Article

Underneath the Promise of Safety and Security in a 'Smart City'

An Ethnographic Study of Eindhoven's *Living Lab Stratumseind*

Sofie Doorman

University of Amsterdam

Brunilda Pali

KU Leuven

Abstract

In this article, we explore the promises of security that are embedded in the smart city technologies and algorithms and their potential implications for creating social inequality and discrimination. Our ethnographic case study is the Living Lab Stratumseind, a popular nightlife street in Eindhoven where smart technologies and algorithms are being tested with the aim of increasing security in the street. First, we introduce the context in which the Living Lab Stratumseind was developed and trace this development and the multiple forms of governance that characterise it and highlight the main 'smart technologies' that can be found there. Second, we focus our attention on the ways in which smart technologies and algorithms promise to enhance public security by directly and uncritically translating technological rationales and discourses into social domains. Third, we argue that the smart city technologies and algorithms risk to create, reproduce and reinforce social inequalities and discrimination, and that it is unclear who is responsible for these unanticipated consequences.

Keywords

smart city, algorithmic governance, living labs, security, social sorting

Unpacking Promises and Assumptions of Smart Cities

Through sophisticated 'corporate storytelling' (Söderström, Paasche and Klauser 2014, 307) the smart city has become a worldwide panacea, a techno-utopian vision, and social and urban imaginary (Mitchell 2002, Townsend 2013, Datta 2015, Wiig 2015, Jasanoff and Kim 2015, Vanolo 2016, Lindner and Meissner 2018, Sadowski and Bendor 2019, Pali and Schuilenburg 2019) that promises to address many complex social problems, including problems of urban unsafety and

insecurity. A smart city is said to be a safe city. Safety and security issues are increasingly handled by multidisciplinary teams of actors and in collaborations between citizens, companies, governments, housing corporations, shopkeepers, insurers, and energy suppliers (Schuilenburg 2015, 11-12). As Marc Schuilenburg writes, ‘[s]ecurity is an elastic concept. The geometry of the concept is so variable that everything can be dropped into its flexible confines’ (Schuilenburg 2015, 17). The new technocratic players joining the ‘smart city, safe city’ game, who are not trained in social sciences, bring along new understandings and interpretations of safety and security. A central objective of this article is to investigate some of these interpretations and to unpack their potential consequences.

Generally, from a smart city perspective, all that is required to understand, manage, and fix all sorts of problems that a city faces and can possibly come to face, are smart technologies, algorithms, and the abstraction of social urban life into large data (Van Dijck 2014). Data are collected, processed, cleansed and re- and interconnected in order to discern relations and patterns, while managing anomalies or abnormalities identified by these patterns and data analysis (Pasquinelli 2015, Galič 2019). This abstraction is then used to tackle complex social problems such as unsafety and insecurity, creating the risk of social inequalities and the reproduction and strengthening of the exclusion of certain groups by smart technologies and algorithms (Lyon 2003, Cheney-Lippold 2011, Benjamin 2019). We focus our attention on the risk of the possible creation of social inequalities and exclusion as a result of the merging of these projects with an agenda of ‘safety and security’.

In our view, it is the assumption of objectivity and neutrality that comes with the use of data, algorithms and technologies that significantly exacerbates this risk (Gillespie 2014, Kitchin 2014, Hong 2020). Although the smart city proponents present the concept as non-ideological and therefore neutral, objective, rational, and evidence-based, as Sadowski and Pasquale (2015) have argued, nothing is more ideological than the deployment of the term ‘non-ideology’ (see also Kitchin and Dodge 2011). Presenting the concept of the smart city as apolitical or post-political, disregards the fundamental political character of urban governance (Lahiji 2014, Wilson and Swyngedouw 2014, Scott 2016). In smart cities, algorithm and technology designers translate their values into the systems, generating a variety of intended and unintended consequences with significant ethical implications (Pasquale 2015, Mittelstadt *et al.* 2016, Yeung 2018). Technocrats are therefore in a very powerful position. By translating their technoutopias and discourses into the area of security, they create safety and security imaginaries which affect people’s lives and the choice architectures within which they find themselves. Therefore, it has been firmly argued that the smart city demands continuous scrutiny and critique (Vanolo 2014, Kitchin 2015, Sadowski and Pasquale 2015, Sadowski and Bendor 2019, Pali and Schuilenburg 2019).

Nevertheless, Rob Kitchin has critiqued critical scholarship on smart cities for ‘the use of canonical examples and one-size fits all narratives’ and ‘an absence of in-

depth empirical case studies of specific “smart city” initiatives and comparative research that contrasts “smart city” developments in different locales’ (Kitchin 2014, 132). Many scholars speak about *the* smart city, emphasizing typical characteristics. Their critique is based on the reading of corporate and policy documents, online information, and previous research on the topic. What is unseen or neglected here, is the messy character of these cities, the diverse histories, contexts and realities, the different starting points, visions, ambitions, and priorities of the cities and involved stakeholders (Kitchin 2014, 133) as well as the everyday tensions, struggles and inconsistencies of smart cities.

Taking this critique seriously, in this article we provide an analysis of an ethnographic study of one particular smart city initiative. We examine and unpack the safety and security imaginaries (Schuilenburg and Pali 2021) embedded in the smart city technologies and algorithms and their potential implications for creating social inequality and discrimination, by focusing on the case of *Living Lab Stratumseind*. Stratumseind is a popular street in the Dutch city of Eindhoven, a city in the south of The Netherlands. The Netherlands is one of the leading European countries in the development of smart cities, with Eindhoven, Enschede and Utrecht as important examples (Naafs 2018). Whole cities, or parts of them, such as streets, neighbourhoods, districts, or university campuses, have become literally laboratories in real-life conditions – so called ‘living labs’. Deeply embedded in techno-utopian ‘permissionless innovation’ (Thierer 2016) and ‘technocratic solutionism’ (Morozov 2014, Williamson 2016), these living labs enjoy freedom to experiment, test and innovate, largely unstified by public regulations and democratic governance.

In the following, we start by briefly describing the methodology and the data used for this article. Second, we describe our case study, more specifically the context in which the *Living Lab Stratumseind* was developed, its progressive development and governance, and the smart technologies that we have found there. After setting the context and introducing the case study, we focus our attention on the ways in which smart technologies and algorithms promise to enhance public safety and security by directly and uncritically translating technological rationales and discourse into social domains. Finally, we show how the smart city technologies and algorithms risk to create, reproduce and strengthen social inequalities and discrimination, arguing that it remains unclear who is responsible for these possible unanticipated consequences.

Methodology

Our study of the *Living Lab Stratumseind* relied largely on participant observation, sensory observation, interviews, and online research. Sofie Doorman (first author), herein referred to as the field researcher, moved to the research site for three months in Spring 2020, just before the Covid-19 outbreak in the Netherlands, to conduct the research and ‘get a feel’ of the place and its people. During this period, she has taken many walks, sat down on terraces, gone out for a drink or

dancing in the clubs, witnessing first-hand how police officers intervened in small fights or observing the Philips Lighting system at work. She has had many informal conversations with visitors of Stratumseind, like students, tourists, and construction workers, focusing on the way smart technologies influenced their experiences of the street.

Besides the more traditional type of participatory observation, very important in this case was the engagement of the field researcher in the sensory observation, through which she focused on sound, light, smell, or touch in the street during different times of the day and week, paying attention to the difference of the street atmosphere and sensory experiences between day and night, but also to the way the sensory experience interacted with the knowledge. Senses show how experiences of a place can differ between people and over time, and therefore influence once knowledge of a place (Ingold 2011).

In addition, the field researcher conducted 10 semi-structured interviews with a variety of key stakeholders of the *Living Lab Stratumseind*. These were representatives from Eindhoven municipality, police, the Dutch Institute for Technology, Safety and Security (DITSS), Sorama and Oddity (local technology companies) and local entrepreneurs in Stratumseind. The interviews were focused on the main interests and practices of different stakeholders and on understanding the interplay between the different parties involved with *Living Lab Stratumseind*. Here we also follow Marc Schuilenburg in his perspective on evaluating security interventions, who argues that ‘[o]ne way of doing this, is to look at the interactions among the actors on the ground. How do they relate to one another and how do they regard one another? Which kind of language do they use, and what do they hope to achieve? How do they interpret the agreements made, and how much importance do they attach to their observance?’ (Schuilenburg 2015, 21).

Lastly, for our analysis we have conducted substantial online research and gathered information from official documents, mission statements, and news-coverage on the *Living Lab Stratumseind*. The analysis that follows uses the material from across these different methods, building up the arguments made in the article.

Context and Development of the *Living Lab Stratumseind*

Eindhoven’s Technological Pride

In order to understand the particular features of the *Living Lab Stratumseind*, it was important to place it in a larger context of technological development and innovation. Eindhoven is the fifth largest municipality in the Netherlands with about 234,400 inhabitants.¹ Technology constitutes an important part of

¹ See <https://www.eindhoven.nl/bevolking> [accessed 09-01-21]

Eindhoven's identity, a city which takes extreme pride in being a global social and technological innovation site. Eindhoven 365, the marketing organisation of the city, writes on their website:

We believe in Eindhoven. That means, we think that this exciting city plays an important role in the current and future international stage of creative innovation. Eindhoven is the city of technology, design and knowledge, and especially a combination of those.²

In 2011, Eindhoven was elected as the 'smartest region of the world' by the Intelligent Community Forum. Smart city competitions and other ranking lists encourage Eindhoven to invest large resources in their image and in those aspects of their city that will make them win these competitions and attract more investors. Morozov and Bria (2018) have critiqued the neoliberal consumption-driven discourse of smart cities, arguing that the main rationale of the development of smart technologies is to create competitive analysis tables to invite smart investments.

Given the overwhelming investments in technology, important players in the growth of the city are major international businesses in the field of information and communication technology, including Atos, IBM, Intel, Cisco, Philips, and the Technological University of Eindhoven (TU/e). Philips has been one of the pioneers and the most influential among these players. Through institutions like Brainport Eindhoven and DITSS, the municipality aims at bringing different actors and stakeholders together and creating shared aims and visions, trying to overcome the problem that local governments lack the capital and knowledge that is owned by companies. Brainport Eindhoven is a region framed as the cradle, the beating heart, and the future of high-tech³ which aims to connect Eindhoven to Europe in the technological field. On their website,⁴ they write:

Together we make complex machines and innovative products that make the world a better place. It is for good reason that we are called the smartest region in the world. While we look at how things can be done even better, the world looks at the way we do it.

DITSS is a non-profit organisation, funded by the government, that uses technological innovation to solve safety and security issues through technology in

² Own translation, see <https://www.eindhoven365.nl/nl#Over%20Eindhoven365> [accessed 09-01-21]

³ See <https://www.brainportindustriescampus.com/en/ideal-for-business/the-brainport-region> [accessed 12-02-20]; <https://www.brainportindustriescampus.com/en> [accessed 09-01-21]; <https://www.brainportindustriescampus.com/en/open-innovation-under-a-single-roof/> [accessed 09-01-20]

⁴ See <https://brainporteindhoven.com/nl/> [accessed 07-11-19]

Brabant (a province in the south of The Netherlands, of which Eindhoven is the largest city). They work according to the 'triple helix principle', which means that they stimulate cooperation between knowledge institutes, governments and companies. The municipality of Eindhoven seconds people from DITSS to manage and organise the living labs and to work together with the different partners. For example, Tinus Kanters, employee of DITSS, is the project leader of *Living Lab Stratumseind* from the beginning of the Lab's existence. Several of the images used in this article have been shared with us by Tinus. Therefore, we cannot overstate the importance of technology and technological pride for Eindhoven. This unquestioned and extreme pride makes critique all the more difficult. During an interview that we conducted with Ton van Gool, director of STRP, an art and technology festival in Eindhoven, he said:

It is quite difficult in Eindhoven to question technological innovation. Because that's what we're good at. If you are going to question that, it is seen as if you are an apostate.

Typical of smart cities' promises and visions, as we argued in the introduction, the improvement of the quality of life through technological innovation is deemed to be a core mission of the city, and Eindhoven's living labs, such as Stratumseind, Strijp-S and Eckart Vaartbroek, are crucial spaces and projects that articulate and try to implement that vision.

Image 1. Stratumseind during King's Day, year unknown. Image taken from the PowerPoint presentation by Tinus Kanters from December 2019, shown to Sofie Doorman on 14-01-20.

Image 2. Stratumseind during the day. Photo taken by Sofie Doorman on 29-11-2019.

Living Lab Stratumseind

Stratumseind, also known simply as Stratum, is a popular nightlife street in the centre of Eindhoven. Over a distance of just 225 meters more than 50 bars, cafés, clubs and restaurants are located. Because of the high density of entertainment industry in a relatively small space, on Thursday, Friday and Saturday nights the street is packed with people (attracting about 20,000 people a weekend).

It was especially interesting to experience the street during both day and night. During the day, the street is quiet, bars are closed, people pass through, and the street has a grey colour. As a result, not much happens in the street during the day. The empty bars lose their identity and their function, and the street simply becomes an environment through which people pass (*see* Image 2).

During the night, the atmosphere in the street changes completely. It is full of people and different colours of light and music come from different bars. During these nights, conflicts happen regularly, and there are hundreds of incidents recorded every year. We were interested in understanding what these incidents were about and therefore the field researcher organised an interview with Richard van den Vijver, project manager of the police team that works in and around Stratumseind during the weekend, and who is football coordinator at local top division football club PSV. Richard said that he liked to work in Stratumseind because of the difference between the nights and the amount of people that go there. He called it 'a unique little street' (*een uniek straatje*) and a 'child disco'. 'The main trouble here,' he explained with a serious voice, 'is caused by the old classical story: alcohol and women. Men touching the wrong woman, men showing

“machismo” (*haantjesgedrag*, lit. rooster/cock behaviour)’. He also added that to understand what happens in the street, it is important to be aware of what happens outside of Stratumseind: young people arguing at schools who meet again at Stratumseind, sport associations, dynamics between villages from outside Eindhoven, dynamics between Eindhoven and Belgium, bachelor parties and football matches. Concerts, parties or other events happening in Eindhoven, university schedules and exam periods influence the dynamics at Stratumseind. To keep updated with the complexity of the situation, at the beginning of each night, Richard and his team take a stroll along the street and visit the security guards of the cafés who know what is going on. Without trivializing the serious character of violence in Stratumseind, Richard also put it into perspective:

It is Stratumseind, a narrow street, a lot of youth, alcohol. Then [the number of incidents] is quite normal. These are not all shocking things. Someone is urinating, someone else is using a false ID to enter a club. And then you see the number of arrests and that sounds like a lot.

Image 3. Stratumseind on a Thursday night. Photo taken by Sofie Doorman on 12-03-2020.

Partly due to these incidents, in 2012 the municipality of Eindhoven started the project *Stratumseind 2.0* in collaboration with the police and with Horecavereniging Stratumseind, an association of the local entrepreneurs of the street. The project aimed to improve the quality of life (or livability/*leefbaarheid*), safety and attractiveness of Stratumseind with direct market-based goals, such as attracting more visitors who spend more money and increasing the real estate value and

income (see Stratumseind 2.0 Action Plan 2013-2017). A year after its start, as part of *Stratumseind 2.0*, in 2013 the *Living Lab Stratumseind* was created. Twenty research institutions, local entrepreneurs, the police, tech companies, the municipality of Eindhoven and many other parties were and continue to be involved in the project, although their degree of involvement differs.

Living Lab Stratumseind, as the name suggests, offers tech companies the opportunity to test their products – some of which we will introduce later on in the article – in real-life situations, making it possible for tech companies to label their products as ‘proven’ in real-life and adapted to potential users (Kviselius and Andersson 2009, Schuurman, Mahr, De Marez and Ballon 2013). This increases the reliability and value of their products, lowers the threshold for social acceptance and shortens the time-to-market (Pierson and Lievens 2005, 114). This is considered to be a service that the municipality of Eindhoven offers to tech companies, in exchange for which tech companies should develop or put their products to the service of the municipality, making the street safer, more liveable and more attractive. An immense amount of energy is put into promoting Stratumseind both to tech companies and potential users as an innovative and lively area. The front page of the promotional website⁵ shows in big and coloured letters:

New Vibes New Tribes Stratumseind. Welcome to the new Stratumseind, an entertainment area, rich with contrasts, in the heart of Eindhoven. We report about this place which is full of new initiatives.⁶

The term ‘new’ reflects the municipality’s attempt to communicate the idea of a positive transformation of the street, whereas the term ‘rich with contrasts’ communicates an idea of diversity and difference. This way, *Living Lab Stratumseind* functions as advertisement for the city, to attract potential users, inhabitants, and investors and as a place where tech companies can create a market for themselves.

Smart Technologies in the Living Lab Stratumseind

Which smart technologies are present in the *Living Lab Stratumseind*? Morozov and Bria defined ‘smart technology’ as ‘any advanced technology deployed in cities with the intent of optimizing the use of resources, producing new resources, changing user behaviour, or promising other kinds of gains in terms of, for example, flexibility, security, and sustainability’ (Morozov and Bria 2018, 4). The invisibility and opacity of the operations of these technologies and algorithms has been mentioned as a critical point of attention (Pasquale 2015, Burrell 2016). Smart technologies that aim to create safety and security are totally ‘subsumed into the background of everyday life’ (Sadowski and Pasquale 2015, 9).

⁵ See <https://stratumseind-eindhoven.nl/> [accessed 09-01-21]

⁶ Original “Welkom op het nieuwe Stratumseind, een contrastrijk uitgaansgebied gelegen in hartje Eindhoven. We doen verslag van deze plek vol nieuwe initiatieven.”

As part of the project *Living Lab Stratumseind*, smart cameras and sound sensors gather data to follow and monitor the people in the street. The cameras and sound sensors register how people move, the density of people in the street, sounds, light, temperature, the number of bikers, the frequency of trucks delivering products to cafés and restaurants and more. Information from breweries (e.g., how much beer is sold), cafés, bars, restaurants and clubs in the street is also collected by the municipality. In the past, data has also been collected through social media use (every time Stratumseind or one of the cafés in Stratumseind is mentioned on Facebook, Twitter or Instagram). The combination of this real-time data makes it possible to find patterns in behaviour of people and dynamics in the street. The cameras and sound sensors are connected to each other and have for example learned to recognise potential conflict or aggressive behaviour based on sudden changes in movement and sound, and to distinguish this from a partying group of people. Eventually, technologies communicate this automatically to the police who intervenes when needed.⁷

Image 4. Software developed for CityPulse, a predictive policing project in Stratumseind. The system worked with software that looked for anomalies in data patterns on which it based predictions for the probability of incidents. This pilot was developed by the municipality of Eindhoven, Atos,⁸ Intel, Sorama,⁹ and other partners. The image comes from a presentation by Tinus Kanter in December 2019, coordinator of *Living Lab Stratumseind*.

⁷ See <https://www.securitymanagement.nl/stratumseind-eindhoven-living-lab/> [accessed 09-01-21]

⁸ See Atos. CityPulse - using big data for real time incident response management <https://atos.net/wp-content/uploads/2016/06/atos-ph-eindhoven-city-pulse-case-study.pdf> [accessed 13-01-21]

⁹ See Atos, Sorama and the city of Eindhoven win Digital Impact Award with 'CityPulse' <https://www.sorama.eu/news/2018/5/6/atos-sorama-and-the-city-of-eindhoven-win-digital-impact-award-with-citypulse> [accessed 13-01-21]

Different kinds of technologies are being tested in Stratumseind. Smart lights developed by Philips are hung up on special poles in the street, these lights can change colour and intensity, based on the moment of the day and the number of visitors. The idea behind this technique is to change the atmosphere in the street in order to decrease aggression and violence. The colour blue, for example, has a cooling effect. When the right shade of blue is used, it can lower heart rates and reduce people's aggression. Smart 3D sound sensors designed by Sorama, an Eindhoven-based tech company, are hung up on similar poles.

Image 5. A pole in Stratumseind with smart technologies: a sound sensor (the white box on top), a camera with software from Oddity.ai, presumably a counting camera and other technologies. Photo taken by Sofie Doorman, 29-11-19.

These sensors register sounds in and around the street and are placed strategically at specific places (see Image 6). Another example is smart camera software, developed by Oddity.ai, an Utrecht-based tech company, which is installed in already existing cameras, sometimes attached to the same pole. Counting cameras are also installed on all entry points of the street (see Image 6).

The sensuous experience in the street interacts constantly with knowledge. The field researcher noticed that the more she knew about the cameras, the more she saw them and the more she felt physically different. Therefore, making the connection between knowledge, spatial experience and unconscious behaviour was important when studying the consequences of the technological innovations in Stratumseind on the daily lives of its users. In contrast with the awareness of the

Image 6. Locations of video counting cameras (red dots) and sound sensors (blue dots) on Stratumseind. Copyright: Eindhoven municipality.

field researcher and the obvious enthusiasm of the technocrats interviewed, users in Stratum were often unaware of the smart technologies, and even when made aware by the researcher they remained largely uninterested in them. The following passage from the diary of the field researcher reflects on this:

On a grey morning in February, when I had just moved to Eindhoven, I went to café De Spijker, a student bar at the beginning of Stratumseind just in front of the church. To get there, I had to walk through Stratumseind. It was quiet, some people walked or biked through the street. In the morning, almost all cafés are closed, so not much was happening in the street. Some trash lay around from the night before. Construction workers were working in one of the bars. During the day, the empty bars lose their identity, their function. It becomes an environment through which people pass. When I arrived at De Spijker, one of the few bars ('bar' is actually not the right term here, De Spijker is a restaurant during the day, a bar in the evening and a night club during the night) open at that time, I sat down at the terrace and ordered a coffee. In front of me, preparations for Carnival were taking place. A large tent was being built up in between the church and café De Spijker. When the waitress, a student, brought me my coffee, I asked her what kind of street Stratumseind is. Enthusiastically, she started telling me about all the students that come here to go out. She explained that the different cafés play different kinds of music. Here in De Spijker it is

mostly pop, sing along and Dutch music; actually, all music which is popular among students. Two cafés play R&B, another café plays house. This tells you a lot about the kinds of people that come to those cafés, she told me. When I asked her to tell me something about *Living Lab Stratumseind*, she looked confused. I explained to her something about the experiments that are being done with light and other technologies to increase safety in the street, but she had never heard of them. She was not really impressed by my story and not really interested in it either. She liked going out here, and that was the most important thing to her. This is a reaction I got almost every time when I spoke about Stratumseind with students, which is the largest group that goes out there. While the living lab has existed since 2014 and is promoted in local newspapers and through online campaigns, the students don't know much about its development. Some students I spoke to, knew some general things, for example that Philips did experiments with lights, but they did not know other details, nor were they interested in them. When I explained more about the living lab, most of them were neither impressed nor did they care. The students were not the only ones to be unaware. When going out in Stratumseind one night, I met two police officers in the street. I asked them whether they made use of the technologies in Stratumseind. They told me they did not. In fact, they did not know much about the technologies in the street and were not eager to talk about it. One of them remarked that they were never informed about these developments, and that they were not interested in them either. They could do their job without them.

A similar – rather ironic – reaction came from Richard, the abovementioned police chief. When the field researcher asked Richard about the technologies that are being tested in Stratumseind, he looked sceptical, explaining that he is not against them, but that he did not yet experience any advantage since the beginning of the living lab. He stated, 'the living lab is presented beautifully to the outside world, but I don't notice anything of it in practice.' A few years ago, he explained, the electronics company Philips joined the police on the street to understand their experiences and needs. Then, Philips developed a dashboard which the police could use to change lighting in the street. Richard said he only uses this dashboard to brighten the lights five minutes before Stratumseind closes in order to let people go home. According to him the whole dashboard was not necessary, but he found that specific function useful. One year later, the license of the dashboard had to be extended, but there was no money for it, so the project stopped. When asked who should have paid this money, Richard answered:

You tell me. Everyone pointed at each other. The municipality said 'the police asked this so they have to pay for it,' Philips said 'we developed this for you so we don't have to pay.' The ball was passed around. I don't know where the ball is now, but we don't have this system anymore.

This ping-ponging about the money that Richard articulates brings attention to similar concerns that have been voiced about the domination of private tech companies over governments (Sadowski and Pasquale 2015). According to Sadowski and Pasquale, tech companies promote 'smartness' as an ideal so that they can make money out of it, pulling city leaders and investors into the world of smartness. They *create* needs in order to create and shape a market where they can sell their smart products. This way, solutions to social and political problems are being commodified (Morozov 2014). Thomas Alflen, director of Oddity.ai, which is one of the local tech companies involved with the living lab, remarked on the financial question:

We have to make the end users enthusiastic, so that's our starting point. Those are the security observers and the police. And then they have to figure out where they get that money. That can come from the police, or the municipality.

We encountered little enthusiasm for the technologies from the so-called end users, at least nothing matching the enthusiasm of the technocrats. Moreover, as we observed to begin with, none of the enthusiastic technocrats lives or works in the street of the living lab itself. Richard had many questions about the technologies: 'What are they doing? In what stage are they? What are the results? Are they going to change something?' Showing a mixture of amusement, confusion and frustration, he said 'it's been the same thing for many years. I see little change.' He ended the conversation laughingly:

There is, actually, just one thing I would really like Philips to design: a sprinkling installation with water from the Dommel [the river next to Stratumseind]. Because when it rains, people always go home.

Meanwhile we heard from several informal sources that the municipality has been planning to start experimenting with citrus smell in the street to make people calmer and discourage aggressive behaviour, but no further formal information could be gathered about this. In what follows, we discuss some of the technologies focusing on the topic of security, the assumption of objectivity, social sorting, and the risk of reproducing social inequality.

Promising Security: Translating the Techno to the Social

As mentioned previously, when a city considers investment in and seeks to legitimize the use of smart technologies, public safety and security are often articulated as key drivers and rationales (Lacinák and Ristvej 2017, Schuilenburg and Peeters 2018). The development and popularisation of smart technologies and algorithms has led to significant changes in practices of security, governance and surveillance of cities. Before the development of smart technologies in urban spaces, embedded in ideas and theories of defensible space and situational crime prevention, security and safety were provided largely through the design of physical space (Pali and Schuilenburg 2019). Whereas these physical designs, such as fences, walls and barbed wire, have not been totally removed, they have been perhaps transferred elsewhere (e.g., refugee camps) and replaced – especially in the city centres – by invisible and smart technologies.

Among the new smart technologies which promise to create safe and secure cities, Pali and Schuilenburg (2019) have made a rough distinction between predictive and psychopolitical technologies. Predictive technologies, such as predictive policing, facial recognition, automated license plate recognition system, biometrical control, and advanced video monitoring, have been implemented in several smart cities raising criticism for their risks for privacy, discrimination, and marginalisation of certain groups. Psychopolitical technologies are broadly techniques used to actively modify the conduct (e.g., reduce tensions or aggression) of visitors of public or semi-public spaces in smart cities, often by modifying the atmosphere in these spaces based on real-time data analysis and smart technologies. It has been argued that the atmosphere, which is created and modified through design, layout, lighting, sound, and other affective means, directs and regulates movement, influences behaviour and perceptions, and induces physiological and psychological dispositions that are essentially conducive to consumption (Allen 2006, 445). As a result, ‘proper’ behaviour is encouraged, while unwanted behaviour – aggression, excessive noise, public drunkenness, vandalism, and violence – is discouraged by the use of these techniques (Schuilenburg and Peeters 2018). Smart technologies and algorithms do therefore not exert power in the classical sense, but provide a script for action, by nudging, manipulating, or managing behaviour both at the collective and individual level (Peeters and Schuilenburg 2018).

In Stratumseind too, increasing safety and security in the street is articulated as one of the main goals of the implementation of smart technologies. The Stratumseind 2.0 Action Plan 2013-2017 states that the mission of the project *Stratumseind 2.0* is to improve ‘livability, safety and attractiveness’. As previously mentioned, DITSS, the institute that manages the *Living Lab Stratumseind* is specialised in safety and security. The tech companies that develop smart sensors, promote their technologies as innovations that will bring us ‘the future of safety’.¹⁰ Nevertheless, these are not traditional security actors, but technocrats, so

¹⁰ Front page of Oddity’s website <https://oddity.ai/#> [accessed 09-01-21]

understanding what brings them to the safety and security area and what sense they make of this is from our perspective highly interesting. In the next section, we largely base our analysis on some of the interviews we had with the technocrats in the Living Lab Stratumseind. We were interested in understanding their interpretation of what and how the technologies and algorithms – which they were so invested in – could contribute to the project of ‘safety and security’.

Of Wanted and Unwanted Sounds

The so-called smart innovations which aim to contribute to enhance safety and security are often a direct result of the simple translation or transference of the application of technological possibilities across sectors. The sensors used in the various living lab projects of Eindhoven, were initially developed to solve purely technological problems. For example, tech company Sorama, which started in 2008 as a spin-off of the TU/e, specialised in the visualisation of sound and sound sensors. Sorama’s main mission is essentially to reduce ‘unwanted noise’, based on the inherent and unquestionable assumption that ‘environmental silence’ improves the quality of life. While in line with this mission, the initial aim of the company was to detect unwanted sounds in machines, and as a result make these machines more silent, Sorama has subsequently started developing products for different ends and industries, including for public space safety, security, and mobility issues.

Paul van Dooren works for Sorama, and is product owner of the Listener64, a sound sensor that can categorise and locate sound, which is commercially available in Europe and Asia. The Listener64 can for example identify breaking glass or aggressive voices, and subsequently show where exactly this sound is coming from in a 3D model of the street. This way, other information becomes available in addition to images recorded by cameras. The Listener64 sends triggers to the police as soon as it identifies certain sounds.

The unwanted sounds that the Listener64 detects, are: ‘a loud vehicle, aggressive people, breaking glass or any other sound disturbance.’¹¹ Detecting a loud vehicle or breaking glass might be relatively straightforward but detecting ‘aggressive people’ or ‘any other sound disturbance’ is not. In addition, in a machine, the meaning of the term ‘sound disturbance’ might be relatively clear, but in a dense and complex urban street such as Stratumseind, it is not so clear. Finding a sound ‘disturbing’ or not, rather than being an objective experience as assumed by the technocrats, is a subjective and contextual experience. This perception depends on what one is used to hearing, what one expects to hear, and on the meaning one gives to a certain sound (Bild 2019). Contrary to a technological reality then, social reality is interpreted differently by different people. Likewise, the category ‘aggressive people’ is quite ambiguous. During the interview, Paul explained who ‘aggressive people’ would be in this context, stating:

¹¹ See <https://www.sorama.eu/smart-city> [accessed 09-01-21]

In the end, there are people, members of the society, who have little respect for others. And I think that technology – definitely the way we implement and handle it – can handle that kind of stuff.

What is essentially happening here, is that by transposing the potential of sound technology directly to the field of security, implicitly a connection seems to be made between 'unwanted sound', 'environmental silence', 'quality of life' and 'aggressive people as people with no respect for others.' In other words, certain sounds in the city that are produced by 'aggressive people as people with no respect for others' are unwanted since they decrease the quality of life for other people, those with respect for others. By detecting and removing those 'unwanted sounds,' technology promises to improve the 'quality of life' for those people.

The idea of 'unwanted sounds' is also tightly related to the idea of 'wanted sounds.' The mission of Sorama is to 'contribute to a better sounding world' and to 'improve the quality of life.'¹² As we mentioned above, the aim of *Stratumseind 2.0* is to make the street 'safer, livable and more attractive,' by attracting a certain kind of people with a certain kind of behaviour to the street, and to create a certain kind of atmosphere that will be conducive to consumption (Allen 2006, 445). Local entrepreneurs in Stratumseind articulate this objective quite openly as the main reason for them to collaborate with the living lab experiments. Through their participation in the *Living Lab*, a promise is made to them that they will get more visitors and therefore sell more drinks.

On the one hand, groups of friends drinking beers without acting out their aggression behave according to the idea of how one is expected to behave in Stratumseind, since they fit in the social imaginary of the smart citizen as a civilised consumer (Brighenti and Karrholm 2018). On the other hand, people who do not fit into this imaginary will be labelled as disturbing and unwanted and will be singled out by means of technologies and algorithms, and eventually removed by the police.

Detecting Anomalies

Partly aiming at addressing such criticism towards the lack of contextuality in sound interpretation, next to the Listener64, Sorama is currently developing and testing (not in Stratumseind) an 'anomaly detector'. This algorithm is said to learn over time what 'normal behaviour' actually means in a particular area. This way, the algorithm becomes applicable to different contexts, and can adjust its triggers to what is considered normal in that particular context. For example, when it is used in a neighbourhood with a lot of construction work, the sounds of construction work, even though loud and disturbing, will not cause a trigger, because the algorithm learns that these sounds are normal in that area. Instead, a sudden silence in this context will be identified as an anomaly and will cause the

¹² See <https://www.sorama.eu/smart-city> [accessed 09-01-21]

algorithm to trigger the police. As explained on Sorama's website under 'smart city' products, the algorithm can 'detect anomalies in environmental noise and send a trigger to authorities.'

Image 7. Screenshot from <https://www.sorama.eu/> [accessed 09-01-21]

Paul explains that this detector is developed so that it is easier to use for the authorities,

Now [with the Listener64] one has to know a lot about the system to be able to use it and to receive the data one needs. With the anomaly detector one only has to install the sensor. The sensor will listen for a few days to learn what is normal, and when it has found a profile, it can identify deviations from that profile.

While the development of this technology shows that Paul and his team are aware of the fact that the meaning that we attach to sound depends on context, it nevertheless remains problematic to characterise 'normal behaviour' by what one can expect, based on the sensors' measurements over time and to trigger the police when so-called 'anomalies' are detected.

When asked about what would happen when, for example, people are having a passionate conversation in a language that is very different from one's own (e.g., Arabic), which could trigger the algorithm and the police because the sounds might be 'unexpected' and the sound is (unintentionally) coded as 'violent' by the programmers who have no contextual clues and no knowledge of the language and culture, Paul answered that he does not expect the algorithm to make a difference between Dutch and Arabic sounds. According to him, aggression has certain cross-culturally recognisable characteristics that would show similar sound patterns in different languages. It would therefore, according to Paul, be possible to distinguish between a fight and a passionate conversation in Dutch or any other language. A passionate conversation would not be the kind of sound that would trigger the sensor.

Nevertheless, cross-cultural psychological studies have found that recognising audible cues between cultures is problematic, and the way one interprets the emotion of someone else is an utterly subjective and cultural experience. The so-called *cultural proximity hypothesis* (Rosenthal et al. 1979) for example, states that miscomprehensions about emotions based on sound increase between people from

different language groups. It could thus be possible that people speaking a foreign language that is very different from the local one, have a higher chance of being misinterpreted by the sensor in Stratumseind, which is not trained at all in such cultural subtleties, as ‘aggressive’.

Another company that tries to identify ‘violent behaviour’ and notify the police, is Oddity, a company that develops camera software. The headline on their website reads ‘Meet Oddity.ai – The future of safety’, and below this heading: ‘We believe that through human and machine cooperation, Oddity can bring public safety to a whole new level.’¹³ The story of what Oddity does is as interesting as the story of how Oddity started. Thomas Alflen, 26 years old, whom the field researcher interviewed for the research, is director of Oddity. Enthusiastically he told her about the exciting journey he and his two study mates have taken. During his master’s in Business Entrepreneurship, Thomas had to set up a start-up in the field of technology and when looking for a market where technology could play a role and where he could set up a successful start-up, he found out that very little innovation took place in the public security sector. After doing some more research, he found that observers of the municipality spend hours in control rooms looking at camera images, waiting for situations where they have to intervene. If software could identify violent behaviour automatically, he thought, these observers would not have to watch the camera for whole days. Also, algorithms never get tired, so more incidents can be registered by algorithms than by humans, Thomas reasoned. Together with two study mates, he turned this idea into a business model and ‘entered the market.’ He refers to it as a ‘high risk, high reward choice.’ Since they finished their master’s two years ago, they continued with the start-up and set up their own company Oddity.ai.

After developing the software, they came into contact with the Dutch Institute for Security and Safety (DITSS) and *Living Lab Stratumseind*. During the same period, they participated in an AI challenge from the Netherlands Enterprise Agency (*Rijksdienst Voor Ondernemed Nederland*, RVO) which they won. These two developments gave them the opportunity to start a long-term pilot in Stratumseind in order to test their product. From September until December 2019, two cameras in Stratumseind were connected to a little box with Oddity’s software. They were content with the results: seven incidents of violence were recognized by the software, out of which four were not recognized by human observers. At the time of the research, Oddity was busy with giving presentations to police teams, having conversations with potential investors and trying to convince potential clients, while finetuning their smart software through pilots in *Living Lab Stratumseind*. The idea behind the smart software is that the work of observers, who usually look at

¹³ This was the literal text on <https://oddity.ai/> [accessed 12-11-19]. Oddity.ai renewed their website in May 2020, in order to show their new vision. They removed the lower text (‘We believe that through human and machine cooperation, Oddity can bring public safety to a whole new level’). It can therefore not be found anymore. The current subtitle states: ‘Oddity is first to develop a commercial violence recognition algorithm using advanced deep learning techniques’ [accessed 09-01-21].

camera images to monitor Stratumseind, will be eventually partly replaced by algorithms. Oddity trains their algorithm by feeding it two types of datasets:

1. One dataset contains 'normal' behaviour, which means the dataset does not contain incidents you want to register
2. The second dataset contains the anomalies (oddities) you aim to detect during analysis.¹⁴

How are these datasets of 'normal' and 'odd' behaviour compiled? Thomas said that he compiled these two data sets together with two colleagues. In order to do that, they searched for videos on YouTube and labelled them as 'normal' or 'violent' when they agreed with two out of three opinions. In turn, they feed the videos to the algorithm to teach it what normal behaviour looks like and what violent behaviour looks like. During the time that the algorithm is tested in Stratumseind, feedback is given as well, so that the algorithm can continue to learn. What is interesting though is that the algorithm tends to misinterpret behaviour with a bias towards overestimating violence. Thomas explains:

It often happens that the algorithm labels normal behaviour as violent. This is called a false positive. But it hardly ever happens that the algorithm considers violent behaviour as normal.

According to Thomas, the first pilot in Stratumseind¹⁵ showed that the tested concept was 'proven'. Now they still have to 'fine-tune' the algorithm so that it will give fewer false positives and it will be easier for the police to work with. Because according to him, 'with many false positives, the police are often paged for nothing.' The algorithm is therefore presented primarily as time and cost efficient for the police.

What is interesting though is that the algorithm is trained with videos taken from YouTube, and that the local context is completely ignored by the technocrats. The dynamics underlying aggression and violence in the street, or the role of alcohol or social media are not investigated or given attention by the team of Thomas. When the field researcher asked Thomas whether he thought there could be a risk of developing an unconsciously biased algorithm when three white men train an algorithm on what violent and non-violent behaviour looks like, he answered that the risk exists but that it has been mitigated mainly by upholding onto a ground

¹⁴ This was the literal text on <https://oddity.ai/> [visited on 12-11-19]. Oddity.ai renewed their website in May 2020 in order to show their new vision. This text can therefore not be found back anymore.

¹⁵ The software was piloted from September until December 2019, when two cameras in Stratumseind were connected to a little box with Oddity's software. The company was content with the results: seven incidents of violence were recognized by the software, out of which four were not recognised by human observers. The only problem was the amount of false positives, so they continued the pilot with three cameras until June 2020.

rule: violence is physical contact. This implies that other types of violence, for example verbal violence, let alone structural violence, are not recognised as such. Another way they have tried to counter the bias, he claims, is by using diverse range of data 'like video material from India, China, Russia, and other countries,' which is also the reason 'why the algorithm can be used all over the world.'

When asked why they were interested in identifying violence in the first place, Thomas answered:

Violence wasn't the first thing we wanted to identify. First, we asked the market: 'what do you want to identify?' because we wanted to have a good business model.

Violence turned out to be what the market was interested in identifying. According to Thomas, violence is therefore a concept of market use like any other and it is a rather unambiguous and simple concept that can be taught to and learned by an algorithm. Thomas states that the algorithm 'is a very simple solution for a simple problem.' As these answers highlight, there is a remarkable lack of awareness of the complexity of violence among technocrats – of its contextual nuances, and most importantly, of the consequences that can result for certain people when they are classified as 'violent', 'dangerous' or 'aggressive' by an algorithm.

In computational science, the anomaly is the outlier, the 'dissonance' in the pattern, caused by 'an extreme manifestation of the random variability inherent in the data' or 'an error in calculating or recording the numerical value' (Frank 1969, 1). The anomalies or outliers in the data used to be regarded as errors and noise that had to be eliminated, but later, a new school of thought in statistics started seeing outliers as 'something interesting, which points to potentially relevant behaviour and observations that need to be investigated further' (Aradau and Blanke 2018, 8). From then onwards, the detection of anomalies in data became a goal in itself, together with 'pattern recognition.' This became a central feature of smart security technologies. Key areas for anomaly detection techniques are terrorism, cybersecurity, online fraud, and critical infrastructure protection (Aradau and Blanke 2018, 9). Regardless of their different fields of application, anomaly detection and pattern recognition are the two epistemic tools of algorithmic governance (Pasquinelli 2015). As Pasquinelli argues,

Today the Abnormal re-enters the history of governance and philosophy of power in a mathematical way, as an abstract and mathematical vector. Power in the age of algorithmic governance is about steering along these vectors and navigating an ocean of data by recognising waves of patterns, and in so doing, taking a decision anytime an anomaly is encountered, taking a political decision when a thousand

anomalies rise their head and make a new dangerous pattern
emerge (Pasquinelli 2015, 8).

For technocrats, the term 'anomaly' in relation to behaviour, is a property that is attached to a situation or individual. When someone's behaviour in urban space is 'anomalous' – deviating from the pattern – a trigger is sent to the police. The police, then, will treat this trigger as a warning for a potentially dangerous situation. The label 'anomaly' thus transforms into 'dangerous' or 'risky' and becomes a property of that particular situation. People who behave differently, who are anomalies or outliers, are potentially dangerous. Translated into the field of security, this means constant monitoring of 'normality' and removal of 'difference.' The removal of difference is becoming an increasingly normalised idea and practice in security industries (Aradau and Blanke 2018, 20). This form of policing of 'anomalies' and 'deviance' creates a public space where certain people are 'out of place' while others 'belong' (Pali and Schuilenburg 2019).

The 'Smart' as a Potential Amplifier of Inequality

As argued above, creators and proponents of smart technologies and algorithms that aim at monitoring and regulating people's behaviour in *Stratumseind* by detecting 'anomalies' and removing 'unwanted sounds' in the pursuit of safety and security, present this as an apolitical mission, a mission, according to Sorama, that is beneficial 'for all people, wherever they are.' But when smart technologies are used in a security and safety context, they have the power to draw boundaries between what and who is acceptable, normal, suspicious, dangerous and what and who is not (Pali and Schuilenburg 2019). Different scholars have shown that the use of smart technologies in public spaces risks bringing forth consequences that were initially not intended by the technologists, companies, policy makers or governments. Even though unintended, these consequences can lead to the reinforcement of social inequalities, classification, stigmatisation, and exclusion.

People and institutions that are perceived and deemed as experts in society, have the power to produce knowledge which in turn produces power (Hacking 1990). When they categorise and label people, these categories and labels are perceived as expert knowledge. Therefore, experts have the power to create or make up 'kinds of people' (Hacking 2006). In *Living Lab Stratumseind* it is the technologists, computer programmers, data analysts and urban planners who are perceived as experts. They develop technologies which are fed categorisations like 'normal', 'abnormal', 'deviant', 'anomalous' or 'risky' behaviour. These labels are built into the technologies and therefore risk to become treated as solid and objective labels. According to Ruha Benjamin, 'tech fixes often hide, speed up, and even deepen discrimination', and this is often not caused by bad intention of the makers, but because the makers 'ignore and thus replicate social divisions' (Benjamin 2019, 8). Once a technology is implemented in a city, it is hard to trace back who developed the technology based on which information, assumptions and ideas. The 'man behind the screen,' writes Benjamin, is invisible.

'Smart' as Neutral

When technology is used as a way to improve human decision making, it is important to also think about the disadvantages of technology – the bias, the false positives, the worldview of the designers that is built into the algorithm. The assumption that technology is objective and neutral, gives it an incredible power, since the 'knowledge' it produces, the way it categorises people, will be perceived as objective and therefore as legitimate knowledge. In other words, the ideas of those who program the software of these technologies and build algorithms will be considered as objective and scientific knowledge. As mentioned, for the tech engineers, technology is neutral and therefore superior. For example, Thomas, not the only respondent who perceives algorithms as 'superior' over human decisions, states:

You will always have human mistakes in the algorithm, but in the end an algorithm can become better than a human being. It can become better in recognising violence, because it doesn't get tired. There exist examples that violence is not recognised by a human, but it is recognised by the algorithm. But still, you will always keep a margin of error. You will always keep that with algorithms. The question is: what is acceptable? Algorithms are always much more critiqued than humans, while humans make more mistakes.

Both Thomas and Paul emphasised several times that it is the police that has the last say in deciding what should be done. The algorithm gives a trigger, but it is the police that has to make the final decision. Paul said:

You will always encounter false positives. As a policeman or *boa*¹⁶ from the municipality, you have the possibility to check on something. The human being must always decide whether one should intervene or not. We only say: we have detected something that looks like aggression, so go and have a look, through a camera or in person, and decide yourself – as a human being – what you will do.

It is, however, unclear whether and to what degree the police are aware of the shortcomings of the algorithm, and even whether they would consider this a shortcoming at all. During an interview with the project manager of the police team that works in Stratumseind, he said that he was not informed about most of the developments of the living lab, that he learns about them through the newspaper, and that he often does not know how the implemented technologies

¹⁶ *Boa's* (*buitengewoon opsporingsambtenaar*) are officers that support the police in investigative practices. They often have a specialised field of work. They are also allowed to check identity cards, arrest suspects and issue fines in order to maintain local order and safety. (see <https://www.politie.nl/themas/buitengewoon-opsporingsambtenaar.html> [accessed 09-01-21])

work. This is not representative, as the police is sometimes involved in the projects and technology development of the *Living Lab Stratumseind* as experts in the field of safety and security, and with street-knowledge.¹⁷ However, this does not mean that they have real influence, and it is the tech companies and the municipality that decide whether and how they involve the police in the process.

Whereas Thomas considers 'the algorithm as supportive, not decisive,' Oddity's sensor is nevertheless marketed pitching on its advantage to detect four times¹⁸ as much violence as a human being.

Also Sorama sells their product with claims of 'fast, efficient and effective [technology]', 'visualised facts and proven analysis and algorithms' and sound waves that 'expose all aspects of the root cause.' Paul in fact admits that there exists a tension between the commercial character of their company and the interests of the public field in which they operate:

The tension is that we are a commercial company. If we make beautiful sensors, we also want to sell them.

However, this makes for potential biases and mistakes the algorithm could make, which would be important for clients, like the municipality or police, and end users to know. Dubois and colleagues explain that we are inclined to ignore the fact that all technological sensors are human artefacts, historical constructions, that rely on the evolution between knowledge and technology. They state:

[T]he information sensors provide (be they numbers on a scale, verbal labels, or something else altogether) is so easily readable for those trained in their use since childhood, that they lend the impression of furnishing a *more direct, obvious and objective relation to the properties of the world than our human senses*. That is, the obviousness of sensor functioning overlooks their status as artefacts, ignoring that they are historical constructions of human cultures and/or civilisations that rely on the evolution between knowledges and technology (Dubois et al. 2014, 100, *emphasis added*).

As mentioned previously, technocrats like Paul and Thomas have no specific knowledge about violent behaviour, about the people exhibiting such behaviour, about contexts and situations eliciting or inducing such behaviour, or even about the situation in Stratumseind. Still, they are the ones who develop the algorithm that decides which behaviour is the one that will trigger the police. These triggers

¹⁷ This was, for example, the case with the project De-escalate.

¹⁸ A similar case is the software adopted by the Los Angeles Police Department developed by a company called PredPol. The algorithm of PredPol is said to guess two times better than a human being the block of Los Angeles where a petty crime is likely to happen (see Pasquinelli 2015).

will have consequences for the people defined as suspicious, consequences Thomas and Paul are not aware of.

Image 8. Screenshot from: <https://oddity.ai/#> [accessed 09-01-21]

When the algorithm will be used at Stratumseind in the future and its indications will be treated as objective information, no one will remember who Thomas and Paul were, how they designed the technology, how their worldview has influenced the algorithm, how false positives are produced or what kind of bias the algorithm produces. Neither will anyone be able to trace back how the technology was designed, which data was used to train it and how this training process was taking place. If the technology is used in other parts of the world, it will be even harder to trace back how and by whom it was initially designed. When the assumptions, biases, and worldviews that are incorporated into the technology, are not discussed and scrutinised, this has consequences for the way the algorithms are used. By not reflecting on the way the algorithm is developed, the algorithm can reproduce, reinforce, and create classifications and categorisations of people and hierarchies of those categorisations that ‘travel’ from the minds of the makers into the algorithm (Lyon 2003).

Sorting Kinds of People

Social sorting processes and practices are a core drive of surveillance, security, punishment and control. Forms of categorisation and classification, division and subdivision, differentiation and hierarchisation are routinely applied to govern populations according to perceived risk or value for the purpose of assessment and judgement (Monahan 2011). They produce different and unequal forms of inclusion and exclusion for those respective categories, such as access and eligibility to rights, services and entitlements, but also in terms of suspicion, monitoring, control, and punishment, therefore affecting life chances (Lyon 2003). In fact, the etymology of the word sorting derives from the Latin *sorte* which

means lot, fate, or destiny, and social sorting becomes self-fulfilling: a process of deciding upon the fate of others.

Tech companies like Oddity and Sorama need to substantially simplify reality in order to make it manageable. They transform individuals into algorithmic subjects to compete on the security industry market (Aradau and Blanke 2018). As Peeters and Schuilenburg (2018) argue, algorithmic decision-making becomes a matter of classification rather than judgment of individual cases. Didier Bigo clearly puts into words the danger of managing security issues through bits of data that are categorised by 'normal' and 'abnormal', and explains how the harmful consequences of this form of governance are invisible to 'wanted' and 'normalised' citizens:

The narrative of filtering through profiles that 'smart' borders can achieve supports the differentiation of EU citizens for whom borders will always be open and quick (...). The system prevents most travellers, the 'normalized' ones, from even seeing the controls. These 'normal' travellers have the impression of moving freely, because surveillance does not stop them. They mistake speed for freedom – never realizing how easily they can change category and become undesirables – not because of anything they have done, but because of the profile associated with their data double. They love the 'smart' borders, because they are watched but are not stopped. They participate in this surveillance; they perform it; they even contribute to it by entering their data into the systems of control, thereby paying for the speed and comfort that are promised. The invisibilisation of the dataveillance for well-off, normalised travellers does not make them freer, just less aware that they are at risk of becoming 'abnormalized' (Bigo 2014, 218-219).

As in the case of border control, in cities where smart technologies are used to detect suspicious behaviour and suspicious individuals, 'normalised' residents and visitors of the city will not notice the surveillance technology. The system will welcome them into the city, make them feel safe and present them a city with an attractive atmosphere. They will be watched and protected, and therefore, they will not mind participating in the smart city utopias and laboratories. The 'abnormalized' individuals, on the other hand, will pay the price for this safe and nice city. They will be aware of the dataveillance as they are targeted as 'unwanted.' The police will pass by to 'check on what they are doing,' which will have an impact on the way they experience public space. Aware of the fact that they do not fit in, they will be slowly 'designed out' of the city.

Our research showed that actors like Thomas and Paul mainly place themselves in the perspective of the police and the victims of violence, and never in the perspective of the violence perpetrator. When asked directly about how exactly the aggression detection works and how to make sure what aggression actually is, Paul answers:

No, well, it is maybe good to say that... you know, it is not 100% fail proof. So, let me say it like this, the algorithm can create a faulty conclusion when it registers football supporters that are being very enthusiastic with each other. But I find it a reassuring thought that in some way the safety of all people is being looked after. I personally don't mind so much about privacy as long as it does not recognise me as an individual. I think Google knows much more about us than Sorama. I find it a nice thought to know that when something happens to me, there is a sensor system that can do something about that. You are not alone. In the end, there are people in society who have little respect for others. And I think that technology – definitely the way we implement and handle it – is targeted to handle that kind of stuff. Not to do something to people who are having fun or to take away privacy from people. That is not what we are interested in.

Paul finds it a 'reassuring thought' that the area where he is, is being watched by a sound sensor. He thus places himself in the perspective of the person that will be protected by the sensor, the person that might be the victim of aggression. The people whom the sensor should target – 'people with little respect for others' – are perceived by Paul as different from himself. Interestingly, he distinguishes them from 'people who are having fun.' The consequences these categorisations can have on society, can be understood through the so-called 'looping effect' (Hacking 1990). When we perceive a 'kind of people' to be a definite group in a fixed reality – for example, 'respectless people,' as expressed by Paul – we treat this 'kind of people' differently, which has in turn an effect on those people.

The question is who is to be held responsible for social sorting and the creation of kinds of people through smart technologies. Also, it is important to question whether it is ethical for the municipality to collaborate with tech companies without having the ability to control and ethically examine the technologies that are used to govern their city. It raises the question of whether socially driven urban visions are given priority in the design of living labs and smart technologies, or whether other (economical and commercial) interests have become more important in governing the city of Eindhoven.

Conclusions

Despite all claims to the contrary, smart city projects with their limitless faith in technologies and algorithms, carry potential risks for individuals and for our societies. This blind faith in technological solutionism and superiority and their ability to adequately address our social problems must be challenged by questioning the assumptions underlying such projects, by tracing their developments and mapping their implementations. Critical research in this area has mostly focused on the consequences that smart city-based living labs have on privacy, but in our article, we aimed to show that there are additional concerns besides privacy to be taken into account in these developments.

Our research showed that technological visions and solutions, embedded in smart technologies and algorithms, are uncritically translated into complex social fields, such as safety and security in our cities. This comes with significant risks for our societies, such as the creation and control of 'abnormal' kinds of people who are deemed dangerous. The assumptions of objectivity, neutrality, superiority, and universalism that come with the use of algorithms and technologies, the lack of transparency and ethical regulations for their development, and the diffuse and unclear responsibilities for their consequences significantly exacerbate these risks.

The reduction and simplification of social life into patterns and anomalies bring with it a significant impoverishment of our social and political imagination. The market driven priorities in smart technology development clearly conflict with social priorities; therefore, public institutions should resist prioritizing market objectives to the detriment of social ones. If we continue to delegate the governance of our cities and its social problems to technocrats, instead of making us smarter, such technologies can make us foolish.

Acknowledgments

We would like to thank the respondents of this research, who despite being aware of the critical perspective of the research on the smart city initiative and on the technologies and algorithms developed there, open, and generously discussed their work. It is in the constructive dimension of critical collaborations and engagements that the future of smart city projects lies. We also want to thank the editor of this special issue Tereza Østbø Kuldova and the anonymous reviewers for their insightful comments on previous versions of this article.

Author Bios

Sofie Doorman recently obtained her master's degree in Cultural and Social Anthropology at the University of Amsterdam. She also has a background in criminology at the KU Leuven and did an internship at the European Forum for Restorative Justice. After graduation, she worked as a junior lecturer in anthropology at the UvA. Her main interests are security studies, critical criminology, science and technology studies, urban anthropology, and philosophy.

Brunilda Pali is a Post-doctoral Researcher in the Leuven Institute of Criminology at KU Leuven. She is co-editor of *Restoring Justice and Security in Intercultural Europe* and *Critical Restorative Justice*. Besides criminology, she has a background in psychology, gender studies, and cultural studies. She is also currently the Secretary of the European Forum Restorative Justice Board. She publishes on multiple themes, like restorative justice, critical criminology, security, social movements, gender, and arts.

References

- Allen, John. 2006. Ambient power: Berlin's Potsdamer Platz and the seductive logic of public spaces. *Urban Studies* 43(2): 441-455.
<https://doi.org/10.1080/00420980500416982>
- Aradau, Claudia and Blanke, Tobias. 2018. Governing others: Anomaly and the algorithmic subject of security. *European Journal of International Security* 3(1): 1-21.
<https://doi.org/10.1017/eis.2017.14>
- Benjamin, Ruha. 2019. *Race after technology*. Oxford: Polity.
- Brighenti, Andrea Mubi, and Karrholm, Mattias. 2018. *Urban walls: Political and cultural meanings of structures and surfaces*. London: Routledge.
<https://doi.org/10.4324/9780203730225>
- Burrell, Jenna. 2016. How the machine "thinks": Understanding opacity in machine learning algorithms. *Big Data & Society* 3(1).
<https://doi.org/10.1177/2053951715622512>
- Cheney-Lippold, John. 2011. A new algorithmic identity: Soft biopolitics and the modulation of control. *Theory, Culture & Society* 28(6): 164-181.
<https://doi.org/10.1177/0263276411424420>
- Bigo, Didier. 2014. The (in)securitization practices of the three universes of EU border control: Military/Navy - border guards/police - database analysts. *Security Dialogue* 45(3): 209-225.
<https://doi.org/10.1177/0967010614530459>
- Bild, A. E. 2019. *Understanding the urban auditory experience: Linking uses, users, and environments*. Doctoral Dissertation, University of Amsterdam.
- Datta, Ayona. 2015. New urban utopias of postcolonial India: 'Entrepreneurial urbanization' in Dholera smart city, Gujarat. *Dialogues in Human Geography* 5 (1): 3-22.
<https://doi.org/10.1177/2043820614565748>

- Dubois, Daniele, Coler, Matt, and Ortche, Heinrich. 2014. Knowledge, sensory experience, and sensor technology. In *The World in Prismatic Views: Proceedings of the Second Interdisciplinary CHESS Interactions Conference*, edited by Rangacharyulu, Chary, Haven, Emmanuel, and Juurlink, Bernhard, 97-133. World Scientific Publishing Company: Singapore.
https://doi.org/10.1142/9789814583411_0006
- Frank, E. Grubbs. 1969. Procedures for detecting outlying observations in samples. *Technometrics* 11(1): 1-21.
<https://doi.org/10.1080/00401706.1969.10490657>
- Galič, Maša. 2019. *Surveillance and privacy in smart cities and living labs: Conceptualising privacy for public space*. Rotterdam: Optima Grafische Communicatie.
- Gillespie, Tarleton. 2014. The relevance of algorithms. In *Media technologies: Essays on communication, materiality, and society*, edited by Gillespie, Tarleton, Boczkowski, Pablo, and Foot, Kirsten, 167-194. Cambridge, US: MIT University Press.
<https://doi.org/10.7551/mitpress/9780262525374.003.0009>
- Hacking, Ian. 1990. *The taming of chance*. Cambridge: Cambridge University Press.
<https://doi.org/10.1017/CBO9780511819766>
- Hacking, Ian. 2006. Making up people. *London Book Review* 28(16): 23-26.
<https://doi.org/10.1353/abr.2006.0177>
- Hong, Sun-ha. 2020. *Technologies of Speculation: The Limits of Knowledge in a Data-Driven Society*. New York: NYU Press.
- Ingold, Tim. 2011. *Being Alive: Essays on Movement, Knowledge and Description*. London: Routledge.
<https://doi.org/10.4324/9780203818336>
- Jasanoff, Sheila and Kim, Sang-Hyun (eds.). 2015. *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*. Chicago: University of Chicago Press.
<https://doi.org/10.7208/chicago/9780226276663.001.0001>
- Kitchin, Rob. 2014. The real-time city? Big data and smart urbanism. *GeoJournal* 79 (1): 1-14.
<https://doi.org/10.1007/s10708-013-9516-8>
- Kitchin, Rob. 2015. Making sense of smart cities: addressing present shortcomings. *Cambridge Journal of Regions, Economy and Society* 8 (1): 131-136.
<https://doi.org/10.1093/cjres/rsu027>

- Sofie Doorman & Brunilda Pali – *Underneath the Promise of Safety and Security in a 'Smart City'*
- Kitchin, Rob, and Dodge, Martin. 2011. *Code/space: Software and everyday life*. Cambridge, US: MIT University Press.
<https://doi.org/10.7551/mitpress/9780262042482.001.0001>
- Kviselius, Niklas, and Andersson, Per. 2009. Living labs as tools for open innovation. *Communications & Strategies* 1(74): 75-94.
- Lacinák, Maroš, and Ristvej, Jozef. 2017. Smart city, safety and security. *Procedia Engineering* 192: 522-527.
<https://doi.org/10.1016/j.proeng.2017.06.090>
- Lahiji, Nadir. (ed). 2014. *Architecture against the post-political: Essays in reclaiming the critical project*. London: Routledge.
<https://doi.org/10.4324/9781315780375>
- Lindner, Christoph and Meissner, Miriam (eds.). 2018. *The Routledge companion to urban imaginaries*. London: Routledge.
<https://doi.org/10.4324/9781315163956>
- Lyon, David. (ed.) 2003. *Surveillance as social sorting: Privacy, risk and digital discrimination*. New York: Routledge.
- Mitchell, Timothy, 2002. *Rule of experts: Egypt, techno-politics, modernity*. Berkeley, CA.: University of California Press.
<https://doi.org/10.1525/9780520928251>
- Mittelstadt, Brent Daniel, Allo, Patrick, Taddeo, Mariarosaria, Wachter, Sandra and Floridi, Luciano. 2016. The ethics of algorithms: Mapping the debate. *Big Data & Society* 3(2). Online <https://doi.org/10.1177/2053951716679679>
- Morozov, Evgeny. 2014. *To save everything, click here: The folly of technological solutionism*. New York: Public Affairs.
- Morozov, Evgeny and Bria, Francesca. 2018. *Rethinking the smart city. Democratizing urban technology*. New York: The Rosa Luxembourg Foundation.
- Monahan, Torin. 2011. Surveillance as cultural practice. *The Sociological Quarterly* 52 (4): 495-508.
<https://doi.org/10.1111/j.1533-8525.2011.01216.x>
- Naafs, Saskia. 2018. Living laboratories. The Dutch cities amassing data on oblivious residences. *The Guardian*, 1 March 2018. <https://www.theguardian.com/cities/2018/mar/01/smart-cities-data-privacy-eindhoven-utrecht> [accessed 08-1-20]

- Pasquale, Frank. 2015. *The black box society*. Cambridge, MA: Harvard University Press.
<https://doi.org/10.4159/harvard.9780674736061>
- Pasquinelli, Matteo. 2015. *Anomaly detection: The mathematization of the abnormal in the metadata society*. Talk given at Transmediale. [file:///C:/Users/u0058818/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/Anomaly Detection The Mathematization of%20\(1\).pdf](file:///C:/Users/u0058818/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/Anomaly%20Detection%20The%20Mathematization%20of%20(1).pdf) [accessed 15 January 2021].
- Peeters, Rik, and Schuilenburg, Marc. 2018. Machine justice: Governing security through the bureaucracy of algorithms. *Information Polity* 23 (3): 267-280.
<https://doi.org/10.3233/IP-180074>
- Pierson, Jo, and Lievens, Bram. 2005. Configuring living labs for a 'thick' understanding of innovation.' *Ethnographic Praxis in Industry Conference Proceedings* 1: 114-127.
<https://doi.org/10.1111/j.1559-8918.2005.tb00012.x>
- Rosenthal, Robert, Hall, Judith, DiMatteo, Robin, Rogers, Peter, and Archer, Dane. 1979. *Sensitivity to nonverbal communication: The PQNS test*. Baltimore: Johns Hopkins University Press.
<https://doi.org/10.1016/B978-0-12-761350-5.50012-4>
- Sadowski, Jathan, and Pasquale, Frank. 2015. The spectrum of control. A social theory of the smart city. *First Monday* 20(7): 1-22.
<https://doi.org/10.5210/fm.v20i7.5903>
- Sadowski, Jathan, and Bendor, Roy. 2019. Selling smartness: Corporate narratives and the smart city as a sociotechnical imaginary. *Science, Technology & Human Values* 44 (3): 540-563.
<https://doi.org/10.1177/0162243918806061>
- Schuilenburg, Marc. 2015. *The securitization of society: Crime, risk, and social order*. New York: New York University Press.
<https://doi.org/10.18574/nyu/9781479854219.001.0001>
- Schuilenburg, Marc, and Peeters, Rik. 2018. Smart Cities and the Architecture of Security: Pastoral Power and the Scripted Design of Public Space. *City, Territory and Architecture* 5 (13): 1-9.
<https://doi.org/10.1186/s40410-018-0090-8>
- Schuurman, Dimitri, Mahr, Dominik, De Marez, Lieven, and Ballon, Pieter. (2013). A fourfold typology of living labs: an empirical investigation amongst the ENoLL community. In *2013 International conference on engineering,*

- Sofie Doorman & Brunilda Pali – *Underneath the Promise of Safety and Security in a 'Smart City'*
technology and innovation (ICE) & IEEE international technology management conference (pp. 1-11). IEEE. <https://doi.org/10.1109/ITMC.2013.7352697>
- Scott, Kristin. 2016. *The digital city and mediated urban ecologies*. Boston, MA: Palgrave Macmillan.
<https://doi.org/10.1007/978-3-319-39173-1>
- Söderström, Ola, Paasche, Till, and Klauser, Francisco. 2014. Smart cities as corporate storytelling. *City* 18(3): 307-320.
<https://doi.org/10.1080/13604813.2014.906716>
- Townsend, Anthony. 2013. *Smart cities: Big data, civic hackers, and the quest for a new utopia*. New York: W.W. Norton & Company.
- Thierer, Adam. 2016. *Permissionless innovation: The continuing case for comprehensive technological freedom*. Arlington: Mercatus Center at George Mason University.
- Van Dijck, Jan. 2014. Datafication, dataism and dataveillance. Big data between scientific paradigm and ideology. *Surveillance & Society* 12(2): 197-208.
<https://doi.org/10.24908/ss.v12i2.4776>
- Vanolo, Alberto. 2014. Smartmentality. The smart city as disciplinary strategy. In: *Urban Studies* 51(5), 883- 898.
<https://doi.org/10.1177/0042098013494427>
- Vanolo, Alberto. 2016. Is there anybody out there? The place and role of citizens in tomorrow's smart cities. *Futures* 82: 26-36.
<https://doi.org/10.1016/j.futures.2016.05.010>
- Wiig, Alan. 2015. IBM's smart city as techno-utopian policy mobility. *City analysis of urban trends, culture, theory, policy, action* 19 (2-3): 258-273.
<https://doi.org/10.1080/13604813.2015.1016275>
- Wilson, Japhy, and Swyngedouw, Erik. 2014. *The post-political and its discontents: Spaces of depoliticization, spectres of radical politics*. Edinburgh: Edinburgh University Press.
<https://doi.org/10.3366/edinburgh/9780748682973.001.0001>
- Williamson, Ben. 2016. Political computational thinking: Policy networks, digital governance and "learning to code". *Critical Policy Studies* 10 (1): 39-58.
<https://doi.org/10.1080/19460171.2015.1052003>
- Yeung, Karen. 2018. Algorithmic regulation: A critical interrogation. *Regulation & Governance* 12(4): 505-523.
<https://doi.org/10.1111/rego.12158>