signed the agreement about establishing the “Safe City” project (Ibid.). Chinese influence in the region and exploitation of weaknesses is exercised in the countries of NIT through the export of the technology, debt diplomacy (providing the loans without strings for borrowing and paying back the loan in a way that creates political dependency), and influence campaign (ibid.: 11).

Serbia belongs to a middle-income country and is currently negotiating for membership in the European Union (from now on: EU). However, historically Serbia has had strong ties with other global power centers such as Russia and China. Moreover, while almost all governments after 2000 have aimed for membership in the EU, Serbia's foreign diplomacy, political-economic ties with China and Russia stayed strong. This is especially important in the struggle to protect “national interest” in the United Nations Security Council by opposing Kosovo's independence, where China and Russia are seen as Serbian closest allies in that mission (Dimitrijević, 2017: 69).

The Silk Road Economic Belt initiative was announced in 2013 by the Chinese president Xi Jinping to establish economic cooperation with European and Asian

countries. This initiative is an essential part of the Chinese national development strategy, which attempts to achieve the "Chinese dream" (Dimitrijević, 2017: 65-66).

The cooperation and influence of China in Serbia was significantly intensified after 2012 when cooperation platform "16+1" was developed as an attempt to integrate Central and East European countries in the Belt and Road Initiative (from now on: BRI) (Hillman & McCalpin, 2019b). After Greece joined the cooperation platform in 2019, it changed the name to "17+1" (Kavalski, 2019). Today the official name of the platform is Cooperation between China and Central and Eastern European Countries (also known as China – CEEC), which includes 12 countries that are member states of the EU and 5 Balkan countries (ibid.; China-CEEC, n.d.). By some, Balkan region is seen as the entry point for China's widening political and economic influence in Europe (Stojanović, 2019). China's infrastructure and economic footprint in Western Balkan are sometimes referred to as the "Balkan Silk Road", which refers to the building of transport and logistical corridors which China started even before the official launch of BRI for the rest of the world (Bastian, 2017). From 2012 China has invested around 15.4 billion US dollars in countries that are part of the "16+1" platform in areas of transport, energy, manufacturing, real estate, and notably in ICT (Hillman & McCalpin, 2019b). Out of all investments made from China in Central and Eastern Europe in the period between 2014 and 2018, 56 percent was made in Serbia (Grubić & Kranner, 2019). Aside from long and lasting diplomatic relations between China and Serbia, Dimitrijević (2017: 70) sees the China – CEEC platform as the catalyst for developing China's strategic relations in various spheres of the economy. During the global pandemic of the COVID-19, ties between China and Serbia were taken to the next level. Almost 70% of all vaccines in Serbia were bought from Chinese producer Sinopharm, and the President of Serbia also received the contingent of vaccines publicly to promote immunization against Covid-19 (Euronews, 2021; Miković, 2021; Savić, 2021). At the same time, the prime minister took Pfizer jab, symbolizing Serbia's geopolitical orientation (ibid.).

China is, through its companies, most notably Huawei, an important provider of ICT and promoter of digital and AI products in Serbia. Therefore, the "Safe city" project should also be perceived in that light, as the realization of different interests, Chinese interest of economic and political presence in the Balkans region, and the interest of political elites in Serbia to attract investments. All of this is made possible through various bilateral cooperation agreements between China and Serbia.

6.2.2. Digitalization and e-Government

The government officials see the implementation and promotion of the ICT as the new development strategy in Serbia, as ICT is often considered fundamental for the market and government development. Digitalization is a process with both the symbolic and material element, implying both conversions of the analog signals into the digital, once and zeros, and the material base, which ultimately refers to concrete pieces of equipment which are used in the process (Slavinski & Todorović, 2019: 245).

Digitalization is a process that is seen as the integration of the ICT in the everyday business operations of both the private and public sectors. There are different policy approaches and regulatory initiatives which are following and leading these processes. The Serbian prime minister sees direct implementation of ICT technology in the government and the private sector as the goal which will help achieve better education, more efficient public administration, create new jobs and attract foreign investment. In addition, the Serbian prime minister has recently praised digital government infrastructure as responsible for making massive immunization with the COVID-19 vaccines possible, as people applied for vaccines through the Government National E-government portal (ITU News, 2021; Higgins, 2021).

Strong political initiative for digitalization came from the government, which was elected in 2017. It recognized the potential for achieving higher economic growth and

higher government efficiency through the digitalization and implementation of ICT (National Assembly of the Republic of Serbia [NARS], 2017). As in the case of the "Safe City" project, implementation of ICT, which is considered part of the fourth industrial revolution, is believed to be directly linked to the improvements in different aspects of social life and is dominantly centralized, led initiated by the state. In contrast, some other bottom-up processes are considered illegal and often prevented from happening. The example is the case of modernizing the market of the transportation services started by the startup company CarGo which developed the application software for connecting the passenger and drivers. At one point, this was perceived by the executive authority as illegal activity of the startup company, and it was sanctioned as such (Danas, 2019a).

6.2.3. Serbia: The Hybrid Regime in the Captured State

For five years in a row, Freedom House is in its annual index of Freedom of the World, noticing the steady erosion of the political freedoms in Serbia, while in the report from 2019 status of Serbia declined from "Free" to "Partially Free" (Freedom House, 2019). According to the Freedom House report, the main reasons why status changed were deteriorating conduct of elections, undermining independent journalism through legal harassment and smear campaigns, and unconstitutional accumulation of power in the hands of the President of Serbia Aleksandar Vučić (Freedom House, 2019).

The disintegration of democracy in Central Europe and Central Asia is evaluated in the already mentioned report NIT. According to that report issued in 2020, the number of Hybrid regimes tripled from 2010 to 2020, from 3 to 9 (Csaky, 2020: 2-3). Serbia gained that status in the report from 2019, which is the first time Serbia is not being characterized as a democracy since 2003 (ibid.). According to the report, a hybrid

regime is characterized as formally electoral democracies with relatively high standards for the elections but with problems in protecting and defending political and civil liberties (Freedom House, n.d.).

The erosion of democracy in Serbia is perceived through Serbian President Vučić and the Serbian Progressive Party[4] (from now on: SNS), which came to power in 2012 (Fruscione, 2020). In 2020 SNS had more than 720 000 members. In other words, every ninth citizen is a member of the SNS, which means SNS has a higher per capita membership than the Chinese Communist Party (CCP) or United Russia (UR) (Ibid.). Also, SNS has more party members than some ruling parties of much more prominent parties, such as the German CDU (Christian Democratic Union of Germany), which has 407 000 party members (Lemstra, 2020: 3). There is almost consensual agreement among civil society organizations that ever since it came to power in 2012, SNS gradually worked on systematic state capture, which led to the erosion of democracy and human rights (Lemstra, 2020; PSSI, 2020). The process of state capturing implies that groups and individuals who are political actors infiltrate the state structures and establish their own "rules of the game". In that way, they can pursue their particular interests, such as the accumulation of political power and/or acquiring material and financial gain at the expense of the public good (Lemstra, 2020: 2). Clientelism is often perceived as the tool for state capture, which is an important aspect of the political mobilization in the Western Balkans and Serbia, and it refers to the exchange of political/electoral support for the material benefits between political party and citizens (ibid.).

A vital consequence of the state capture is the secrecy of information and closure of the security sector institutions to the public, media, civil society organizations, but also to the independent state bodies such as the Commissioner and Ombudsman of Serbia (PSSI, 2020: 5). Diminishing the control function of the independent state bodies was

[4] Original name in Serbian language is: Srpska napredna stranka.

also conducted by appointing people who lack the will to conduct control and oversee the executive authority or are close to the ruling party (Petrović, 2020: 16). Party patronage, the appointment of the people loyal to the ruling party, in the context of Serbia, has been one of the main ways for capturing the state institutions and the security sector, which assures that actions conducted by state institutions are in line with the interest of the party and its leader (Petrović, 2020: 14; Pejić Nikić & Petrović, 2020: 23). The control of the production of the information is established through the control of the financial resources and manipulation of the public resources, making it almost impossible for critical voices to be heard on national and local media (PSSI, 2020: 3). While there are some independent and investigative media, they are constantly targeted by the members of the parliament, president, high government officials, and members of the SNS and are pressured through different institutions such as the Tax office (Fruscione, 2020). Petrović (2020: 18) argues that this level of concentration of power in one party and one-party leader, who is currently holding the position of the country's president, has not been seen since the period of Milosevic.

Currently, there is an ongoing dialog between the opposition parties, which were boycotting the last elections in 2020, and state and ruling party representatives, under the facilitation of the members of the European Parliament (European Western Balkans [EWB], 2021a). The structure of the current Serbian parliament was chosen in the elections which were held in 2020, during the pandemic, and which were boycotted by the five biggest opposition parties because of the ruling's party monopoly over media and lack of electoral integrity, ranging from political pressure on voters to the institutional malfunctioning (Stojanović & Bértoa, 2020). The consequence of this is that in the current parliament structure the most significant number of ruling seats belongs to the SNS, which has 188 seats out of 250. There are just two more parties/coalitions, representing minorities in Serbia, with seats in the parliament besides four parties representing the ruling coalition (NARS, 2020). Today, the Serbian Parliament has almost no representatives of the opposition (EWB, 2021b).

6.2.4. Personal Data in Serbia

Although protection of personal data in Serbia is inscribed and guaranteed by Article 42 of the Constitution of the Republic of Serbia from 2006, the violations are often occurring (Official Gazette of the Republic of Serbia, 2006; Share Foundation, 2016). The institution mandated to protect and control the right to freedom of information and privacy is the Commissioner. This independent state institution was established in 2004 and at first was limited to the protection of the right to freedom of information, while after 2008 mandate was extended to protecting the right to data privacy (Share Foundation, 2018). The big change in data protection came after the adoption of the Law on Personal Data Protection[5] (from now on: LPDP) in 2018, which replaced the old one from 2008, and came into force in 2019. This new Law is considered to be mostly harmonized with the regulation in EU and thus represents modern regulation that is more in line with the development of the technology which allows automatic collection and processing of vast volume, variety, and velocity of data. This new LPDP represents an adapted translation of the General Data protection Regulation (from now on: GDPR) and Police Directive of the EU (Krivokapić, et al., 2019). However, although the law, according to the digital rights organizations, represents the highest normative act of data protection, there are still shortcomings in the way that is written and especially in the way it is applied in real life (Krivokapić, et al., 2019: 13-14; Živić, 2020; Nikolin, 2019). Regulation in this sphere was very rarely implemented in real life partly because of the "low level of culture of data protection" (Krivokapić, et al., 2019: 14).

Civil society organizations, since the beginning of the monitoring of the Digital Rights in Serbia, just as the Commissioner, noted many violations of the Law on Data Protection and abuse of the personal data by the public authority institutions and

[5] Law is adopted on 9 November 2018, and it is applicable from 21 August 2019 (Paragraf, n.d.).

security sector for the purpose of compromising political opponent and intimidation and surveillance (Perkov et al., 2019; Živić, 2020). Personal data often leaks from public institutions due to low information security, education, and ignorance (Živić, 2018; Živić, 2019). One of the most staggering cases of data leaks happened in 2013 when the link towards the database of the Agency for privatization[6] was circulating on social media platforms (Share Foundation, 2018: 28). The database contained personal data[7] of more than 5 million people, almost all the adult population in Serbia (ibid.; Perkov et al., 2019: 46). Although this database was completely legally assembled, it was illegally shared on the internet and thus violated the people's privacy rights (Perkov et al., 2019: 44). There are also cases when databases are created illegally, for example, the case with the database created for the profiling of citizens by an unknown political party in Serbia, when the personal data of 400 thousand people was created and stored (ibid.). One of the descriptions of voters from such a database was: "6209: So far voted for DS. Won't do that anymore. Disabled. Children 20 and 22 years. Unemployed, the wife works in a pub for 11,000 RSD. He is disabled person from Bosnia" (Ibid.).

Besides massive leaks of databases and their illegal creation, there are also cases when personal data, which are contained in the state institutions, such as hospitals and police, are used for intimidation or compromising of political opponents, journalists, and critics (Commissioner for Information of Public Importance and Personal Data Protection [Commissioner], 2017; Glas Amerike, 2019; Perkov et al., 2019: 44).

Data from the monitoring of the invasion of privacy conducted by civil society organizations show that victims of privacy invasions are most often citizens, and entities who are committing the privacy invasions are most often state institutions (Kovačević, 2021). For example, during the COVID-19 pandemic, there were also cases of exposing the personal data collected through the centralized information

[6] Active between the 2001 and 2016 (Nova ekonomija, 2016).
[7] Personal number, name, middle name, surname, and information about the status in the base of the holders of the right on the free shares.

system called “Informacioni Sistem Covid – 19”, which the public health institutions used for contact tracing and getting patients’ information for the suppression of the pandemic (Share Foundation, 2020). Namely, credentials for logging into the centralized government system were publicly exposed, a clear sign of inadequate organizational and technical measures for personal data management (Ibid.). Also, this was just one of the many cases of invasion of informational privacy noted by the civil society organizations during the COVID-19 pandemic in the region of the Balkans (Čubrilović, 2020; Kovačević, 2020).

7. Analysis and Interpretation

To uncover how data colonialism operates in the case of the "Safe City" project in Belgrade, but also how it is contested through the work of the "Hiljade kamera" initiative, I will provide the answers to the three research questions that I posed before:

> **RQ1:** How can colonization through data potentially occur in the case of the "Safe City" project in Belgrade?
>
> > **RQ1.1:** How might the extraction of data influence different social actors?
>
> **RQ2:** How the "Hiljade kamera" initiative opposes the process of colonization through data in the case of the "Safe City" project in Belgrade?

Since this is explorative research that aims to discover new spaces of application of the theoretical concept of data (de)colonialism, I will try to analyze the "Safe city" project in Belgrade. To do that, I will use the decolonial lens and focus on the following characteristics of data colonialism: rendering the world through data and its appropriation, fueling the power and capital, or working in the interests of those who control it. The theoretical interpretation will follow data analysis.

Firstly, I will outline the characteristics of the "Safe City" project in Belgrade and how biometric data is imagined to be produced within the system by examining material infrastructure, its capabilities to produce data and knowledge, and also discuss the legal status of data extraction. I will discuss how datafication and data centralization affect different social actors (citizens, government, political elite, and private companies). Finally, I will discuss decolonial elements around the "Safe city" project in Belgrade manifesting through the "Hiljade kamera" initiative.

The symbol *** is used to distinguish between citations from different interviews that belong to the same theme/subject to which interviewees are referring. All the words in brackets () within the cited text from the interviews are my comments, making it easier to understand what interviewees are referring to. Symbol (…) refers to the place in interviews left out due to irrelevance that either belongs to the same sentence as the cited text or sentences before/after the cited text.

7.1. Data Colonization in the "Safe City" Project in Belgrade

This section will describe how biometric data extraction is made possible by technology, what capabilities the system of "Safe City" is designed to have when fully established but also how datafication might affect different social actors. This section will provide answers to RQ1 and RQ1.1.

7.1.1. Infrastructure for Data Extraction: From Face to Personal Biometric Data

As revealed in Data Protection Impact Assessment (from now on: DPIA), by the end of the implementation of project "Safe City" in Belgrade, a total of 8100 cameras with the software for face detection, will be installed (MIARS, 2020: 6). Out of that number, 2500 fixed and movable cameras on the pillars or objects in public use; 3500 cameras for audio and video recording, which is considered an essential part of the police equipment; 600 fixed cameras on the police vehicles and 1500 body cams on police uniforms (MIARS, 2020: 7). Data collection and analysis are backed with the key hardware characteristics, which made possible the rendering reality into measurable objects and later use of it. Human faces are datafied in the project through

the synergy of the latest video and AI technology achievements, which makes intelligent video analysis possible (MIARS, 2019b: 22).

The "eyes" of the system are cameras, which possess the capability to film and recognize the objects and faces from the continuous video material. Three types of cameras are installed which can be used for biometric surveillance; the camera types identified by the digital rights activist and acknowledged by Huawei documents are IPC6625-Z30[8], IPC6225-VRZ-ES[9], and IPC6285-VRZ[10] (Hiljade kamera n.d.a, n.d.b; Crnjanski, 2020). All these types of cameras support intelligent video analysis. Cameras can differentiate between objects such as cars, people, faces, and abandoned objects. Video feed from the cameras is then transmitted and monitored in real-time using the system VCN3020[11] (Hiljade kamera, n.d.a). Data is then stored with the system OceanStore[12], which combines high storage efficiency and security according to the supplier specifications. Certainly, the brain of the "Safe City" and the one that enables usage of the data gathered through the video surveillance represents the system of the intelligent video analysis VCM5020[13], which allows the search for the faces and the objects according to the given parameters, which were filmed by the intelligent cameras.

An IT expert, Interviewee 2, describes the "Safe city" in Belgrade as the "centralized infrastructure which has a huge peripheral part.". These cameras already have object detection capabilities and make the difference between the different objects (i.e., body, car, and suitcase). This is the initial datafication that I call "datafication by the specification of technology" since this process is essentially a characteristic of the camera itself, which is capable of autonomously converting human life into data

[8] (Huawei, n.d.a).
[9] (Huawei, n.d.b).
[10] (Huawei, n.d.c).
[11] (Huawei, n.d.d).
[12] (Huawei, n.d.e).
[13] (Huawei, n.d.f).

through the categorization (Mejias & Couldry, 2019). Although this categorization process is usually found at the end of the spiral of the data relations, in the context of the "Safe City" project, it represents the entry point (Couldry & Mejias, 2019a: 29). That is because biometric data can only be generated from human bodies, so human faces initially have to be isolated from the rest of the materials for future analysis. After that, the datafied signal is sent through the closed network to the Police Command Center in Belgrade, from where it is possible to monitor the system, analyze the video feed and datafied content, physically move cameras, and conduct zoom-in/out. The analytical part of the system allows reverse search based on the face image or by chosen parameters (name, biometric data, time). Also, the system allows advanced search, which could provide information about where the person of interest was spotted in a specific period of time, with whom that person met, or how long they stayed at the specific address. Also, parameters could be used as the notification triggering mechanisms. If a chosen parameter (i.e., a specific person) is being spotted, it will send the notification about it.

According to Interviewee 2, this system is "very economical" since it saves the video record according to the trigger parameters (unknown to the interviewee and public). At the same time, the rest is being converted and stored in quantified format. The trigger parameter is a decision-making function possessed by the software, allowing it to autonomously initiate action (trigger) under some conditions (parameter). While the action is known, and that is saving the video record, the parameter or conditions under which the system will autonomously do that are unknown. Interviewee 2 explains: "It (system) will certainly quantify and register every time it recognizes your face in its database, but it may not keep a (video) recording of the event itself".

In the DPIA (MIARS, 2020) is stated that video surveillance system collects biometric data which relates to the bodily characteristics of the face of the person which is filmed by the camera; data about the health of the individuals, registering the number

of the vehicle, the color of the vehicle, and characteristic signs (ibid.: 7). Also, the system possesses the capability of behavior analysis, as stated in the DPIA (Ibid.). In the interpretation of Interviewee 2, behavior analysis represents movement analysis: "It is (…) movement analysis. Behavior in a social sense cannot be recognized. The pattern you walk, speed and so on (…) it can in some way recognize and build your profile." This "profile" is, in fact, a Unique Identifier (from now on: UID), code or number in the system which differentiates between individuals in the system records and which can be used, as Interviewee 2 noted, to create "data doubles" (Haggerty & Ericson, 2000) or profiles of the people who are differentiated based on biometric data.

FR in the system of the "Smart City" in Belgrade is the tool through which biometric data is being "extracted" from bodies in the form of seamless data flow and turned in the "data doubles" so that it can be more easily controlled and accessed by those who are in charge of the system-the government (Haggerty & Ericson, 2000: 606). As the concept of surveillance assemblage suggests, data flows from different sources are being integrated into data abstracts called data doubles (Ibid.; Couldry & Mejias, 2019b: 345). In the case of "Smart City" in Belgrade, data doubles are filled with the biometric and behavioral data and the interviewees and documents of MIARS suggest from the other sources such as biometric personal documents registry (MIARS, 2020). In literature, this phenomenon is known as "control creep", a concept which emerged after September 11 to address the growing practice of using the data generated for civil purposes for profiling and surveillance (Kitchin, 2014: 219; Innes, 2001).

7.1.2. The Legality of Data Colonialism

One important aspect of framing the data extraction is the legal framework. Besides the national legal framework, this also includes international declarations such as the Universal Declaration on Human rights and the European Convention on Human

rights, which the Government of Serbia is obliged to enforce. In today's world, privacy protection became the essential part of the liberal democracies, one that is inscribed in constitutions and in-depth reasoned by laws and regulations such as LPDP in Serbia or GDPR in the EU (Kitchin, 2014: 212). These legislations give specific personal rights to the individuals regarding their data, such as the right to control it through the provision of consent to those who collect it and process it, but also the "right to be forgotten" (Ibid.; Wolford, n.d.). Data collection must be conducted according to the privacy regulations and consumer-rights constraints, although that is usually not the case in practice, particularly not in developing countries (Arun, 2020: 590-600; Couldry & Mejias, 2019a: 52).

In the case of "Safe city" in Belgrade, legal experts, and activists I interviewed, claim that the collection and the processing of biometric data through FR, are not foreseen in the legal framework of the Republic of Serbia. The Commissioner also notes this fact, but regardless of that, installing the cameras, which have FR technology, has continued as part of the "Safe City" project (Commissioner, 2019). Also, lack of transparency and deliberation regarding the project implementation is one more aspect that is in collision with the existing LPDP, which in Article 5 defines the data processing principles[14]. All requests that activists have sent to the MIARS (based on the free access to the information of public importance) were denied, and details about it were declared state secret.

> *In our regulations, the use of face recognition system is not foreseen. Video surveillance is. There are bylaws that provide the use of biometrics, but it is not at the level of law that it should be. Another thing, even if there is such a possibility in a law, all those other elements of the LPDP, such as transparency, to inform people about how you will treat their data, their rights, and even the guidelines of the Council of*

[14] Principles: legality, fairness, and transparency; constraint on the purpose of processing; data minimization; accuracy; storage restriction; integrity and confidentiality; responsibility for action (Paragraf, n.d.).

Europe for participatory public processes where it is discussed, etc. we don't have it, it's not part of this story and it doesn't seem that it will be.

(Interviewee 5)

***

The Commissioner said that the collection of biometric data is illegal. What are the reasons for that?

(PK)

There are several reasons. One reason is that in our regulation, biometrics is not regulated at all. As a means of evidence, the police does not have the possibility of using biometric surveillance. But there are general principles of personal data protection, which are proposed by the Law on Personal Data Protection, which clearly state that the use of such a system is neither legal nor legitimate.

(Interviewee 3)

7.1.3. "Two winners and one looser"

While in historical colonialism, racism and eurocentrism made the colonial acquisition of land and slavery available to capital, today data is fueling the power of government and companies through the process of data colonialization (Quijano, 2000; Van der Spuy, 2020). This process of power and profit gain depends on the social circumstances of data use, and that is to say, the way in which data is being framed, generated, stored, analyzed, and used (Kitchin, 2014; Dalton and Thatcher, 2014). CDS' approach to the analysis of data use suggests that we should approach it as if it is never raw, but created by people, their interests, and goals. As such, data represents the consequence of human construction, interpretation, measuring, defining and decision (Dalton and Thatcher, 2014), just as Kitchin and Lauriault (2018: 17) ask: "Who controls 'big data', their production and analysis? What motives and imperatives drive their work?" I hold those are crucial questions to be asked when conducting analysis of the case of whichever social fact. That said, the further goal is to find the answer to RQ1.1: How might the extraction of data influence different social actors?

7.1.4. A Synergy of Interest of the Private Company and Political Elite

In the contemporary era, data colonialism aims to acquire the bodies and human life through data, which is often legitimized or justified though claiming that it is advancing scientific knowledge, allowing rational management (Couldry & Mejias, 2019a), helping to fight crime, and modernizing the police work (ibid.; MIARS, 2020). As such, video surveillance with the capability of facial and plate recognition can contribute to the 3E (efficient, economical, and effective) police work in protecting the citizens' safety, and the MIARS sees it as an indispensable part of the modernization of the police work (MIARS, 2020: 3). My interviewees argue that the real beneficiaries from the data extraction through "Safe City" project in Belgrade are the private company Huawei, the state apparatus, and the political elite. The interviewees point out that interests behind the "Safe City" project are questionable, since this kind of technology is incapable of curbing the more resilient type of crimes such as organized crime and terrorism, which is why the system is being implemented in the first place according to MIARS. Also, they argue that Belgrade is compared with some other capitals of Europe safer place to live, which some data shows (Numbeo, 2020).

> *You mentioned the context and to whom the biometric data might be of use. (…). Who are the potential losers and winners, if any?*
>
> (PK)

> *I can't put security on that list. Will the citizens get security? Because we don't have that low level crime, there is no pickpocketing on the streets (…). We will neither solve organized crime nor we have terrorist attacks. We have no need for all that this system could provide, and then I cannot say that the citizens will get something out of it, even though I would like to say that (…). Belgrade is not an unsafe city, even on the periphery. In Paris, London you can't go around some parts of the city as easily and*

safely as you can in Belgrade, so it is logical to me that London has a strong CCTV system.

(Interviewee 1)

***

To whom do you think that (biometric data) might serve?

(PK)

Well, to the MIARS, they did it for themselves. Because you, as a citizen, get absolutely nothing. Will you get a safer city? All research shows that, firstly, Belgrade is not unsafe, and secondly, such a system does not protect against mass security threats such as terrorism. You came to prevent the theft of cars, bicycles, and that is not an essential threat. And the benefit is (…) *I don't see it.*

(Interviewee 2)

In the case of the "Safe City" project in Belgrade, data colonization is unfolding as part of a private-public surveillance partnership between state institutions and private company Huawei (Couldry & Mejias, 2019a: 123). That is to say, it has internal data colonialism aspects because the main beneficiaries of data extraction are internal actors, above all the security apparatus and political elite (Couldry & Mejias, 2019a: 24). But also, external actors, most notably, Chinese company Huawei is an important profiteer[15] of the project since all the equipment is manufactured by it.

Are there any potential losers and winners in relation to that collected personal data?

(PK)

Two winners and one looser. One is our Ministry of the Interior. It's like killing a fly with a canon instead of a flytrap. Certainly, there is Huawei, which got a lot of money. What is even more important for Huawei, is that it got a breakthrough in the European market. You now have a capital city in Europe that has covered its entire territory with this technology. This represents examples for both Poland and Hungary, and for Bosnia and Montenegro, even Romania, Bulgaria, Czech Republic, and Slovakia. Even

[15] I am conscious that this qualification comes with this word. However, it could not be more appropriate to describe their activities on the project, which is illegal to use and if in use violates human rights and personal autonomy.

> *for France and the Netherlands, I do not exclude them, they are not immune to such things either. It is much easier when there is an example that exists here, it is not the technology that exists far away in China, we are now talking about something right next to us. It will not be difficult to force Orban, no one will force him, he will introduce this himself, so the next time someone goes out on the street, he will know exactly who it is. (…) You can't have public interest in your mind and implement this, this is the particular interest of a certain elite that decides this will work and that has the resources to buy things like this.*
>
> (Interviewee 2)

So, as it can be seen, it is not just the direct monetary gain that Huawei is gaining from the project of the "Safe City". By implementing the project and its latest FR, Huawei is also gaining a presence in the European market, which is part of the strategic goal of China. Disproportionate usage of the technology for collection and processing of data, together with the untransparent and secret procurement behind the project, supports the argument that there is a particular interest of the national political and international economic elite. As a result, the domestic political elite could gain more effective control over the public spaces and over its citizens. According to Couldry and Mejias (2019a), data colonialism is the global and universal social order which is exploiting the data for economic gain. The case of "Safe City" project in Belgrade suggests that there is also a specific political interest behind the data exploitation, which is rooted in the specific social context of Serbia, most notably the captured state.

> *The current government and that political structure would definitely be at the top of the list of winners, which can be used against them when they are no longer in power. They are definitely winners because it increases their control.*
>
> (Interviewee 1)

The absolute losers from the project of the "Safe city" are, according to my interviewees, citizens and their sense of freedom and autonomy. In literature, some

authors like Couldry and Mejias (2019b: 346) call for the protection of "minimal integrity" from omnipresent surveillance and data extraction, which tends to penetrate all aspects of our lives and erase the border between us and the system. One possible direct harm to the citizens could be done through data misuse, which represents illegal actions against citizens' privacy. The existing shortcoming in the rule of law in the privacy domain makes my interviewees very skeptical that the procedures will be respected once the system is in use. This depends on who will be able to derive the knowledge from data and for what it will be used.

> *How do you see the possibilities for abuse? You did mention at one point the political repercussion of that data that would be stored when this system is operational?*
>
> (PK)
>
> *This is the biggest fear, in fact, that these systems are run by people and that the centralization of power that will happen, and that is happening, will allow them to use it as a mechanism to intimidate opposition and dissidents, suppress activism where it still exists and blackmail opponents. You name it. It can be used so creatively that anyone who questions anything can be discredited because they pull out a folder with information about where he/she was and what they were doing at a certain moment. With all my efforts to believe that the main purpose is security, I have never received enough information about how unsafe Belgrade is. Especially since we had information about how Belgrade is a safe place to live, how the crime rate has been reduced, and it seems to me this is just at the moment when the cameras started to be installed. What is the reason? Has anyone done an analysis? (…) All this brings me fears about abuse. Because we had data leaks, and we have them in the media all the time. In fact, they are not leaks, they are classic misuse of (personal) data pouring in for the needs of some political confrontations and discrediting happening in the tabloids. It happens even without this system (FR). Journals were pulled out of psychiatric clinics, diagnoses were read in live programs, all this was done by officials. I'm just not convinced that this system will be used any differently.*
>
> (Interviewee 5)

The scenarios in which the personal data might be used for the oppression are depending on the interests of those who are in control of the personal data, the system of control over the data, enforcement of law, but also in the fact that this data is being

extracted in the first place. Although data colonialism is most notably linked to the monetary gain of the private sector in the literature (Couldry & Mejias, 2019a, 2019b), in countries like Serbia, the process of state capture has made boundaries between the public and private sphere blurry at least.

> *It gives you the opportunity to follow everyone in the city without being targeted, which is the biggest problem, you can commit all the abuses in this position, whether you will blackmail political opponents or some others. This system, when fully operated, can enable some directors of the public enterprise to check whether his employees were on the protest. You just list, these are my employees, these are their pictures, find me matches from yesterday's protests. That is the level of science fiction movies, what you can do with it.*
>
> (Interviewee 3)

Interviewees see the great risk in the merging of data from other registries with the one collected through the system, which could be:

> First, the database that is kept in a centralized place is the systematic supervision of one authority that simultaneously handles other data that can be easily determined by a person. Not only are they from the arrest warrant, we are talking about a government body that has all ID cards, information about the residence, stay, citizenship, and these are all records in one place. The possibility of networking these databases already exists.
>
> (Interviewee 4)

One interviewee claims that this technology is not fully precise. For example, it might often make mistakes falsely recognizing someone else since it calculates the probability of the match in its analysis (MIARS, 2020). As one interviewee noted:

> (…) each part of the code, i.e., the software that is made, contains a certain type of discrimination. In the technical sense, discrimination does not imply everything that it

> implies in the human rights, social sense. It does not mean that it a priori discriminates against one or the other. However, each product actually incorporates certain types of bias that someone has installed in them. As you have probably seen it, facial recognition (technology) recognizes black people as monkeys, black women in particular. (…) that is a racial bias, you can have different levels of bias that aren't even intentionally built-in, but simply intuitively built-in. If white men are the main basis on which a certain algorithm is trained, it will recognize white men most efficiently, and everything else will have a bigger risk of error. When it comes to errors, this system is not flawless. However, striving to make this system more accurate is very problematic for two reasons. Firstly, the manufacturer will then say that it needs an even larger set of data in order for the system to be accurate, which means that it violates the privacy of citizens further on, and on the other hand, if it is so precise, then it can be an even more powerful weapon. That's why we don't advocate it. Our campaign is based on banning this technology practically everywhere because it is conceptually corrupt. You can't fix it in any way.
>
> (Interviewee 2)

7.2. Contesting Data Colonialism

In this part of I analysis, I will focus on the process of liberation from data colonialism in the case of "Safe City with the aim of answering RQ2: How the "Hiljade kamera" initiative opposes the process of colonization through data in the case of the "Safe City" project in Belgrade?

A group of human rights activists, individuals, and organizations are gathered in the initiative "Hiljade kamera" which advocates for the responsible use of surveillance technology (Krivokapić et al., 2021: 2). The Share foundation leads the initiative to protect the "privacy and dignity of all citizens" (ibid., 9). The initiative started the website that provides all the known information about the "Safe City" project in Belgrade and opens the way for citizens to fight for transparency and raise awareness about biometric surveillance. In November 2020, the Initiative launched the petition (Hiljade kamera, 2020a) for the ban of biometric surveillance technology in Serbia, which was signed by 16 800 people, and which is part of the wider civil society organizations movement gathered around advocacy group European Digital Rights

(EDRi) for the ban of the biometric mass surveillance in the EU (European Digital Rights, 2021). The work of the initiative is financed through the crowdfunding campaign, which managed to raise 9000 EUR, around one million Serbian dinars, which is a rare model of financing in the Serbian civil sector-which mainly depends on foreign donations (Krivokapić et al., 2021: 10; United States Agency for International Development, 2012: 176).

Their contestation of the Safe City project contains both the elements of fighting the massive CCTV and biometric surveillance, which is sometimes hard to differentiate because both are interdependent phenomena tackled by activists and their actions. I will elaborate the process of the data decolonization, from the top-down datafication of the public places, through the contestation politics of data. This means that I will focus on policies and activities that contest dominant power relations and narratives regarding data extraction (Beraldo & Milan, 2019).

The data contestation politics of the "Hiljade kamera" initiative could be seen as both narrative and power contestation of MIARS. I identified raising awareness and mobilization of the community as direct tools for challenging data colonialism. Furthermore, research and data collection could be perceived as indirect but still a very important part of contesting the "Safe City" project in Belgrade. It is interesting to mention that "fighting" is exactly the word used by the activists to describe the actions targeted towards the "Safe City" project in Belgrade. This indicates a resemblance with the vocabulary of the liberation movement in the era of historical colonialism, which fought for national and political freedom. Activists who are members of the "Hiljade kamera" initiative fight for territories to be freed from massive and biometric surveillance in Belgrade.

"Hiljade kamera" initiative is a group of activists that does not have the legally defined status and organizational structure, but still functions as a stable grassroots movement of digital rights activists gathered around the Share Foundation. Their work

started spontaneously, with a mission to challenge the official narrative around the "Safe City" project which was that it will increase safety in Belgrade.

> *From the start, when we heard Stefanovic's statement that Belgrade will receive mass biometric surveillance, which we have been afraid of for a long time because we are privacy enthusiasts and lawyers, we immediately started thinking about how to bring this topic into public discourse and create a counter-narrative. Since their basic narrative is that it is a great project, we are aware that there must be a counter-narrative that it is not necessarily just good.*
>
> (Interviewee 1)

7.2.1. Research and Data Collection

The first information about the "Safe City" project was publicly announced in 2017 when the minister of MIARS announced the beginning of the pilot project of the installation of smart video surveillance. However, the real scope of the project was unknown to the public until 2019 and 2020, when the first and second DPIA was published (Vladisavljev, 2019). Although the official information about the project was changing over time, it was clear from the beginning that there will be thousands of cameras in Belgrade, which will cover the whole city with the software for the face and car plates recognition (Danas, 2019b). This idea was manifested in the minister of the MIARS, which famously formulated the idea behind the "Safe city" project in Belgrade in his announcement of the project implementation: "There will be no significant street, entrance, or passage between buildings left uncovered by cameras. Therefore, we will know from which car, entrance or building the perpetrator came."[16] (N1, 2019).

Despite the ongoing pressure on the MIARS by the civil society organizations to publish the whole project documentation, that never happened. Instead, information

[16] Original sentence: "Neće biti značajnije ulice, ulaza ili prolaza između zgrada koji neće biti pokriven kamerama. Znaćemo iz kog ulaza i zgrade je počinilac došao, iz kojeg automobile".

about the project came to the public selectively through the officials who have been announcing the beginning of the implementation of the project since 2017. Also, information was gathered from a case study on the Huawei website, which soon after the revelation of the civil organizations was deleted but archived. Another source of information of the project came as the consequence of the LPDP. This law made it mandatory that before processing the personal data with a high risk on the rights and freedoms of the individual's processor must assess that risk in the form of DPIA which has to be approved by the Commissioner before the processing starts (Paragraf, n.d.; Krivokapić et al., 2021: 8).

MIARS submitted the first DPIA for the new video surveillance system to the Commissioner in September 2019 (Commissioner, 2019). That document was rejected since it did not meet the legal requirements which are set by the LPDP (Krivokapić et al., 2021: 8). In April 2020, MIARS submitted a second DPIA, which satisfied all the legal requirements and thus was fully assessed by the Commissioner (MIARS, 2020; Krivokapić et al., 2021: 9). However, it was rejected because the government does not have a legal basis for collecting personal biometric data from video surveillance of public places (Krivokapić et al., 2021: 9). Also, it is stated that MIARS have not delivered documents to which DPIA is referring such as “Safe city” and “Safe Society” and did not confirm nor deny whether the team has already started with the processing of the personal biometric data (ibid.). In mentioned DPIA documents, the size, and the scope of the “Safe City” project is revealed. As noted before, conceptual and legal difference between the projects of “Safe City” and “Safe society” is unclear and has not been clarified by the MIARS. As such, in my thesis, “Safe City” refers to the ongoing activities on the installation of video surveillance technology in the city of Belgrade, often referred to by the MIARS as the “Safe Society” project in Belgrade.

One important part of the whole “Hiljade kamera” initiative is research and data collection, which turned out to be very important for informing the public about the project, since institutions were not making it available to the public before the start of

the project. With the lack of the information provided by the MIARS, activists were in some way substituting with their own research. Knowledge and understanding of the extraction system is the first step towards data decolonization, in other words, understanding material circumstances that make data extraction possible (Mohamed et al. 2020: 664).

> *As for the 'Hiljade Kamera' initiative, we started it two years ago when the then Minister of Police (this is colloquial name used to refer to the MIARS) Nebojsa Stefanović, stated that there would be no part of Belgrade that cameras would not cover. Our initial reaction was in the direction of let's see what this means, what these people are doing, and what do they want to do. They didn't even start installing cameras then. It came later. We have gathered a group of experts first of all. In that sense, it is grassroots, but what is specific is that the initial step comes from the sphere of knowledge, expertise, and study of all that. It is an activist movement that fights against something without working, I am not saying that it is a small job, but it also includes the mass research and research work behind it all. (...) us, as researchers, need to learn what the possibilities of this technology are when you see a camera on a pole, but you don't know how it works. We mapped out the whole system, how it works, a logical map of how and where the system collects data, how to train a face recognition model based on artificial intelligence on that AI chip that Huawei patented and produced and now uses, it has been practically in use since a year and a few days ago. We did that in order to see what our Ministry, law information agencies will have available as a resource.*
>
> (Interviewee 2)

The two legal bases for gathering information from public institutions are the LPDP and the law on the free access of information. Although, the latter one was not useful for the activist because MIARS declared information concerning the project as secret. MIARS was obligated to develop the DPIA, which as for now, represents the most concise information regarding the project.

> *(...) (requests based on) Law on Free Access to Information of Public Importance was not particularly successful because the MIARS did not answer us. Our main tool was the DPIA based on the LPDP because MIARS is obliged to draft this document if it plans such a surveillance system. Through that, we managed to find out a lot about it. The police did not provide us with that document, but the Commissioner provided us*

with the document (...). What is great is that the Commissioner said that there is currently no legal basis for biometric surveillance of this kind. (...) Our Commissioner said that there are currently no legal conditions. The move is now on the police to see how they will solve that problem.

(Interviewee 3)

Knowledge about how data is collected and how the system functions in the project "Safe City" becomes even more critical when the government hides information from the public. Also, to me, it seems that research and information collection are essential for raising awareness and community mobilization.

7.2.2. Raising Awareness

Raising awareness regarding the data collection in the case of the "Safe City" is seen as the opportunity to communicate the ideas about other issues regarding the digital rights for which activities are advocating, but which "overlap" with the questions raised as the part of the "Safe City". So, fighting against the mass biometric surveillance in Belgrade is seen as the chance for the education of the public and explaining the relationship between the use of data and surveillance in both public and private sectors. Important aspects of raising awareness are the data and information activities that provide the information to communicate with the public.

People understand this problem much better than other issues in the field of digital rights because here, you have something in the physical space, you have a camera, and you see it. It's not like you have a tracker or cookie in your browser, or you don't understand it. The camera is still something that people understand. At the same time, the fact that we are a post-socialist society, where you had the paranoia about

> *'OZNA'[17] following you constantly and taking care of everything, plays a big part. Then it's etched in people's brains, that paranoia, so they can understand what's going on much faster than when we start talking to them, well people, do you know that Facebook knows everything you do when they say let me click accept and yes I'm moving on. It comes to mind much faster that these issues overlap.*
>
> (Interviewee 2)

The main channel of distribution of information regarding the activities concerning the contest from the beginning was the website of the "Hiljade Kamera" initiative, engaging the citizens and mobilizing for action.

> *When we figured out how to deal with it, we created a micro-website where we tried to communicate that we are interested in stepping into this subject with the people who are interested in it but who are not from Share foundation, which is already interested in that. People were contacting us soon as we released that website-where it was written that this system is being established in Belgrade and called the people to contact us with the ideas, comments, and willingness to join the activities.*
>
> (Interviewee 1)

The activities around the promotion of the idea about the harmfulness of the "Safe City" project were promoted through the many articles about the activities of MIARS and the potential harms of the FR technology. Besides this, accounts on social media websites such as Twitter and public appearances on local and national media, which almost exclusively belong to the group of "independent media" in the country.

[17] OZNA is the abbreviation for Department for People's Protection (original name: Odeljenje za zaštitu naroda) often used to denote the strength of security apparatus, most notably secret service, during the Communist Regime in Yugoslavia.

7.2.3. Community Mobilization

As I mentioned, it seems that both research and data collection, raising awareness, and community mobilization are interconnected. The same people who are targets of the raising awareness campaign against the "Safe city" project also participate in collecting the information and resources that are being used to raise awareness about the harmfulness of mass and biometric surveillance.

Although the Commissioner stated that automated collection and processing of the personal biometric data (anticipated as the part of the project "Safe City") is unlawful, technology that allows this continues to be implemented day by day in Belgrade (Hiljade kamera, n.d.b).

The community of people gathered around the "Hiljade Kamera" initiative includes those interested in engaging in the "fight" and activities of the initiative. In addition, the wider public and citizens were involved through the call to map the camera by tagging "Hiljade Kamera" twitter account and sending pictures with the camera coordinates, which would then be authenticated by the initiative members.

> *When we mapped the cameras, me and my friends from the hack club took an open-source tool called a camera hunt, so we involved the community on twitter to take photos of cameras and coordinates. In addition to mapping the cameras and finding new information that we did not receive from the MIARS, we also gave people a chance to get involved, it is very important that they have a sense of fighting with us and getting involved and get a sense of helping and participating through that campaign. People took photos and sent them. It's not like we are an NGO trying to make a campaign, and it failed. It makes sense. People have become active.*
>
> (Interviewee 1)

Up till November of 2020, activists gathered around the initiative "Hiljade kamera" and volunteers identified 1001 cameras that can conduct facial recognition and collect

biometric data on 447 locations in Belgrade (Hiljade kamera, 2020b). However, the number of cameras which the digital rights activist and citizens identified does not match the list made by the MIARS, which raises serious doubts about the truthfulness of the information about the project coming from the state institutions (MIARS, n.d.; Kojić, 2021).

Also, fundraising activity was the way to engage people with the initiative since those who could not engage through writing, hunting cameras or brainstorming could pay, so that these activities can reach even more people.

> *That campaign was successful, but again, it's still a bubble now. Not a lot of people paid, maybe 400 people, some more, some less. It was another way to talk about it and give it a chance to get involved because there are tons of people who now don't want to share things on the internet but have money, so they will give money.*
>
> (Interviewee 1)

8. Summary and Conclusions

The analysis of data and its interpretation through theory gave me insight into how the data colonization might look and be distributed among different social actors. First of all, the "Safe City" project is still on its way to become a reality; its future effect, infrastructure, and capability for data extraction I attempted to reconstruct through the anticipation found in the official documents as well as interviews. I believe that data colonialism is becoming the dominant order of structuring reality and power. Those who possess the privilege also possess control over our data, and through it, over our lives. By writing and disseminating the narratives, we can resist the optimistic and capitalistic ideas that data should be a universal way of knowing reality and mediating all relations, including human.

RQ1: How can colonization through data potentially occur in the case of the "Safe City" project in Belgrade?

If the project is fully implemented, it will have 8100 cameras, out of which 2500 cameras have confirmed capability of biometric surveillance and thus extraction of the data from people's faces. These abstracted faces are converted into data and other information about when the information is recorded. Abstracted personal information is then fed into data doubles with attached UID, making analysis and search easier and integrating it with other data generated through the system, such as moving patterns and profiling. Also, UID allows integrating data records made and collected outside of the system. According to the current national legal framework, this projected extraction of data from human faces is illegal, noticed by both Commissioner and digital rights activists.

RQ1.1: How might the extraction of data influence different social actors?

There is a very clear difference in narratives about the effects of "Safe City". Government officials and documents on the one side claim that the beneficiaries of the project, and thus datafication, which is an essential part of the project, will be citizens and a safer city. On the other hand, digital rights activities and literature indicated that beneficiaries and "winners" of the project would be those who initiated the project and worked on its implementation. Theoretical propositions and the bulk of Critical Data Studies literature indicate that real winners are those in power. In the Safe City project, the interviewees identify them in MIARS, political and economic elite. While state institutions of coercion might gain more effortless accomplishment of their task, Serbia's political elite might get new sources of knowledge for oppressing political opponents and journalists. Also, Chinese company Huawei has the latest technology for data extraction, profiting both in the material sense through selling equipment and maintenance services and the excess on the European market. In that way, the Safe City project represents the case of both internal, but also external data colonization. Citizens might be considering the biggest losers from the process of datafication. Their faces are being colonized, for the purpose of surveillance which for the consequence has loss of personal autonomy. Also, data extraction and centralization opens the field of risks of data misuse and discrimination by all three identified actors profiting from the data gathered through the project.

RQ2: How the "Hiljade kamera" initiative opposes the process of colonization through data in the case of the "Safe City" project in Belgrade?

I identified three interdependent groups of activities in which the "Hiljade kamera" initiative is confronting the top-down process of colonization through data:

1. They are collecting the information about the project through research, but also through institutionally defined channels. This is challenging since there is a lack

of transparency regarding the project plan and its implementation from the beginning;

2. By raising awareness about the harmful effects of biometric and mass surveillance, they disseminate information gathered through research and data collection. They use different channels such as social media accounts (YouTube, Twitter), web pages (Hiljade Kamera, n.d.), and others to raise awareness;

3. Community mobilization is conducted through mapping the surveillance system, inclusion of citizens in planning actions against the "Safe City" project, organizing conferences and meetings, launching petitions, and finally fundraising through crowdfunding.

8.1. Suggestion for Further Research

It is essential to understand privacy and its strength as the legal norm in the Global South. Unfortunately, in Serbia, just as in many other middle and low-income countries, a legal norm of privacy is ignored. So, it stands as an open question of how this norm might be enforced to provide real protection from data colonization in case of "Safe City" projects or other similar initiatives. Also, further research is necessary to understand the role of big data in state capturing and strengthening the political elites in non-democratic contexts.

9. References

Alvial-Palavicino, C. (2016). The future as practice. A framework to understand anticipation in science and technology. *TECNOSCIENZA: Italian Journal of Science & Technology Studies*, 6(2), 135-172.

Aragona, B., Felaco, C., & Marino, M. (2018). The politics of Big Data assemblages. *Partecipazione e conflitto*, *11*(2), 448-471.

Arora, P. (2016). Bottom of the data pyramid: Big data and the global South. *International Journal of Communication*, Vol. 10.

Arora, P. (2019). General Data Protection Regulation—A Global Standard? Privacy Futures, Digital Activism, and Surveillance Cultures in the Global South. *Surveillance & Society*, 17(5), 717-725.

Arthur, C. (2013). Tech giants may be huge, but nothing matches big data. *The Guardian*. Retrieved March 2 2021, from: https://www.theguardian.com/technology/2013/aug/23/tech-giants-data

Arun, C. (2020). AI and the Global South: Designing for Other Worlds. In M. Dubber, F. Pasquale & S. Das (Eds.), *The Oxford Handbook of Ethics of AI* (pp. 579-606). New York: Oxford University Press

Bastian, J. (2017). *China's Balkan Silk Road: Examining Beijing's Push into Southeast Europe*. Reconnecting Asia. Retrieved August 1 2021, from: https://reconasia.csis.org/chinas-balkan-silk-road/

Beraldo, D., & Milan, S. (2019). From data politics to the contentious politics of data. *Big Data & Society*, 6(2). DOI: https://doi.org/10.1177/2053951719885967

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2), 77-101. Retrieved August 2 2021, from: https://www.researchgate.net/publication/235356393_Using_thematic_analysis_in_psychology

Cao, Z. (2016). *Nowhere to hide: Building safe cities with technology enablers and AI*. Huawei. Retrieved August 4 2021, from: https://www.huawei.com/ch-en/publications/winwin-magazine/ai/nowhere-to-hide

Carter, D. (2018). Reimagining the big data assemblage. *Big Data & Society*, 5(2). DOI: https://doi.org/10.1177/2053951718818194

China – CEEC. (n.d.). Retrieved August 3 2021, from: http://www.china-ceec.org/eng/

Commissioner for Information of Public Importance and Personal Data Protection. (2017). Zloupotreba podataka o ličnosti je i krivično delo [Misuse of personal data is also a criminal offense]. Retrieved from: https://www.poverenik.rs/sr-yu/saopstenja/2620-zloupotreba-podataka-o-licnosti-je-i-krivicno-delo.html

Commissioner for Information of Public Importance and Personal Data Protection. (2019). Mišljenje Poverenika na akt Ministarstva unutrašnjih poslova – Procena uticaja obrade na zaštitu podataka o ličnosti korišćenjem sistema video nadzora [Opinion of the Commissioner on the act of the Ministry of the Interior - Assessment of the impact of processing on the protection of personal data using the video surveillance system]. Retrieved August 1 2021, from: https://praksa.poverenik.rs/predmet/detalji/FB967E2A-AE57-4B2C-8F11-D2739FD85A9B

Couldry, N., & Mejias, U. A. (2019a). *The Costs of Connection: How Data Are Colonizing Human Life and Appropriating It for Capitalism*. Stanford: Stanford University Press

Couldry, N., & Mejias, U. A. (2019b). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media*, 20(4), 336-349.

Creswell, J. (2015). A Concise Introduction to Mixed Methods Research. London: SAGE.

Crnjanski, M. (2020). *Sve je više Huawei kamera na beogradskim ulicama – čemu služe i da li prepoznaju tvoje lice?* [There are more and more Huawei cameras on the streets of Belgrade - what are they for and do they recognize your face?]. Netokracija. Retrieved August 1 2021, from: https://www.netokracija.rs/huawei-kamere-beograd-171048

Csaky, Z. (2020). Dropping the Democratic Facade. In *Nations in Transit: Dropping the Democratic Façade*. Retrieved August 1 2021, from: https://freedomhouse.org/report/nations-transit

Čubrilović, M. (2020). *Privatnost i zaštita ličnih podataka u vreme pandemije Kovida-19: sa pojedinca na kolektiv* [Privacy and protection of personal data during the Covid-19 pandemic: from individual to collective]. Novosadska Novinarska Skola. Retrieved August 1 2021, from: https://novinarska-skola.org.rs/sr/privatnost-i-zastita-licnih-podataka-u-vreme-pandemije-kovida-19-sa-pojedinca-na-kolektiv/

Dalton, C., & Thatcher, J. (2014). *What Does A Critical Data Studies Look Like, And Why Do We Care?* Society and Space. Retrieved March 15 2021, from: https://www.societyandspace.org/articles/what-does-a-critical-data-studies-look-like-and-why-do-we-care

Danas. (2019a). *Privedeno nekoliko ljudi, odneto više vozila CarGo* [Several people were detained, several CarGo vehicles were taken away]. Retrieved August 1 2021, from: https://www.danas.rs/drustvo/cargo-u-toku-akcija-oduzimanja-vozila-clanu-udruzenja-u-novom-beogradu/

Danas. (2019b). Policija postavlja oko 1.000 novih kamera u Beogradu [Police are installing about 1,000 new cameras in Belgrade]. Retrieved August 1 2021, from: https://www.danas.rs/politika/policija-postavlja-oko-1-000-novih-kamera-u-beogradu/

Daskal, E. (2018). Let's be careful out there…: how digital rights advocates educate citizens in the digital age. *Information, Communication & Society*, 21:2, 241-256. DOI: https://doi.org/10.1080/1369118X.2016.1271903

DATACTIVE. (n.d.). *The Big Data from the South.* Retrieved August 3 2021, from: https://data-activism.net/publications/big-data-from-the-south/

Dimitrijević, D. (2017). Chinese Investments in Serbia—A Joint Pledge for the Future of the New Silk Road. *TalTech Journal of European Studies*,7(1), 64-83. DOI: https://doi.org/10.1515/bjes-2017-0005

Euronews. (2021). *Serbia in 'world first' as citizens offered €25 to have COVID vaccine*. Retrieved August 1 2021, from: https://www.euronews.com/2021/05/05/serbia-in-world-first-as-citizens-offered-25-to-have-covid-vaccine

European Digital Rights (EDRi). (2021). *ReclaimYourFace and help prevent the end of privacy as we know it!* Retrieved August 1 2021, from: https://edri.org/our-work/reclaim-your-face-and-help-prevent-the-end-of-privacy-as-we-know-it/

European Western Balkans. (2021a). *EP-facilitated Dialogue in Serbia: First meetings concluded, possible arrival of MEPs in June*. Retrieved August 1 2021, from: https://europeanwesternbalkans.com/2021/05/10/ep-facilitated-dialogue-in-serbia-first-meetings-concluded-possible-arrival-of-meps-in-june/

European Western Balkans. (2021b). *Opposition in Serbia: The Assembly has no legitimacy for constitutional changes*. Retrieved August 1 2021, from: https://europeanwesternbalkans.com/2021/04/12/opposition-in-serbia-the-assembly-has-no-legitimacy-for-constitutional-changes/

Ferguson, A. G. (2019). *The rise of big data policing: Surveillance, Race, and the future of law enforcement*. NYU Press.

Freedom house. (2019). *Freedom in the world*. Retrieved August 1 2021, from: https://freedomhouse.org/country/serbia/freedom-world/2019

Freedom House. (n.d.). *Nations in Transit Methodology - 2020*. Retrieved August 4 2021, from: https://freedomhouse.org/sites/default/files/2021-04/NIT2020_Methodology_WEBSITE.pdf

Fruscione, G. (2020). *Serbia: From Milosevic to Vucic, Return Ticket*. ISPI. Retrieved August 3 2021, from: https://www.ispionline.it/it/pubblicazione/serbia-milosevic-vucic-return-ticket-27699

Gallagher, B. (2020). *The amount of data in the world doubles every two years*. Medium. Retrieved April 5 2021, from: https://medium.com/callforcode/the-amount-of-data-in-the-world-doubles-every-two-years-3c0be9263eb1

Giacaglia, G. (2019). *Data is the New Oil*. Hackernoon. Retrieved March 5 2021, from: https://hackernoon.com/data-is-the-new-oil-1227197762b2

Glas Amerike. (2019). *Huavei nadzorni sistem u Srbiji: Život u senci Velikog brata* [Huawei surveillance system in Serbia: Life in the shadow of Big Brother]. Retrieved August 1 2021, from: https://www.glasamerike.net/a/huavej-beograd-kamere-kina-nadzor-/5128298.html

Gray, M. (2003). Urban surveillance and panopticism: will we recognize the facial recognition society? *Surveillance & Society*, 1(3), 314-330.

Greitens, S. C. (2020). *Dealing with demand for China's global surveillance exports*. The Brookings Institution. Retrieved March 5 2021, from: https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200428_china_surveillance_greitens_v3.pdf

Grubić, J. & Kranner, L. (2019). *Serbia's increasing importance for China's BRI*. Discover CEE. Retrieved August 1 2021, from: http://www.discover-cee.com/serbias-increasing-importance-for-chinas-bri/

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British journal of sociology*, 51(4), 605-622.

Harari, Y. N. (2018). *Why fascism is so tempting and how your data could power it* [Video]. TED Conferences. Retrieved March 5 2021, from: https://www.ted.com/talks/yuval_noah_harari_why_fascism_is_so_tempting_and_how_your_data_could_power_it?language=en#t-903

Higgins, A. (2021). *As Vaccinations Speed Along in Serbia, the Country Basks in the Glow of a Successful Campaign*. The New York Times. Retrieved August 1 2021, from: https://www.nytimes.com/2021/03/17/world/europe/as-vaccinations-speed-along-in-serbia-the-country-basks-in-the-glow-of-a-successful-campaign.html

Hiljade kamera. (2020a). *Ne snimaj mi lice* [Do not record my face]. Retrieved August 1 2021, from: https://hiljade.kamera.rs/sr/peticije/ne-snimaj-mi-lice/

Hiljade kamera. (2020b). Spisak kamera [List of cameras]. Retrieved August 4 2021, from: https://hiljade.kamera.rs/Documents/SpisakKamera.xlsx

Hiljade kamera. (n.d.a). Retrieved August 4 2021, from: https://hiljade.kamera.rs/en/home/

Hiljade kamera. [@hiljadekamera]. (n.d.b). Twitter. Retrieved August 4 2021, from: https://twitter.com/hiljadekamera

Hillman E. J., & McCalpin M. (2019a). *Watching Huawei's "Safe Cities"*. Center for Strategic and International Studies (CSIS). Retrieved April 5 2021, from: https://www.csis.org/analysis/watching-huaweis-safe-cities

Hillman, E. J., & McCalpin, M. (2019b). *Will China's '16+1' format divide Europe?* Center For Strategic & International Studies (CSIS). Retrieved August 1 2021, from: https://www.csis.org/analysis/will-chinas-161-format-divide-europe#:~:text=A1%3A%20The%2016%2B1%20format,%2C%20Croatia%2C%20the%20Czech%20Republic%2C

Hoffmann, A. (2017). *Interview - Walter Mignolo/Part 2: Key Concepts*. E-International Relations. Retrieved March 20 2021, from: https://www.e-ir.info/2017/01/21/interview-walter-mignolopart-2-key-concepts/

Huawei Technologies Co., Ltd. (2018). *Huawei Safe City Solution: Safeguards Serbia*. Retrieved August 1 2021, from: https://archive.li/pZ9HO

Huawei Technologies Co., Ltd. (n.d.a). *IPC6625-Z30 (-P/-S) 2-Megapixel 30x Intelligent IR High-Speed PTZ Dome Camera.* Retrieved August 2 2021, from: https://e.huawei.com/en/products/enterprise-networking/video-surveillance/hd-ip-cameras/ipc6625-z30

Huawei Technologies Co., Ltd. (n.d.b). *IPC6225-VRZ-ES 2.0-Megapixel IR Bullet IP Camera with a Motorized Zoom Lens.* Retrieved August 2 2021, from: https://e.huawei.com/en/products/enterprise-networking/video-surveillance/hd-ip-cameras/ipc6225-vrz-es?id={4E31BEDA-090F-4C51-A2F3-53B6507E81E5}&itemId={D6F3C6D1-0035-4CF1-8F43-A6D5AB92F8F9}

Huawei Technologies Co., Ltd. (n.d.c). *IPC6285 - VRZ.* Retrieved August 2 2021, from: https://support.huawei.com/enterprise/en/intelligent-vision/ipc6285-vrz-pid-22034864

Huawei Technologies Co., Ltd. (n.d.d). *VCN3020.* Retrieved August 2 2021, from: https://support.huawei.com/enterprise/en/video-surveillance/vcn3020-pid-21565784

Huawei Technologies Co., Ltd. (n.d.e). *OceanStor 5000 and 6000 V3 Series V300R006 Product Description.* Retrieved August 2 2021,

from: https://support.huawei.com/enterprise/en/doc/EDOC1000138866/80f42bc5/product-features

Huawei Technologies Co., Ltd. (n.d.f). *VCM5020*. Retrieved August 2 2021, from: https://support.huawei.com/enterprise/ae/video-surveillance/vcm5020-pid-21481882

Hydén, H. (2020). AI, Norms, Big Data, and the Law. *Asian Journal of Law and Society*, 7(3), 409-436.

Iliadis, A., & Russo, F. (2016). Critical data studies: An introduction. *Big Data & Society*, 3(2). Retrieved March 15 2021, from: https://doi.org/10.1177/2053951716674238

Innes, M. (2001). Control Creep. *Sociological Research Online*, 6(3), 13–18. DOI: https://doi.org/10.5153/sro.634

ITU News. (2021). *Digital commitment enables vaccine uptake in Serbia*. Retrieved August 1 2021, from:https://www.itu.int/en/myitu/News/2021/05/04/10/03/Digital-commitment-vaccine-uptake-Serbia-Prime-Minister-Ana-Brnabic

Kavalski, E. (2019). *China's "16+1" Is Dead? Long Live the "17+1."*. The Diplomat. Retrieved August 3 2021, from: https://thediplomat.com/2019/03/chinas-161-is-dead-long-live-the-171/

Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures and their consequences*. Sage.

Kitchin, R., & Lauriault, T. (2018). Toward Critical Data Studies: Charting and Unpacking Data Assemblages and Their Work. In Thatcher J., Eckert J., & Shears A. (Eds.), *Thinking Big Data in Geography: New Regimes, New Research* (pp. 3-20). London: University of Nebraska Press. DOI: 10.2307/j.ctt21h4z6m.6

Kojić, N. (2021). Interaktivna mapa i spisak lokacija saobraćajnih kamera koje prepoznaju tablice [Interactive map and list of locations of traffic cameras that recognize registration plates]. N1. Retrieved August 1 2021, from: https://rs.n1info.com/auto/lokacije-saobracajnih-kamera/

Kovačević, A. (2020). Digitalna prava na Balkanu: privatnost pacijenata na udaru [Digital rights in the Balkans: privacy of patients under attack]. Share Foundation. Retrieved August 1 2021, from: https://www.sharefoundation.info/sr/digitalna-prava-na-balkanu-privatnost-pacijenata-na-udaru/

Kovačević, A. (2021). *Baza povreda privatnosti: praćenje kršenja prava građana* [Base of privacy breaches: monitoring citizens 'violations]. Share Foundation.

Retrieved August 1 2021, from: https://www.sharefoundation.info/sr/baza-povreda-privatnosti-pracenje-krsenja-prava-gradana/

Krivokapić, D., Adamović, J., Tasić, D., Petrovski, A., Kalezić, P., Krivokapić, Đ. (2019). *Vodič kroz Zakon o zaštiti podataka o ličnosti i GDPR: tumačenje novog pravnog okvira* [Guide to the Law on Personal Data Protection and GDPR: interpretation of the new legal framework]. Belgrade: Share Foundation. Retrieved August 1 2021, from: https://www.sharefoundation.info/Documents/vodic_zzpl_gdpr_share_2019.pdf

Krivokapić, D., Bajić, M., & Perkov, B. (2021). *Shaping the Future of Multilateralism Biometrics in Belgrade: Serbia's path shows broader dangers of surveillance state*. Heinrich-Böll-Stiftung's European Union and Washington, DC offices. Retrieved August 3 2021, from: https://eu.boell.org/en/2021/05/19/shaping-future-multilateralism-biometrics-belgrade-serbias-path-shows-broader-dangers?dimension1=anna2021

Kvale, S., & Brinkmann, S. (2014). *Interviews: Learning the craft of qualitative research interviewing*. Sage. Third Edition.

Larsson, S. (2019). The Socio-Legal Relevance of Artificial Intelligence. *Droit et Société*, 103(3), 573-593.

Lee, C. S. (2019). Datafication, dataveillance, and the social credit system as China's new normal. *Online Information Review*, 43(6), 952–970. https://doi.org/10.1108/OIR-08-2018-0231

Lehtiniemi, T., & Ruckenstein, M. (2019). The social imaginaries of data activism. *Big Data & Society*, 6(1). DOI: https://doi.org/10.1177/2053951718821146.

Lemstra, M. (2020). *The destructive effects of state capture in the Western Balkans EU enlargement undermined*. Clingendael - the Netherlands Institute of International Relations. Retrieved August 3 2021, from: https://www.clingendael.org/sites/default/files/2020-10/Policy_Brief_Undermining_EU_enlargement_2020.pdf

Manokha, I. (2018a). Surveillance, panopticism, and self-discipline in the digital age. *Surveillance & Society*, 16(2), 219-237.

Manokha, I. (2018b). *Cambridge Analytica's closure is a pyrrhic victory for data privacy*. The Conversation. Retrieved March 8 2021, from: https://theconversation.com/cambridge-analyticas-closure-is-a-pyrrhic-victory-for-data-privacy-96034

Mason, J. (2002). *Qualitative researching*. London: SAGE Publications

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.

Mejias, U. A., & Couldry, N. (2019). Datafication. *Internet Policy Review*, 8(4). DOI: 10.14763/2019.4.1428

Mignolo, W. D. (2007). Introduction: Coloniality of power and de-colonial thinking. *Cultural studies*, 21(2-3), 155-167.

Miković, N. (2021). *Serbia's vaccine diplomacy: Balancing China and the West*. The Interpreter. Retrieved August 1 2021, from: https://www.lowyinstitute.org/the-interpreter/serbias-vaccine-diplomacy-balancing-china-and-west

Milan, S., & Treré, E. (2017). Big Data from the South: The beginning of a conversation we must have. *SSRN Electronic Journal*. Retrieved March 15 2021, from: https://www.researchgate.net/publication/320941650_Big_Data_from_the_South_The_Beginning_of_a_Conversation_We_Must_Have

Milan, S., & Treré, E. (2019). Big data from the South (s): Beyond data universalism. *Television & New Media*, 20(4), 319-335.

Mohamed, S., Png, M. T., & Isaac, W. (2020). Decolonial AI: Decolonial theory as socio-technical foresight in artificial intelligence. *Philosophy & Technology*, 33(4), 659-684.

N1. (2014). *Podnet optužni predlog protiv Marka Milićeva* [An indictment was filed against Marko Milić]. Retrieved August 1 2021, from: https://rs.n1info.com/vesti/a4207-podnet-optuzni-predlog-protiv-marka-miliceva/

N1. (2019). Stefanović: Hiljadu kamera sa softverima za prepoznavanje lica i tablica [Stefanovic: A thousand cameras with face recognition and license plate software]. Retrieved August 1 2021, from: https://rs.n1info.com/vesti/a456247-stefanovic-hiljadu-kamera-sa-softverima-za-prepoznavanje-lica-i-tablica/

National Assembly of the Republic of Serbia. (2017). *Program Vlade Republike Srbije kandidata za predsednika Vlade Ane Brnabić* [Program of the Government of the Republic of Serbia]. Belgrade: National Assembly of the Republic of Serbia. Retrieved from: https://media.srbija.gov.rs/medsrp/dokumenti/ekspoze-mandatarke-ane-brnabic280617_cyr.pdf

National Assembly of the Republic of Serbia. (2020). *Number of mandates won - XII National Assembly Convocation*. Retrieved August 1 2021, from: http://www.parlament.gov.rs/national-assembly/national-assembly-in-numbers.1743.html

Nikolin, G. (2019). *Već problemi u primeni novog zakona o zaštiti podataka o ličnosti, institucije lenje i spore* [There are already problems in the implementation of the new law on the protection of personal data, institutions, laziness and disputes]. 021. Retrieved August 1 2021, from: https://www.021.rs/story/Info/Srbija/224330/Vec-problemi-u-primeni-novog-zakona-o-zastiti-podataka-o-licnosti-institucije-lenje-i-spore.html

Nova Ekonomija. (2016). *Agencija za privatizaciju danas prestaje sa radom* [The Privatization Agency will stop working today]. Retrieved August 1 2021, from: https://novaekonomija.rs/vesti-iz-zemlje/agencija-za-privatizaciju-danas-prestaje-sa-radom

Numbeo. (2020). Europe: Crime Index by City 2020. Retrieved August 3 2021, from: Retrieved August 1 2021, from: https://www.numbeo.com/crime/region_rankings.jsp?title=2020&region=150&displayColumn=0

Official Gazette of the Republic of Serbia. (2006). *Constitution of The Republic of Serbia*. Retrieved August 1 2021, from: https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/74694/119555/F838981147/SRB74694%20Eng.pdf

Paragraf. (n.d.). *Law on Personal Data Protection*. Retrieved August 3 2021, from: https://www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html

Pasquale, F. (2015). *The black box society*. Harvard University Press.

Pejić Nikić, J., & Petrović, P. (2020). Capturing the Security Services in Serbia. In P. Petrović & J. Pejić Nikić (Eds.), *Security Sector Capture in Serbia: an Early Study*. Belgrade Centre for Security Policy

Perkov, B., Ćendić, K., Kovačević, A., Milošević, F. (2019). Digitalna prava u Srbiji 2014-2019 [Digital Rights in Serbia 2014-2019]. Belgrade: Share Foundation. Retrieved August 1 2021, from: https://resursi.sharefoundation.info/wp-content/uploads/2019/11/Greska_404.pdf

Petrović, P. (2020). *State Capture in Serbia – A Conceptual and Contextual Introduction*. In P. Petrović & J. Pejić Nikić (Eds.), Security Sector Capture in Serbia: an Early Study. Belgrade Centre for Security Policy

Prague Security Studies Institute (PSSI). (2020). *The Sum of All Fears – Chinese AI Surveillance in Serbia*. Retrieved August 4 2021, from: https://www.pssi.cz/publications/36-the-sum-of-all-fears-chinese-ai-surveillance-in-serbia

Price, D. H. (2014). The new surveillance normal: NSA and corporate surveillance in the age of global capitalism. *Monthly Review*, 66(3).

Quijano, A. (2007). Coloniality and modernity/rationality. *Cultural studies*, 21(2-3), 168-178.

Quijano, A.. (2000). Coloniality of Power, Eurocentrism, and Latin America. Nepantla: Views from South, 1(3), 533-580.

Ricaurte, P. (2019). Data epistemologies, the coloniality of power, and resistance. *Television & New Media*, 20(4), 350-365.

Ruppert, E., Isin, E., & Bigo, D. (2017). Data politics. *Big data & society*, 4(2). DOI: https://doi.org/10.1177/2053951717717749

SAGE Publications. (2019). Thematic Analysis of Interview Data in the Context of Management Controls Research. Retrieved August 2 2021, from: https://methods.sagepub.com/base/download/DatasetStudentGuide/thematic-analysis-management-controls

Saldana, J. (2013) The Coding Manual for Qualitative Researchers, 2nd Edition. London: Sage

Santos, B. d. S. (2016). *Epistemologies of the South: Justice against epistemicide*. Routledge.

Savić, M. (2021). *'Comrade Xi' Statue? Serbia Wants to Thank Its Friends in China.* Bloomberg. Retrieved August 1 2021, from: https://www.bloomberg.com/news/articles/2021-05-26/-comrade-xi-statue-serbia-wants-to-thank-its-friends-in-china

Schwab, K. (2016). *The Fourth Industrial Revolution: what it means, how to respond*. World Economic Forum. Retrieved March 2 2021, from: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Share Foundation. (2016). *Agencija za privatizaciju - jedinstven slučaj* [Privatization Agency - a unique case]. Retrieved August 1 2021, from: https://resursi.sharefoundation.info/sr/resource/agencija-za-privatizaciju-jedinstven-slucaj/

Share Foundation. (2018). Vodič kroz GDPR i zaštitu podataka o ličnosti - moji podaci , moja prava [Guide through GDPR and personal data protection - my data, my rights]. Share Foundation. Retrieved August 1 2021, from: https://resursi.sharefoundation.info/wp-content/uploads/2018/07/Podaci-u-doba-interneta-Final.pdf

Share Foundation. (2020). *Pandemija jedne lozinke. Kako je šifra za covid-19 završila na internetu?* [One password pandemic. How did the code for Covid-19 end on the

internet?]. Retrieved August 1 2021, from: https://www.sharefoundation.info/sr/pandemija-jedne-lozinke/

Slavinski, T., & Todorović, M. (2019). The impact of digitalisation on the organisational capability changes–Evidence from Serbia. In *Proceedings of the 5th IPMA SENET Project Management Conference* (pp. 244-50).

Smith, G. J. (2020). The politics of algorithmic governance in the black box city. *Big Data & Society*, 7(2). DOI: https://doi.org/10.1177/2053951720933989

Stojanović, B. & Bértoa, F.C. (2020). Serbia's ruling party just scored a landslide victory. Here's why the opposition boycotted the election. *The Washington Post*. Retrieved August 1 2021, from: https://www.washingtonpost.com/politics/2020/06/30/serbias-ruling-party-just-scored-landslide-victory-heres-why-opposition-boycotted-election/

Stojanović, D. (2019). *China's spreading influence in Eastern Europe worries West*. Asscociated Press. Retrieved August 1 2021, from: https://apnews.com/article/eastern-europe-ap-top-news-international-news-croatia-china-d121bfc580f04e73b886cc8c5a155f7e

Stojkovski, B. (2019). *Big Brother Comes to Belgrade*. Foreign Policy. Retrieved August 1 2021, from: https://foreignpolicy.com/2019/06/18/big-brother-comes-to-belgrade-huawei-china-facial-recognition-vucic/

Thales. (2021). *Facial recognition: top 7 trends (tech, vendors, markets, use cases & latest news)*. Retrieved August 3 2021, from: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition

Thatcher, J., O'Sullivan, D., & Mahmoudi, D. (2016). Data colonialism through accumulation by dispossession: New metaphors for daily data. *Environment and Planning D: Society and Space*, 34(6), 990-1006. DOI: https://doi.org/10.1177/0263775816633195

The Economist. (2017). The world's most valuable resource is no longer oil, but data. Retrieved April 5 2021, from: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

The Ministry of Internal Affairs of the Republic of Serbia. (2019a). *02/4 br072/1-106/19-4*. Retrieved August 1 2021, from: https://resursi.sharefoundation.info/wp-content/uploads/2019/03/Resenje-MUP-7.3.2019..pdf

The Ministry of Internal Affairs of the Republic of Serbia. (2019b). Procena uticaja obrade na zaštitu podataka o ličnosti korišćenjem sistema video nadzora [Assessment of the impact of processing on the protection of personal data using a

video surveillance system]. Retrieved August 1 2021, from: https://www.sharefoundation.info/wp-content/uploads/MUP-Procena-uticaja-obrade-na-zastitu-podataka-o-licnosti-koriscenjem-sistema-video-nadzora.pdf

The Ministry of Internal Affairs of the Republic of Serbia. (2020). *Procena uticaja obrade na zaštitu podataka o ličnosti upotrebom savremenih tehnologija video nadzora u okviru projekta "Sigurno društvo" u Beogradu* [Assessment of the impact of processing on the protection of personal data using modern video surveillance technologies within the project "Safe Society" in Belgrade]. Retrieved August 1 2021, from: https://www.sharefoundation.info/wp-content/uploads/Procena_uticaja_2_0.pdf

The Ministry of Internal Affairs of the Republic of Serbia. (n.d.). *Lokacije kamernih mesta* [Camera locations]. Retrieved August 1 2021, from: http://www.mup.gov.rs/wps/wcm/connect/1e2337b2-f258-4f46-95f5-73d25f991415/lat-Lokacije+kamernih+mesta.pdf?MOD=AJPERES&CVID=nBH2RCw

The World Wide Web Foundation. (2017). *Artificial Intelligence: The Road Ahead in Low and Middle-Income Countries*. Retrieved from: www.webfoundation.org

United States Agency for International Development (USAID). (2012). *The 2012 CSO Sustainability Index for Central and Eastern Europe and Eurasia 16th Edition*. Retrieved August 1 2021, from: https://www.usaid.gov/sites/default/files/documents/1863/SRB.pdf

Van der Spuy, A. (2020). Colonising ourselves? An introduction to data colonialism. LSE blog. Retrieved August 3 2021, from: https://blogs.lse.ac.uk/medialse/2020/03/19/colonising-ourselves-an-introduction-to-data-colonialism/

van Dijck, J. (2014) Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, 12(2), 197-208.

van Dijck, J., Poell, T., & De Waal, M. (2018). *The platform society: Public values in a connective world*. Oxford University Press.

Vladisavljev, S. (2019). *How Did Serbia And Huawei Cooperate: A Chronology*. BFPE. Retrieved August 1 2021, from: https://en.bfpe.org/in-focus/region-in-focus-focus/how-did-serbia-and-huawei-cooperate-a-chronology/

Vuksanović, V. (2019). *Securing the Sino-Serbian Partnership*. *CHOICE*. Retrieved August 1 2021, from: https://chinaobservers.eu/securing-the-sino-serbian-partnership/

Wolford, B. (n.d.). *Everything you need to know about the "Right to be forgotten"*. GDPR.EU. Retrieved August 3 2021, from: https://gdpr.eu/right-to-be-forgotten/

Yin, R. K. (2018). *Case study research and applications: Design and methods*. Sage publications.

Živić, M. (2019). *Gošće N1: Zloupotreba ličnih podataka česta, više iz neznanja nego iz namere* [Guests of N1: Misuse of personal data is common, more out of ignorance than out of intent]. N1. Retrieved August 1 2021, from: https://rs.n1info.com/vesti/a509909-gosce-n1-zloupotreba-licnih-podataka-cesta-vise-iz-neznanja-nego-iz-namere/

Živić, M. (2020). *Koliko građani i institucije znaju o zaštiti podataka o ličnosti i zloupotrebama* [How much do citizens and institutions know about personal data protection and abuse?]. N1. Retrieved August 1 2021, from: https://rs.n1info.com/vesti/a564720-koliko-gradjani-i-institucije-znaju-o-zastiti-podataka-o-licnosti-i-zloupotrebama/

Živić, P. (2018). Država ne poštuje digitalna prava građana, pokazalo istraživanje Šer fondacije [The state does not respect the digital rights of citizens, a study by the Shere Foundation showed]. *BBC*. Retrieved August 1 2021, from: https://www.bbc.com/serbian/lat/srbija-45004839

Zuboff, S. (2019a). Surveillance capitalism and the challenge of collective action. *New labor forum*, 28(1), 10-29.

Zuboff, S. (2019b). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: PublicAffairs.

10. Appendix

10.1. Appendix A. Details about Conducted Interviews

Tabel 1. Information about Conducted Interviews

Codename	Date	Location/medium	Length of interview	Profession
Interviewee 1	16.04.2021	Telegram	≈ 55 min	/
Interviewee 2	16.04.2021	Google Meet	≈ 37 min	IT engineer
Interviewee 3	20.04.2021	Zoom	≈ 30 min	Lawyer
Interviewee 4	21.04.2021	Zoom	≈ 35 min	Lawyer
Interviewee 5	26.04.2021	Zoom	≈ 36 min	Lawyer
Interviewee 6	27.04.2021	Zoom	≈ 43 min	/

10.2. Appendix B. Guide for Semi-Structured Interviews

Introduction

- What is your relation to the “Hiljade kamera” initiative? When and why you became part of it?
- Why do you think that MIARS launched the project of the “Safe city”?

Questions about the data collection

- What is the role of big data in the whole project?
- What do you think the data gather from the “Safe city” project will be used?

- What kind of knowledge through data can be derived by using the “Safe City” technology?
- What could be the consequences of data collection when the project is fully realized and in full capacity?
- In the conception of the project, can people control how the data is extracted from their faces?
- What is the position of those who have control over the data and those to whom data refer?
- Are there any potential losers and winners from collecting the data in the “Safe city”?
- Is collection and processing of the biometric data legal according to the Law on Data Protection?
- What do you think about the assessment of the risks on the rights and freedoms of the people in DPIA?
- Is there any new knowledge about us that is produced through the “Safe City” project? If yes, in what form?

Questions about the Initiative “Hiljade kamera”

- What is the goal of your Initiative?
- So far, how have you contested the Safe city project and possible generation of data in Belgrade?