Article

The Making of Crime Predictions: Sociotechnical Assemblages and the Controversies of Governing Future Crime

Daniel Edler Duarte

University of São Paulo, Brazil
danielcedler@usp.br

Abstract

We are witnessing an upsurge in crime forecasting software, which supposedly draws predictive knowledge from data on past crime. Although prevention and anticipation are already embedded in the apparatuses of government, going beyond a mere abstract aspiration, the latest innovations hold out the promise of replacing police officers' "gut feelings" and discretionary risk assessments with algorithmic-powered, quantified analyses of risk scores. While police departments and private companies praise such innovations for their cost-effective rationale, critics raise concerns regarding their potential for discriminating against poor, black, and migrant communities. In this article, I address such controversies by telling the story of the making of CrimeRadar, an app developed by a Rio de Janeiro-based think tank in partnership with private associates and local police authorities. Drawing mostly on Latour's contributions to the emerging literature on security assemblages, I argue that we gain explanatory and critical leverage by looking into the mundane practices of making and unmaking sociotechnical arrangements. That is, I address the chain of translations through which crime data are collected, organized, and transformed into risk scores. In every step, new ways of seeing and presenting crime are produced, with a significant impact on how we experience and act upon (in)security.

Introduction

The goal of anticipating criminal behavior and preventing an incident before it happens has long been pursued by security practitioners (Deflem 1997). Until a few years ago, research in the field of crime analysis had only managed to describe the spatio-temporal distribution of occurrences, but recent developments in environmental criminology, computer science, and econometric modelling have arguably moved us closer to the "holy-grail of policing" (Ferguson 2017a: 1115). Based on two core assumptions—that when it comes to criminal patterns, "past is prologue" (Perry et al. 2013: 8) and that "built-in features of the environment strongly influence associated aftershocks" (Muggah 2016a)—crime forecasting services are presently available for police departments that keep a few years' worth of records on crime and whose administration can afford the initial investment and periodic maintenance.¹

Yet evidence of the impact of crime forecasting remains scarce. As much as enthusiasts applaud it as a "brilliantly smart idea" (Tett 2014), the lack of in-depth accounts of specific systems casts a shadow over predictions. Most police departments refrain from sharing data and talking about strategies with the public,

¹ While vendors in the public safety industry have popularized the term, "predictive policing" encompasses software that predicts victims, offenders, or locations and that employs various methods, including self-exciting point processes, risk-terrain modelling, artificial neural networks, and Markov chain geostatistics. For taxonomies of the multiple products in the market, see Perry et al. (2013) and Robinson and Koepke (2016).

and those responsible for writing codes and designing software are often unwilling to fully disclose details regarding how their tools are built (Lum and Isaac 2016). Despite recent advances in the literature,² we still have scant information on crime dynamics, can barely evaluate results, and cannot tell how inputs are transformed into outputs. As often happens with big data and machine-learning innovations, automated decisions with deep influence in society are made by algorithms hidden in black boxes (Pasquale 2015).

Predictive analytics have also been the object of heated debate regarding checks and balances for police operations. On one hand, private companies and police departments often join forces to promote these tools, advertising a new era of more efficient control in which costs are cut, accuracy is enhanced, and arbitrary arrests are reduced (Bratton and Malinowski 2008; Beck and McCue 2009; Mohler et al. 2015). On the other hand, critical scholars and civil rights advocates claim that such tools advance neoliberal practices of mass incarceration (Benjamin 2019), also raising concerns regarding underlying racial profiling and risks of technocratic dystopia (Jefferson 2018; Scannell 2018). In short, critics have claimed predictive policing systems concentrate “law enforcement in already over-policed communities while ignoring underlying causes of crime—structural racism, systemic disinvestment, and poverty” (Shapiro 2019: 457).

Despite the above controversies, the Igarapé Institute, a think tank devoted to issues of citizen security and urban fragility, recently partnered with public and private associates to design the “world’s first public-facing crime forecasting platform” in Rio de Janeiro, Brazil (Muggah 2017).³ Launched during the 2016 Olympics, CrimeRadar aimed to provide “a way to help citizens take action to promote their own security and safety rather than relying exclusively on the police” (Griffiths 2016). As Robert Muggah (2017), Igarapé’s director, further clarifies, “the hope is that [it] can be applied by local businesses, politicians, and activists to call for action to improve safety. Communities can use the tool to mobilize for change as well as to shape prevention strategies.”

In this article, I investigate the development of CrimeRadar with a view to offering insights for critical approaches to security and surveillance technologies. Drawing on recent debates on the performativity of security devices (Bourne, Johnson, and Lisle 2015; Aradau and Blanke 2017; de Goede 2018), I propose to supplement grand narratives of a “revolution in police affairs” (Palidda 2010) and an algorithmic turn in governance (Rouvroy and Berns 2013) with empirically situated practices of assembling. As Ziewitz (2016) argues, close scrutiny and large doses of skepticism are necessary when analyzing the development of technological solutions, not only to evade the siren song of techno-enthusiasts but also to avoid the kind of superficial structural critiques that depict algorithms simply as “pathways through which capitalist power works” (Lash 2007: 71). While sweeping arguments about neoliberal modes of order can assist in tracing the global context of security innovations (Wacquant 2009), such frameworks have been criticized for failing to capture the multiple ways in which crime is rendered (in)visible, (un)knowable, and actionable (Aas, Gundhus, and Lomell 2009). Thinking in terms of assemblages shifts our focus from the immutable essences and purposes of technologies toward more productive research of practices of association (Latour 2005). Instead of jumping to conclusions about what technologies do, this draws attention to how they are composed.

There is strong theoretical work on actuarial justice and algorithmic policing in both surveillance and critical security studies (Harcourt 2007; Lyon 2007; Leese 2014). A lot has also been written on how predictive policing plays out on the ground, contraposing claims that data-driven policing is more efficient and less

² Recent contributions to the field include ethnographies of the security industry (Shapiro 2019), considerations of pattern-based algorithms (Kaufmann, Egbert, and Leese 2019), analyses of how predictive systems impact productivist policing (Benbouzid 2019; Brayne 2020), and reviews of the assumptions of predictive policing algorithms and modes of evaluation and accountability (Bennett Moses and Chan 2018).

³ Igarapé is a non-profit organization that has achieved considerable global outreach, helping set the agenda on issues of peace building and urban violence throughout Latin America and Africa. It has almost forty employees and fellows, and its operations are supported by development agencies, international foundations, and private donors.

discriminatory than traditional reactive policing models.⁴ Nevertheless, the way crime forecasting programs are designed remains largely an open empirical question.⁵ The problem of neglecting this process is that if we only analyze the impact of security technologies once they become functioning instruments, we lose most of the ways in which they change, stabilize, and depoliticize social relations. As Akrich (1992: 222) reminds us, after artifacts are produced “the processes involved in building up technical objects are concealed. The causal links they establish are naturalized. There was, or so it seems, never any possibility that it could have been otherwise.” Thus, I aim to “uninvent” crime prediction as an “indisputable fact by showing the rhetorical and material practices of its demonstration” (Suchman 2020: 3). In other words, this article documents the many political choices, criminological assumptions, and inherent uncertainties involved in the algorithmic analysis of crime patterns, raising evidence against the supposed impartiality and color-blindness of predictive policing solutions.

This research hinges upon fieldwork activities conducted through a sixteen-month period in Rio. In September 2016, I was offered a visiting fellowship at Igarapé and got involved with the development of CrimeRadar.⁶ I arrived in Brazil a few weeks after the app was launched, but still managed to retrace the practices of the programmers, designers, statisticians, and police officers from field sites (crime scenes) to the app, as the criminal events were translated, step by step, from dynamic happenings into ordered data streams that fed maps on future crime. The reconstruction of the app’s assemblage is based on a methodological combination of focused interviews and frequent informal conversations with the team of developers and security professionals who took part in the project, as well as analyses of assorted documents I was presented with, including internal reports, databases, and news stories. In short, I employed qualitative methods to find out how crime is rendered quantitative (Haggerty 1998).⁷

The article proceeds as follows. In the first section, I briefly explore the analytical tools available for assemblage-inspired research in critical technosecurity studies. Next, I unpack the assemblage of crime prediction in Rio, following the translations necessary to produce maps of future crime. I then examine controversies surrounding CrimeRadar, reconstructing the debates on imaginaries of insecurity and biased policing. Discussing the links between the visual representation of risk scores and discriminatory practices, I argue in the conclusion for the need to recalibrate critiques of predictive policing systems.

Security Assemblages: Unraveling Grand Narratives of Police Technologies

The widespread belief that algorithmic forecasting has the power to bring objectivity and justice to otherwise violent, ineffective police practices often resembles a “computational theocracy” (Bogost 2015), whereby investments in techno-fixes are guided more by faith in their effectiveness than by evidence-based analyses. However, critics of recent technological developments may also be blamed for exaggerating the impact of such systems, overlooking the variegated contexts in which they operate and “mythologizing the algorithm’s place as an all-powerful arbiter of social life” (Knox 2016). Lyon (2007: 147) has described the techno-determinism that characterizes both approaches as “sociological shallowness,” since they seem to believe that “the presence of high technology speaks for itself, somehow guaranteeing its own effectiveness.” Here, I propose that the concept of security assemblages affords an ecological view of the making of crime forecasts that may overcome the above limitations.

⁴ For a thorough analysis of the shift from after-the-fact, reactive policing to risk-based, pre-emptive security practices, see Ratcliffe 2016; Ferguson 2017b; Jefferson 2018; Shapiro 2019; Egbert and Krasmann 2019; Brayne 2020.

⁵ For valuable exceptions, see: Kaufmann 2019; Shapiro 2019; Benbouzid 2019.

⁶ Most interviewees and informal sources have been anonymized. I only identify Igarapé’s research director, who went public many times to talk about the app and public officials who would easily be identified anyway.

⁷ The access I had to scrutinize the making of the app and to talk to the Igarapé team was unusual. Other crime forecasting developers claim to be open about algorithms and even publish papers with results of randomized control trials (Mohler et al. 2015), but independent researchers still struggle to investigate their products (Lum and Isaac 2016). Conversely, Igarapé not only let me join meetings and interview programmers but also helped me to make contact with Rio’s crime statistics bureau and sent me all the documents I requested.

More than a theory, the literature on assemblages offers critical repertoires for addressing how power and knowledge are embedded in practices, norms, and discourses, as well as in objects and codes.⁸ It affords analytical tools to investigate how technological devices react back to the social, not only redistributing competencies and agency through a broader chain of actors but also inscribing negotiated values and interests in durable entities. As Latour (2004: 225) argues, societies need to outsource their regulating principles, politics, and morality to more solid materials: “it is when power is exerted through things that don’t sleep and associations that don’t break down that it can last longer and expand further.” As such, security assemblages are social accomplishments, or contingent products of institutional regimes and processes, and play important roles in practices of governance (Haggerty 1998). To say that crime forecasts are socially constructed means that, beyond speculating on their impact, sociological analysis should focus on how crime data are gathered, the techniques employed to validate them, and the algorithms used to identify patterns and future trends.

Assemblages have been conceived as “more than one, less than many” (Law 2002: 3), which impels us to “think in terms of movement, trajectories and becoming rather than the fixed and static, the separate and self-contained” (Basaran et al. 2017: 4). It means that parts, interactions, and wholes are not distinguished from one another but swirl into (or are embedded in) one another: “it is the relations between agents that permit us to understand their practices and what constitutes and transforms their identities” (Basaran et al. 2017: 4). For example, police officers, algorithms, and databases are part of a heterogeneous multitude that compose crime prediction systems. But they are not randomly scattered fragments; they hang together in particular shapes and are connected through specific sets of practices. Hence, they form what Law (2002: 3) calls a “fractional coherence,” or provisional “overlaps that produce singularity out of multiplicity.” As a result of these diverse and fragmentary coalitions, assemblages “are never simply a realization of a programme, strategy or intention: whilst the will to govern traverses them, they are not simply realizations of any simple will” (Rose 1999: 52). Thus, assemblage-thinking demands closely examining how the assorted elements that compose technological devices are organized, telling their history (how they were negotiated and achieved), and evincing the processes of translation through which standards, purposes, and functionalities were established (Amicelle, Aradau, and Jeandesboz 2015).

The act of *translation* is key, since it indicates the mechanisms through which hybrid elements connect to one another (Callon and Latour 1981). As we will see in the next section, crime predictions would have never been possible if algorithms were not fed data that were already streamlined, edited, and geolocated. For translations to happen (crime events into data and data into risk scores), actors draw on several *inscription devices* (instruments of measurement, representation, manipulation) that ascribe stable meanings and abstractable forms to previously unrelated *things* (Latour 2005; see Figure 1). Think of crime reports and how they let multiple security professionals access crime when the event has long passed. They create standard classifications for criminal activities, which can be gathered and analyzed by scholars or investigators. Thus, translations allow for larger assemblages to be formed, encompassing geographically and temporally distant entities.

Translations also imply relations of power and dominance: “intrigues, calculations, acts of persuasion and violence” (Callon and Latour 1981: 279). But unlike broad ideological disputes, these are often manifested in everyday controversies about design decisions and engineering solutions. Developers might disagree on what type of crimes should constitute the database used to train algorithms, influencing whether the software will yield results biased towards burglaries and thefts or homicides and aggressions. How to represent risks of victimization is also a seemingly unremarkable decision taken by programmers, but it is one that might influence security anxieties. Before CrimeRadar was launched, similar questions had to be answered by its developers: how do you compare burglaries, sexual assaults, and homicides? How do you deal with chronic

⁸ The incorporation of the conceptual lexicon of assemblages in surveillance and critical security studies is quite plural and draws from different theoretical inspirations. For analyses of the nuances of different approaches, including cross-fertilizations between actor-network theory and assemblage-inspired frameworks, see: Haggerty 1998; Müller 2015; Müller and Schurr 2016.

underreporting in different neighborhoods? These are all intrinsically political choices, which remain forgotten in techno-determinist approaches to policing innovations.

Following Haggerty (1998: 8), I argue that the “development of classifications of people, events and processes, ongoing political negotiations, standardization and rhetoric” are essential steps in the validation of truth about crimes, but the multiple choices involved in these practices are naturalized and de-politicized in the process of translating crime events into strings of codes, datasets, and maps. In other words, statistical officers and crime map designers accrue their influential role from their capacity to invest their work with epistemological qualities, and present crime predictions as eminently technical and politically agnostic. In this sense, attention to the everyday politics of data (Kitchin 2014)—the subtle ways in which different institutional interests are negotiated and struggles over who “owns” the data and who decides on modelling parameters are settled—is important to understand the app’s assumptions and consequences.

Figure 1: *CrimeRadar's translations and inscription devices.*

Assemblage-thinking calls on critical scholars to unpick the “banal” practices and concerns of security practitioners, exploring controversies, internal critiques, and failures. The focus on mundane decisions and frictions as a methodological orientation allows the analyst to disentangle the chain of security in multiple practices and avoid generalizations about modes of governance and counter-strategies. Rather than nebulous processes of domination and exploitation, assemblages enable an analytical approach that does not ratify or denounce but “seeks to think with professionals, using their own doubts, challenges, and hesitations as anchors of (public) critique” (de Goede 2018: 40). As such, it affords attention to the development of technological devices, including the paths there were not taken, the mistakes, surprises, multiple iterations, and choices, bringing a more nuanced explanation to the fragmentary dynamics that effectively build discriminatory apps and power asymmetries in general. Hence, this article lays bare the mechanisms by which security is framed and problematized, demonstrating the amount of work necessary for specific modes of security governance to take root. The next section aims at showing how seemingly unremarkable design decisions may have significant impacts on (in)security practices and perceptions.

The Crime Prediction Assemblage in Rio de Janeiro

Rio is often pictured as both a city of great natural beauty and of appalling social and racial inequalities, where violence is “embodied and experienced in everyday urban space” (Garmany 2011: 1161). This meant that organizing the 2016 Olympics was a particular security challenge, prompting massive investments in digital technologies to reduce the threat of crime and promote more efficient and accountable policing.⁹ As

⁹ Local authorities have invested in digital policing applications and acquired many devices aimed at improving situational awareness and crime-control capabilities, including acoustic sensors for automatic gunfire alerts, body cameras, crime-mapping

a result, Rio rapidly became a “real-life laboratory for the new field of ICTs for violence prevention” (Muggah and Diniz 2013: 15). CrimeRadar is one such techno-fix for public safety, claiming to render the future knowable to local citizens and tourists through the aggregation of data and the automation of encoded hypotheses regarding crime rates. The app was developed by Igarapé in partnership with the Montreal-based data engineering company Via Science and the state Institute of Public Security (Instituto de Segurança Pública, ISP).¹⁰ Unlike PredPol, HunchLab, and the technologies of other renowned companies that forecast crime to inform police patrols, CrimeRadar’s main objectives are “to promote transparency and open data [and] to close the gap between the perception of insecurity and its reality with a more informed conversation about insecurity” (Interview with Igarapé practitioner by the author, November 2017).

CrimeRadar was conceived to be intuitive and user-friendly, making use of the familiar Google Maps interface. Carving the urban area into 250 m² sectors, the app draws on more than five years of data—about fifteen million registered occurrences—to visually display the potential for new incidents in the subsequent six-hour period. Risk scores are summarized on a scale of 0 to 9 and grouped using a color-coded scheme ranging from green and yellow (lower probability) to orange and red (higher probability). It is also possible to search for addresses or zoom in on specific sectors, opening a bar at the bottom of the screen that displays assessed risks for selected areas at different times of the day and week (see Figure 2). Users can simply access the website (rio.crim radar.org) to find out the risk of victimization in their neighborhood or the safest route to a given destination. The whole process may take under a minute, but during this brief interaction a wide matrix of actors is invoked.

Crime prediction software is developed in three main phases: data collection and preparation, modelling, and mapping. Here I concentrate on a few steps to bring forth some of the design choices and the messiness and contingency inherent to the making of the app.

Unpacking Crime Forecasting: Police Reports, Crime Data, and Models

Crime predictions are extremely reliant on structured datasets, but where do these come from? How are the inputs feeding the algorithms constituted and converted into formats that can be read, stored, shared, and compared? Crime numbers are concomitantly the result of recording practices and a political instrument for concrete actions in society. On one hand, the data handled by CrimeRadar are contingent on the notation, computation, and calculation techniques employed by the police and statistical officers. In Rio, these practices are often carried out in a hostile epistemological context, with civil society and the media contesting the role of the police as disinterested data-loggers.¹¹ On the other hand, crime statistics and predictions are reliant on classificatory schemes that establish “the contours of the objects of governmental strategies, rendering them knowable and subject to political intervention” (Haggerty 1998: 45). Official classifications are often naturalized, but how we label people (suspects, victims, etc.) and events (homicides, burglaries, etc.) impacts our governmental rationality and the ways in which we experience crime.

software, onboard computers for patrols, drones, surveillance balloons, etc. For an overview of the security investments in preparation for the Olympics, see Edler Duarte 2019.

¹⁰ ISP is a statistical clearing-house responsible for organizing official crime numbers in the state of Rio. It has access to the datasets kept by the Civil Police and produces statistics and maps that are subsequently publicized, serving the managerial needs of the police. As such, ISP is an important “calculation hub,” where myriad statistical techniques are implemented to produce authoritative knowledge on crime dynamics, which becomes the object of government practices (Latour 2005).

¹¹ The accuracy of crime data in Brazil is contentious. Researchers and journalists claim that underreporting is rampant, so victimization surveys should be carried out more frequently, and that registering practices need closer scrutiny, since the quality of crime reports depends a lot on the proclivities of police authorities and the social status of both suspects and victims. The politicization of crime data is also a matter of concern, and the police are often accused of hiding or distorting information that makes them look bad (Miranda, Oliveira, and Paes 2010). Conversely, statistical officers often criticize the media and civil society organizations for mishandling public data and touting misleading depictions of violence in Rio (Monteiro and Caballero 2021).

Figure 2: CrimeRadar interface; screenshot by the author.

Police stations are state institutions with the power not only to collect and organize information on crime but also to enact crime in standard (indexable) forms. This is where matter gains digital form, or “where some of the materiality of [crimes] is sloughed off in favor of greater mobility of data” (Ribes and Jackson 2013: 161). Using multiple classification and representation technologies (criminal law, medical reports, forensic expertise), the police simplify the messiness of the world and make it amenable to analysis and control. When registering a homicide, for example, police officers translate blood, gunpowder, bullets, and witnesses’ accounts into a crime report, which is stored in police servers and archives. Thus, producing crime reports means isolating, interpreting, and translating discrete pieces of crime scenes back to police stations in ways that produce comparable categories (suspects, victims, weapons, place, time, etc.) and retain meaningful relationships to crime dynamics. Once reports are issued, they feed spreadsheets, where they begin to lose their qualitative character and become a quantitative inscription of crimes, which are finally available for authorized others to check and download. One of these is ISP.

The datasets retrieved from police servers are still “dirty”; reports often contain errors and are not ready to be made public. Before building the information that will be released, ISP cleans, redraws, and corrects the data. At the same time, it erases classified information and discards details rendered useless. At ISP, no one goes back to the evidence of every murder, much less restages violent encounters in order, for example, to design a representation of the upsurge of homicides. While drawing graphics and maps, the institute enrolls to the assemblage other instruments, such as mathematical formulas and statistical techniques, effectively enacting new ontologies of crime. Transformed into numbers, complex criminal dynamics are again simplified. Hence, when others look into crime trends, they do not see huge piles of paper or “dirty” datasets, but aggregated statistics, maps, and graphics. At this point, not much can be said about specific events, but a great deal can be understood from crime figures. What is left is a quantitative representation of crime that includes some features while excluding others.

Igarapé received the database containing pieces of information on every crime registered in Rio since January 2010. Yet when the programmers checked the files, they realized that most of the crimes listed were non-violent offenses (e.g., transporting voters who reside in rural areas), which did not relate to the purpose of the app. Thus, they decided to distribute the different types of crime in tiers according to their perceived harm: homicidal and violent acts, less-serious felonies, and “victimless” or nuisance crimes. After applying

its own categorization of crimes and filtering the dataset, Igarapé sent the new database to its partners at Via Science, who hired a geocoding service to map the data points.

However, the geocoding service could not attribute exact coordinates to many of the crimes. The reasons for this were multiple, including outdated cartographic references. However, the main problem, I was told, was the low quality of the crime reports, which, even after being edited by ISP, generated databases full of flaws. Mistakes are not always attributable to the authorities. When victims inform law enforcers of an incident, sometimes they do not know (or prefer not to say) precisely where it took place. In such a severely overstretched police force as the one serving Rio, it is virtually impossible to verify the exact location of every reported crime. Accordingly, when dealing with occurrences whose exact location is missing, most officers simply make up something (e.g., street A) or leave an empty space and move on to the next field. At ISP, I was told that this happens in about 35 percent of reports, but the actual number of idle data is larger than that, since the cartographic base does not always recognize the addresses, even when they are given correctly. As a result, between 50 and 60 percent of data points had to be ditched before being used for the modelling, which disproportionally affected poor and recently urbanized areas (Interview with ISP by the author, August 2017).

For CrimeRadar's architects and users, geocoding reveals crime clusters and assists in pattern-based analysis, indicating the spatial and geographical distribution of crime. But as the above description evinces, the Cartesian grid conceals the sociotechnical context in which databases are produced and overlooks the processes that compose a rather specific ontology of crime. CrimeRadar does not process information on crime events per se, but edited, recombined, and quantified bits that have been manipulated by multiple human and nonhuman actors in various sites for "crime" to be fit for consumption by the algorithms. It was only after traversing this convoluted route that batches of data finally reached the hands of Via Science's mathematicians, who used them to train and test different statistical models. Here, attempts to retrace the chain of translations get a bit troublesome. Via Science saw CrimeRadar as an opportunity to showcase its machine-learning engine and was not willing to fully disclose details, not even to its partners at Igarapé.

Many discussions were held between the developers about what parameters to use in the app, such as demographics, economics, and weather conditions. Analyzing the data and talking to local security professionals, both teams realized early on that specific events (Carnival, music festivals) impact crime dynamics. Likewise, they considered including variables for police operations and flare-ups of disputes between criminal factions, both of which cause significant, temporary spikes in micro-regions. The possibility of adding information on local terrain (schools, parks, bars) was also raised, but the tight project deadline and limited number of professionals soon forced the developers at both institutions to abandon more elaborate ideas. As I was told, "it would be possible to build a model with all the variables, including information on individuals, geography, income distribution, bus stops, [military] police battalions, and so on. Not only would this make a highly complex model, but the inclusion of each new variable would demand the reorganization of the whole thing. That's why we work with an approximation" (Interview with Igarapé practitioner by the author, May 2017).

As we can see, the developers of CrimeRadar struggled to find an optimal balance between the complexity of the models and their capacity to generalize the results. If very few parameters were included, the outputs would misrepresent the distribution patterns found in the training data, producing several biases. However, more elaborate models that accurately accounted for identified patterns in the past yielded high variance, which could handicap the algorithm's capacity to generalize and predict future data (a problem known as overfitting). The dilemma was summed up by one programmer in the following terms:

As for the artificial parameters, when you insert too many the model gets so volatile, so unpredictable, that you can have anything [as the output]. The idea is to find those that best represent variations and apply them. To the point that you can say, "now I've got a parameter that works sufficiently well for the city." Only then can I apply the model with confidence. (Interview with Igarapé practitioner by the author, May 2017)

Also, besides being easier to handle and explain, simpler models have two decisive advantages: lower computational costs and better data trafficking performance, which are paramount for a successful user experience.

In the face of time and resource constraints, both institutions decided to replicate the framework of other crime forecasting services and use only three data points: type of crime, location, and date/time. Sector adjustments were considered for seasonality and population density. Via Science then used its patented machine-learning engine to design models (purportedly thousands) and horse race them in simultaneous out-of-the-sample tests for each sector. The little information they provided on this phase indicates that they used a self-exciting point process (SEPP): a common clustering mechanism in which the occurrence of past points in a certain place and time makes its future occurrence in proximate sectors and periods more likely (see Figure 3) (Mohler et al. 2015). Thus, embedded in CrimeRadar's algorithms are certain assumptions deriving from environmental criminology and situational crime prevention, such as rational choice theory and near repeat hypothesis. From this perspective, criminals are seen as opportunistic individuals who choose their targets based on analyses of suitable victims, the vulnerability of the location (i.e., escape routes, number of targets, lack of police oversight), and their own experience (criminals tend to operate in their comfort zone; Bennett Moses and Chan 2018).

Figure 3: CrimeRadar's SEPP clustering rationale.

After adjusting the model, Muggah (qtd. in Capps 2016) celebrated CrimeRadar's achievements: "We have over an 85 percent accuracy of mirroring risk against actual events. The beauty of machine learning is that this improves over time.... The more data, the more information you feed into it, the higher-resolution your risk projections are going to be." The algorithms, however, proved to be rather recalcitrant. Data engineers at Via Science were often puzzled by the results obtained, and while they tried to tackle some of the setbacks, they were unable to address many others. There also were minor mistakes, such as incompatibilities between the georeferencing systems and a failure to account for daylight saving time, which meant that the locations and timings of the risk scores were discrepant. But even after these problems were ironed out, multiple discrepancies were still identified. Reflecting on this process, one of Igarapé's programmers told me:

The model isn't a perfect mirror of the data.... We have knowledge on the region, but when you apply the model you inevitably introduce distortions. The better the model is, the less [it happens], but we had to find a balance between the distortion and artificial parameters.... We tested the parameters until it got close to what we initially expected. The catch is that when we make it right in one area, it's possible that we're failing to notice an important distortion in other areas.... The model doesn't fit softly as a silk

tissue lying over the city. It looks more like a rough towel. When you put it [over the map], it goes down here but goes up somewhere else. Of course it must distort, or all you'll have is the raw data. (Interview with Igarapé practitioner by the author, May 2017)

As the programmer explains, there were uncertainties regarding what inputs had been used to develop the algorithm upon which the app was based, forcing programmers to create workarounds to compensate for them. The underlying function that fully explains crime dynamics in Rio is not known. Algorithms cannot predict every crime in every sector, but the better the parameters, the smaller the average error. The challenge is not to find one rule that perfectly fits the multiple variations in crime across town but the mathematical optimization that captures broad patterns in the datasets. The assumption is that, however complicated human behavior may be, there is a model (or a set of models) capable of deciphering it.

Essentially, the problem is not that the app simplifies multi-causal phenomena but that users are not fully aware of how future crime is enacted and what representations of risk actually imply. As usually happens with technological innovations, after the model was built and the crime map was designed, the intricate processes described above were erased. Igarapé still put some effort into explaining the app's analytical engine and data validation process,¹² but the theoretical debates on criminological assumptions, decisions about the thresholds of false positives and negatives, and the contingency and malleability of results have been black-boxed (Latour 2005). As Amoore (2019: 148–149) puts it, “though this arrangement of probabilities contains within it a multiplicity of doubts in the model, the algorithm nonetheless condenses this multiplicity to a single output... [which] is rendered as a decision placed beyond doubt; a risk score or target that is to be actioned.”

Once the app's designers had worked through and resolved the various issues, they were able to draw a clear line between the social and technical features and produce credible claims of neutrality. I was told that, unlike other mapping platforms designed for Rio, CrimeRadar operates with official data (supposedly, the best available), and although it might be biased, this is not down to the algorithm. The fact is that the police issue crime reports inconsistently across the city's landscape and CrimeRadar can only extrapolate from these data to map future trends. As a team member explained, the algorithm itself is powered by “concrete data, and its mathematics has no bias.... If a crime happened, the algorithm will see it, will read it without putting human values, and will make a prediction based on that. So, it's certainly impartial” (Interview with Igarapé practitioner by the author, April 2017). As we will see in the next section, the neglect of feedback loops—the algorithm reinforcing biased statistics—prompted criticisms from the police and civil society.

By briefly unpacking CrimeRadar's assemblage, I have sought to demonstrate in this section how political choices, institutional regimes of practices, and criminological assumptions are inscribed in algorithmic calculations of future crime. Crime itself was enacted according to the interests of those who designed the app. Programmers at Igarapé and Via Science could have chosen to attribute more weight to financial crime, for example, shedding light on white collar felonies. Or they could have featured only homicidal crimes, sexual violence, and cases of police abuse. To assume, then, that algorithms are flawless machines that objectively predict such a subjective category as crime is to miss the vast amount of editing work required to translate social features into computable form (Aradau and Blanke 2017). In other words, “it is to mistake maps for territories” (Seaver 2013: 9). Leaving these questions out of sight means ignoring the politics of translation, which, as we will see in the next section, has controversial consequences.

¹² The app was launched with a FAQ sheet and a brief explanation of the algorithm. After a while, the Igarapé team decided to improve the information available to users and even published a policy report debating the pros and cons of crime prediction (Aguirre, Badran, and Muggah 2019).

The Politics of Predictive Algorithms

Understanding the sociotechnical composition of CrimeRadar has important implications for how we access the pressing debates regarding security governance. Multiple studies have shown that when algorithmic calculations become responsible for flagging certain areas and people as potentially violent, it is easier to avoid the ethical dilemmas raised by targeted policing and rephrase disputes around discretionary security practices in terms of efficiency and productivity, effectively hiding the social implications of datafying, coding, and representing crime (Harcourt 2007; Ferguson 2017b). The underlying punitivism of situational crime reduction strategies is reinforced by algorithmic forecasts that claim to be better than human analysts at picking risky sectors (Fry 2018; Siegel 2018).

In this sense, the proponents of predictive policing are said to ignore decades of research on racialized police operations (and records) (Scannell 2018; Benjamin 2019; Brayne 2020). As Jefferson (2018: 2) puts it, “official crime datasets shape predictive crime mapping and... the maps reciprocally legitimize those datasets through their ostensibly scientific presentation.” Thus, they tend to validate discriminatory practices of control, inducing unreasonable fear of poor communities and concentrating police enforcement efforts against marginalized populations. However, an analysis of CrimeRadar’s composition brings some nuances to such assumptions. Perhaps surprisingly, while critics assumed the app would reproduce results observed in other predictive software, the forecasts did not emphasize the risks of navigating through Rio’s poor neighborhoods.

A few days after CrimeRadar was launched, the first dissenting voices started to be heard. Writing for RioOnWatch, a news website aimed at bringing visibility to favela communities, Natalie Southwick (2016) raised concerns about the potential for prejudice to be inherently reproduced by its algorithms:

The source—and extent—of the data being used is a potential cause for concern. While Igarapé’s app uses the most complete set of available official information... police officers are known for tampering with crime scenes or mischaracterize crimes in their official reports, often to cover up human rights abuses. This unreliability of official data, and the simultaneous criminalization of certain neighbourhoods and communities, is exactly what has given rise to citizen-driven apps... which allow citizens to report incidents and violations by the police in their communities.

There was also backlash against CrimeRadar among social movements. Fransérgio Goulart (2016), a local activist, claimed that Igarapé’s turn to predictive algorithms was evidence that “the criminalization of the favelas comes from all sides.” Fórum da Juventude, a group of activists from the favelas and suburbs, also denounced the app as an attempt to stigmatize the urban poor: “Igarapé Institute has just created an app that will deepen the criminalization of favela dwellers. That’s why our discourse is #UsforUs” (NósporNós 2016). Further commenting on the app’s impact, Matt Moffett (2016) emphasized the dilemmas embedded in it: “Can you warn people about risky areas without stigmatizing those neighborhoods, potentially hurting businesses and denting property values? It’s a question that’s set to become more pressing everywhere... but it’s an especially tricky one in Rio, already deeply polarized between haves and have-nots.”

CrimeRadar did produce contentious results in traditionally marginalized spaces, but not in the way Moffett, Goulart, or Southwick expected. As a retired police officer who assisted in designing the app explained, “Rio has dangerous areas, hot areas, with underreporting. You won’t see high indicators for street robberies in favelas. When you carry out a predictive analysis, you must consider these particularities. They [Igarapé and Via Science] wanted me to give specific information on different sites so they could better configure the algorithm, but I said it was too complicated” (Interview with police officer by the author, September 2017). In other words, the crime forecasts for Rio do not highlight poor neighborhoods, where crime is said

to cluster, but the opposite. In the initial map iterations, most of the favelas were colored light green, while affluent neighborhoods came out as crime-ridden areas.¹³

The Igarapé team identified underreporting early on, but it was not clear how best to deal with it. When the initial map iterations began to indicate no hot spots in favelas, debates were held about how to proceed. One of the developers told me that she was an advocate for either removing risk scores from favelas or even redesigning the algorithm to produce more credible results: “crime predictions are complicated and the first were pretty wrong. Ipanema [a rich beachside neighborhood] was more dangerous than Costa Barros [a favela in the north zone].... It simply wasn’t ready. It produced errors and more errors” (Interview with Igarapé practitioner by the author, August 2017). Others felt that there were enough data on favelas to produce accurate predictions and that the unexpected results would raise interesting questions on the perception of crime and the irrational fear of these neighborhoods. Interestingly, they proposed exploring the epistemological authority of maps and algorithms to question common sense views on crime and risk. Some also pondered that removing such areas could further distort the predictions and alienate multiple urban sectors in the map (indicating the non-existence of data, as in forests and water bodies).

In the end, the developers opted not to attribute risk scores to favelas. As Muggah (2016b) explained: “large favelas... are effectively dominated by gangs and experience episodic violence, often at a very high level of intensity. [But] the data gathered from these areas is often unreliable and subject to high levels of volatility.” Commenting on this topic, Via Science’s CEO also lamented the need to erase favelas from the map, but blamed the datasets while rephrasing the well-known adage among computer scientists: garbage in, garbage out: “While we would like to fill in current data gaps—such as the favelas—our ability to do so depends on improvements to the quality of data collection and reporting” (qtd. in Griffiths 2016).

Figure 4: The Favelas Complexo do Alemão and Maré (in gray) and Surrounding Areas (<https://rio.crimeradard.org/>); screenshot by the author.

While the removal of favelas from the app (see Figure 4) raised serious concerns about effectively erasing large portions of the urban landscape, it also failed to appease critics, as doubts regarding the app’s accuracy were still raised. Joana Monteiro, ISP’s former president, for example, was clear about her position:

¹³ Discrepancies in crime reporting across social groups are not found just in Rio. For similar processes in the US, see Benbouzid (2016) and Shapiro (2017).

CrimeRadar isn't working. It's as simple as that. To understand why, you must stop, scrutinize the project, recheck the models and what they're producing. It's a very complex thing.... But they did the first iteration, threw it [online], and said "this is what we could come up with".... It shouldn't be online. They should be reviewing the models. I think it's a great idea, the platform is beautiful, but you're sending out the wrong information. (Interview with Joana Monteiro, former president of ISP, by the author, September 2017)

The results are so controversial that during an interview, a professional at ISP told me wryly that CrimeRadar is at best "crime speculation" and would need several improvements before it could have any real value. He told me that ISP had already tried predictive algorithms but had abandoned the idea when it realized how hard it was to achieve good results. In his opinion, the parameters used should be complemented by time-dependent variables (weather, seasons, events, holidays, recent police operations) and opportunity variables (population density, escape routes, bars). When I asked him to evaluate the app, he told me, "Honestly, it doesn't picture the reality, not even close. It's not the problem of CrimeRadar. None of the systems I've seen could depict reality.... The simple fact of whether it's raining or not already affects the dynamic of crime. If you don't have this information in the algorithm, you're lost" (Interview with ISP practitioner by the author, October 2017).

During an interview, Muggah agreed that some critiques are not ill-founded, but when I questioned him on matters of accuracy, he endorsed the app and shared part of the responsibility with ISP. For him, CrimeRadar performed satisfactorily in the tests ran by Via Science. Liabilities, then, were not to be found in the algorithms, but in the low-quality data provided as an input:

A lot of the algorithm's power derives from the quality of the data that are provided. There are going to be assumptions about how crime data are reported, but the assumptions in CrimeRadar are exactly the same as those reported in existing real-time crime mapping.... That applies to any police department, to a greater or lesser degree. So, unfortunately, it is the case that people from Barra and Ipanema and Leblon are probably reporting more frequently across a wider range of crimes than people in other areas. There's no way to adjust for that, unless you decide not to use the data. Now, you can make that call: "because the data is inherently biased, I've decided not to use it." Or you can say, "let's be clear about these biases. Let's make a point that there are limitations to the information".... There are a lot of caveats, but at the end of the day we're probably more honest than most people when it comes to reporting on crime. So, I accept the criticism, but I also say: it's systemic and it's the nature of the underlying biases and errors in reporting on crime. (Interview with Robert Muggah, Director of Igarapé, by the author, November 2017).

Echoing Muggah's viewpoint, private developers and security practitioners often share the belief that algorithmic bias could be corrected through the collection of more reliable data. They acknowledge that police departments may mess with crime reports, that many entry points are lost while inscribing criminal events in datasets, and, to a certain extent, that crime statistics are flawed (Aguirre, Badran, and Muggah 2019). But, as the previous section shows, such appeals overlook the fact that crime is, in principle, a messy social phenomenon and that crime data have never been objective. In other words, crime rates do not relate to crime per se; they are indicators of multiple police organizational processes. This is especially true in Rio, where even data on homicides, allegedly the best available, have been questioned due to uncertainties regarding missing people and challenges in defining causes of death in cases of suicide or when decomposed corpses are found (Araújo 2016).

Also, it is often the case that heavily surveilled populations generate reams of data, while others are less scrutinized and have multiple resources at their disposal to evade the justice system. In Rio, historical circumstances linked to the dominance of organized crime in poor neighborhoods and fear of violent

reactions by the police have condemned favela-dwellers to be reported more often as perpetrators of crime than victims. Witnesses in favelas are often frightened of being identified as police informants, and victims decline to report crimes due to the negative consequences of contacting the authorities, or else they choose other (extrajudicial) methods to handle the situation (Penglase 2014). In this sense, however much favelas may be seen as the epitome of dangerous places in security imaginaries, they do not produce enough inputs to be identified by CrimeRadar's algorithms as high-risk areas. Accuracy, then, is not just a matter of investing in technical capabilities to build better datasets, but understanding the dynamics of local violence and the multiple political decisions underlying the way policing is done in the first place.

As we have seen, multiple translations end up embedding political issues in techno-scientific terms, concealing conflicts over social norms, algorithmic bias, and injustice. Pre-crime systems claim to simplify the complicated dynamics of criminal activity into seemingly straightforward inscriptions (hotspots), producing scientific knowledge on society and rendering crime more manageable and predictable. However, CrimeRadar does not merely organize information that is available out there or simply discover patterns and correlations or produce knowledge from dispersed information; it actively assembles certain profiles and relations to the detriment of others. To produce the information consumed by the public, violent encounters are codified in criminal law, datafied, transported through multiple public and private institutions, and treated by different sorts of actors before they are finally plotted on a map that can be accessed via any device connected to the internet. At every stage, new classifications of crime or new ways of seeing and presenting risks of victimization are produced, all of which influence the way we experience and act upon (in)security.

Ultimately, CrimeRadar produces ideas of crime and acts upon the places and times with which the data are associated, informing users where to go, when to go, and how to behave. The app's representations contribute towards new forms of public consciousness of urban violence, portraying the landscape and crime events as visual cartographies of targeted territories, and potentially transforming the calculation of risk into a primary way in which spaces, populations, and subjects are constituted.

Conclusion

The aim of this paper was twofold. On one hand, it demonstrated how crime forecasting stems from multiple socio-material entanglements and cannot therefore be "tech-washed" as impartial or objective. Not only are uneven quantities of data gathered across different social groups and urban areas, but programmers also have to make decisions and address ethical dilemmas while developing the app. Most importantly, by tracing the chain of political decisions back to seemingly banal procedures, I demonstrated that security is not simply governed at the moment of surveillance, at the site of police raids, or during encounters between police officers and suspects; rather, police practices result from the frictions and controversies inherent to the making of sociotechnical assemblages (Bourne, Johnson, and Lisle 2015). On the other hand, I also argued that critics should remain skeptical about the implications of new security technologies. Instead of rushing to conclusions and assuming that such systems contribute to the over-policing of marginalized populations, we should explore their composition. Detailed descriptions of the symbiotic relationships between data, algorithms, and humans must be pieced together before an understanding can be reached of how (in)security practices are produced in the everyday. Of course, this does not mean that there is no such thing as discrimination by design. The decision to erase crime predictions in local favelas, for example, was informed by questionable conceptions about criminogenic spaces. My point is not that claims of stigmatization and racism are unfounded but that detailed examinations of technologies-in-the-making may uncover different discriminatory practices and effects. Instead of making favela-dwellers more visible to the eyes of the state and thus more governable, CrimeRadar has erased Rio's poor areas, which is also indicative of its target audience.

Lyon (2003: 150) claims that rather than being subject to fully fledged strategies of containment, people and territories are increasingly categorized as "safe" or "risky" through routine procedures of classification and semi-autonomous devices that enable "fresh forms of exclusion that not only cut off certain targeted

groups from social participation but do so in subtle ways that are sometimes scarcely visible.” The challenge for critical surveillance and security studies, then, is to trace the associations and translations that enable such scarcely visible mechanisms of power and violence. Viewing crime forecasts as emerging ontologies of vibrant gatherings demands us to recalibrate our analyses of modes of order from overarching structures to observing the silent politics that allow assemblages to be forged and maintained. More importantly, it brings to the fore the “small violences” perpetrated by state and private actors long before suspects are imprisoned and shots are fired.

Finally, this approach directs our attention to how crime and violence are made (un)knowable and how controversies and contestations are rendered (in)visible in the making of digital policing devices. Once we grasp the ordinary practices of “othering” and boundary-drawing ingrained in crime forecasts, we may have a better understanding of *how* such tools induce security anxieties and *how* they authorize practices of control against specific groups. Perhaps, we may even produce insights about how to build more effective spaces of contestation.

Acknowledgments

I wish to thank Claudia Aradau, Jef Huysmans, and Brian Balmer for their comments on previous versions of this article. I also thank the blinded referees for their constructive comments.

Funding

This work was supported by São Paulo Research Foundation (FAPESP) [Grant No. 2020/05628-1] and CAPES/Pró-Defesa [Grant No. 88887.368551/2019-00].

References

- Aas, Katja, Helene Gundhus, and Heidi Lomell, eds. 2009. *Technologies of InSecurity: The Surveillance of Everyday Life*. Abingdon, UK: Routledge-Cavendish.
- Aguirre, Katherine, Emile Badran, and Robert Muggah. 2019. *Future Crime: Assessing Twenty First Century Crime Prediction*. Strategic Note 33. Rio de Janeiro, BR: Igarapé Institute.
- Akrich, Madeleine. 1992. The De-Description of Technical Objects. In *Shaping Technology/Building Society: Studies in Sociotechnical Change*, edited by Wiebe Bijker and John Law, 205–224. Cambridge, MA: MIT Press.
- Amicelle, Anthony, Claudia Aradau, and Julien Jeandesboz. 2015. Questioning Security Devices: Performativity, Resistance, Politics. *Security Dialogue* 46 (4): 293–306.
- Amoore, Louise. 2019. Doubt and the Algorithm: On the Partial Accounts of Machine Learning. *Theory, Culture & Society* 36 (6): 147–169.
- Aradau, Claudia, and Tobias Blanke. 2017. Politics of Prediction: Security and the Time/Space of Governmentality in the Age of Big Data. *European Journal of Social Theory* 20 (3): 373–391.
- Araújo, Fábio. 2016. “Não tem corpo, não tem crime”: notas socioantropológicas sobre o ato de fazer desaparecer corpos. *Horizontes Antropológicos* 46: 37–64.
- Basaran, Tugba, Didier Bigo, Emmanuel-Pierre Guittet, and R. B. J. Walker, eds. 2017. *International Political Sociology: Transversal Lines*. London: Routledge.
- Beck, Charlie, and Colleen McCue. 2009. Predictive Policing: What Can We Learn from Wal-Mart and Amazon about Fighting Crime in a Recession? *The Police Chief* 26 (11): 18–25.
- Benbouzid, Bilel. 2016. Who Benefits from Crime? Books and Ideas, October 31. <https://booksandideas.net/Who-Benefits-from-the-Crime.html> [accessed June 19, 2019].
- . 2019. To Predict and to Manage: Predictive Policing in the United States. *Big Data & Society* (January): 1–13. <https://doi.org/10.1177/2053951719861703>.
- Benjamin, Ruha. 2019. *Race After Technology: Abolitionist Tools for the New Jim Code*. Cambridge, UK: Polity Press.
- Bennett Moses, Lyria, and Janet Chan. 2018. Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability. *Policing and Society* 28 (7): 806–822.
- Bogost, Ian. 2015. The Cathedral of Computation: We’re Not Living in an Algorithmic Culture So Much as a Computational Theocracy. *The Atlantic*, January 15. <https://www.theatlantic.com/technology/archive/2015/01/the-cathedral-of-computation/384300/> [accessed June 19 2019].
- Bourne, Mike, Heather Johnson, and Debbie Lisle. 2015. Laboratizing the Border: The Production, Translation and Anticipation of Security Technologies. *Security Dialogue* 46 (4): 307–325.

- Bratton, William, and Sean Malinowski. 2008. Police Performance Management in Practice: Taking COMPSTAT to the Next Level. *Policing: A Journal of Policy and Practice* 2 (3): 259–265.
- Brayne, Sarah. 2020. *Predict and Surveil: Data, Discretion, and the Future of Policing*. Oxford, UK: Oxford University Press.
- Callon, Michel, and Bruno Latour. 1981. Unscrewing the Big Leviathan: How Actors Macro-Structure Reality and How Sociologists Help Them to Do So. In *Advances in Social Theory and Methodology: Toward an Integration of Micro- and Macro-Sociologies*, edited by Karin Knorr-Cetina and Aaron Cicourel, 277–303. London: Routledge.
- Capps, Kriston. 2016. Mapping “Pre-Crime” in Rio. *CityLab*, August 19. <http://www.citylab.com/crime/2016/08/mapping-pre-crime-in-rio/496553/> [accessed September 10, 2016].
- de Goede, Marieke. 2018. The Chain of Security. *Review of International Studies* 44 (1): 24–42.
- Deflem, Mathieu. 1997. Surveillance and Criminal Statistics: Historical Foundations of Governmentality. *Studies in Law, Politics and Society* 17: 149–184.
- Edler Duarte, Daniel. 2019. *Reassembling Security Technologies: Police Practices and Innovations in Rio de Janeiro*. PhD Dissertation, Department of War Studies, King’s College London.
- Egbert, Simon, and Susanne Krasmann. 2019. Predictive Policing: Not Yet, but Soon Preemptive? *Policing and Society* 30 (8): 905–919.
- Ferguson, Andrew. 2017a. Policing Predictive Policing. *Washington University Law Review* 94 (5): 1113–1195.
- . 2017b. *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: New York University Press.
- Fry, Hannah. 2018. *Hello World: How to Be Human in the Age of the Machine*. New York: W.W. Norton and Company.
- Garmany, Jeff. 2011. Drugs, Violence, and Death: The Necro- and Narco-Geographies of Contemporary Urban Space. *Urban Geography* 32 (8): 1148–1166.
- Goulart, Fransergio. 2016. A criminalização das favelas vem por todos os lados!. Facebook, August 24. https://www.facebook.com/fransergiogoulart/posts/10154489216039801?_tn=-Ru [accessed November 27, 2018].
- Griffiths, Sarah. 2016. CrimeRadar is Using Machine Learning to Predict Crime in Rio. *Wired*, August 18. <http://www.wired.co.uk/article/crimeradar-rio-app-predict-crime> [accessed on June 19, 2019].
- Haggerty, Kevin. 1998. *Making Crime Count: A Study of the Institutional Production of Criminal Justice Statistics*. PhD Dissertation, Department of Anthropology and Sociology, The University of British Columbia.
- Harcourt, Bernard. 2007. *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age*. Chicago, IL: The University of Chicago Press.
- Jefferson, Brian. 2018. Predictable Policing: Predictive Crime Mapping and Geographies of Policing and Race. *Annals of the American Association of Geographers* 108 (1): 1–16.
- Kaufmann, Mareile. 2019. Who Connects the Dots? Agents and Agency in Predictive Policing. In *Technology and Agency in International Relations*, edited by Marijn Hoijtink and Matthias Leese, 141–163. London: Routledge.
- Kaufmann, Mareile, Simon Egbert, and Matthias Leese. 2019. Predictive Policing and the Politics of Patterns. *British Journal of Criminology* 59 (3): 674–692.
- Kitchin, Rob. 2014. Big Data, New Epistemologies and Paradigm Shifts. *Big Data & Society* 1 (1): 1–12.
- Knox, Jeremy. 2016. Algorithms. *New Materialism*, September 19. <https://newmaterialism.eu/almanac/a/algorithms.html> [accessed June 19, 2019].
- Lash, Scott. 2007. Power after Hegemony: Cultural Studies in Mutation? *Theory, Culture & Society* 24 (3): 55–78.
- Latour, Bruno. 2004. Nonhumans. In *Patterned Ground: Entanglements of Nature and Culture*, edited by Stephan Harris, Steve Pile, and Nigel Thrift, 224–227. London: Reaktion.
- . 2005. *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford, UK: Oxford University Press.
- Law, John. 2002. *Aircraft Stories: Decentering the Object in Technoscience*. Durham, NC: Duke University Press.
- Leese, Matthias. 2014. The New Profiling: Algorithms, Black Boxes, and the Failure of Anti-Discriminatory Safe-Guards in the European Union. *Security Dialogue* 45 (5): 494–511.
- Lum, Kristian, and William Isaac. 2016. To Predict and Serve? *Significance* 13 (5): 14–19.
- Lupton, Deborah. 2016. *The Quantified Self*. Cambridge, UK: Polity Press.
- Lyon, David. 2003. *Surveillance after September 11*. Cambridge, UK: Polity.
- . 2007. *Surveillance Studies: An Overview*. Cambridge, UK: Polity.
- Miranda, Ana Paula, Marcella Oliveira, and Vivian Paes. 2010. A reinvenção da “cartorialização”: análise do trabalho policial em registros de ocorrência e inquéritos policiais em “Delegacias Legais” referentes a homicídios dolosos na cidade do Rio de Janeiro. *Segurança, Justiça e Cidadania* 2 (4): 119–152.
- Moffett, Matt. 2016. Waze Can Now Warn You about High-Crime Neighborhoods in Cities. But Is That a Good Idea? *Quartz*, August 23. <https://qz.com/764036/waze-can-now-warn-you-about-high-crime-neighborhoods-in-cities-but-is-that-a-good-idea/> [accessed June 7, 2019].
- Mohler, George, Martin B. Short, Sean Malinowski, Mark Johnson, George E. Tita, Andrea L. Bertozzi, and P. Jeffrey Brantingham. 2015. Randomized Controlled Field Trials of Predictive Policing. *Journal of American Statistical Association* 110 (512): 1399–1411.
- Monteiro, Joana, and Barbara Caballero. 2021. Crimes e Violência. In *Guia Brasileiro de Análise de Dados: Armadilhas e Soluções*, edited by Claudio Shikida, Leonardo Monasterio, and Pedro Nery, 127–167. Brasília, BR: Enap.
- Muggah, Robert. 2016a. Does Predictive Policing Work? *The Cipher Brief*, December 4. <https://www.thecipherbrief.com/article/tech/does-predictive-policing-work-1092> [accessed June 7, 2019].
- . 2016b. Big Math Spotlight: Robert Muggah. *Via Science*, March 11. <http://www.viascience.com/big-math-spotlight-robert-muggah/> [accessed July 13, 2017].

- . 2017 What Happens When We Can Predict Crimes before They Happen? *World Economic Forum*, February 2. <https://www.weforum.org/agenda/2017/02/what-happens-when-we-can-predict-crimes-before-they-happen/> [accessed February 7, 2017].
- Muggah, Robert, and Gustavo Diniz. 2013. Digitally Enhanced Violence Prevention in the Americas. *Stability: International Journal of Security & Development* 2 (3): 1–23.
- Müller, Martin. 2015. Assemblages and Actor-networks: Rethinking Socio-material Power, Politics and Space. *Geography Compass* 9 (1): 27–41.
- Müller, Martin, and Carolin Schurr. 2016. Assemblage Thinking and Actor-Network Theory: Conjunctions, Disjunctions, Cross-Fertilisations. *Transactions* 41 (3): 217–229.
- NósporNós. 2016. Instituto Igarapé cria aplicativo que vem ampliar a criminalização. Facebook, August 24. https://www.facebook.com/appfjrj/posts/955743197884649?_tn=H-R [accessed November 27, 2018].
- Palidda, Salvatore. 2010. Revolution in Police Affairs. In *Conflict, Security and the Reshaping of Society: The Civilization of War*, edited by Alessandro Dal Lago and Salvatore Palidda, 118–128. London: Routledge.
- Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.
- Penglase, Ben. 2014. *Living with Insecurity in a Brazilian Favela: Urban Violence and Daily Life*. New Brunswick, NJ: Rutgers University Press.
- Perry, Walter, Brian McInnis, Carter Price, Susan Smith, and John Hollywood. 2013. *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Washington, D.C.: Rand Corporation.
- Ratcliffe, Jerry. 2016. *Intelligence-Led Policing*. 2nd ed. London: Routledge.
- Ribes, David, and Steven Jackson. 2013. Data Bite Man: The Work of Sustaining a Long-Term Study. In “Raw Data” Is an *Oxymoron*, edited by Lisa Gitelman, 147–166. Cambridge, MA: MIT Press.
- Robinson, David, and Logan Koepke. 2016. *Stuck in a Pattern: Early Evidence on “Predictive Policing” and Civil Rights*. Washington, D.C.: Upturn.
- Rose, Nikolas. 1999. *Powers of Freedom: Reframing Political Thought*. Cambridge, UK: Cambridge University Press.
- Rouvroy, Antoinette, and Thomas Berns. 2013. Algorithmic Governmentality and Prospects of Emancipation: Disparateness as a Precondition for Individuation through Relationships? *Réseaux* 177 (1): 163–196.
- Scannell, R. Joshua. 2018. *Electric Light: Automating the Carceral State During the Quantification of Everything*. PhD Dissertation, Graduate Faculty in Sociology, The City University of New York.
- Seaver, Nick. 2013. Knowing Algorithms. Paper presented at *Media in Transition 8, Cambridge, MA, April 2013*. <http://nickseaver.net/papers/seaverMIT8.pdf> [accessed July 15, 2020].
- Shapiro, Aaron. 2017. Reform Predictive Policing. *Nature* 541 (26): 458–460.
- . 2019. Predictive Policing for Reform? Indeterminacy and Intervention in Big Data Policing. *Surveillance & Society* 17 (3/4): 456–472.
- Siegel, Eric. 2018. How to Fight Bias with Predictive Policing. *Scientific American* (blog), February 19. <https://blogs.scientificamerican.com/voices/how-to-fight-bias-with-predictive-policing/> [accessed July 15, 2020].
- Southwick, Nathalie. 2016. The Importance and Challenges of Putting Favelas on the Map. *RioOnWatch*, October 11. <http://www.rioonwatch.org/?p=32519> [accessed November 18, 2019].
- Suchman, Lucy. 2020. Algorithmic Warfare and the Reinvention of Accuracy. *Critical Studies on Security* 8 (2): 175–187.
- Tett, Gillian. 2014. Mapping Crime – or Stirring Hate? *Financial Times*, August 22. <https://www.ft.com/content/200bebee-28b9-11e4-8bda-00144feabdc0> [accessed June 19, 2019].
- Wacquant, Loïc. 2009. *Punishing the Poor: The Neoliberal Government of Social Insecurity*. Durham, NC: Duke University Press.
- Ziewitz, Malte. 2016. Governing Algorithms: Myth, Mess, and Methods. *Science, Technology, & Human Values* 41 (1): 3–16.