Big data surveillance across fields: Algorithmic governance for policing & regulation

Anthony Amicelle

Original Research Article

BIG DATA & SOCIETY

Big Data & Society
July–December: 1–12

DOI: 10.1177/20539517221112431
journals.sagepub.com/home/bds
SAGE

Big data surveillance across fields: Algorithmic governance for policing & regulation

Anthony Amicelle[1]

Abstract

While the academic separation of policing and regulation is still largely operative, points of convergence are more significant than ever in the digital age, starting with concomitant debates about algorithms as a new figure of power. From the policing of illegal activities to the regulation of legal ones, the algorithmization of such critical social ordering practices has been the subject of growing attention. These burgeoning discussions are focused on one common element: big data surveillance. In accordance with such similarities and paralleled developments in policing and regulation, the article aims to further bridge the gap between literatures to respond to the calls for studying big data surveillance across institutional domains and social fields. To do so, it is focused on one case study that articulates algorithmic policing and regulation domains, in-between security and economic fields. This is the fight against illicit finance, i.e. 'the global action against the financial flows that fuel crime and terrorism'. To what extent does big data surveillance make a difference in the main global policy of crime-fighting and financial regulation? Drawing on a fieldwork in a large North American bank, the present article takes stock of the algorithmic overlap between policing and regulation. It argues that the final result is policing and regulation of neither too much nor too little, which gives rise to automated and everyday mass surveillance while remaining as far removed from regulatory and crime-fighting ambitions as it is from dystopian visions of big data and algorithmic drama.

Keywords

Big data surveillance, algorithmic regulation, policing, security, finance, money laundering

Introduction

> *The literatures regarding policing and regulation are largely separate, reflecting the common assumption that there is some essential distinction between the activities*. (Gill, 2002: 523)

> [This] *calls for systematic research on the relationship between the goals, means, and ends of big data surveillance across institutional domains*. (Brayne, 2017: 1003)

While the academic separation of policing and regulation is still operative, points of convergence are more significant than ever in the digital age, starting with concomitant debates about algorithms as a new figure of power. Indeed, the algorithmic governance for both policing and regulation is increasingly discussed "as a form of social ordering that relies on coordination between actors, is based on rules and incorporates particularly complex computer based epistemic procedures" (Katzenbach and Ulbricht, 2019: 2). From the policing of illegal activities to the regulation of legal ones, the algorithmization of such critical social ordering practices has thus been the subject of growing attention. These burgeoning discussions are notably focused on one common element of policing and regulation: surveillance and the related rise of big data.

On the one hand, as a specific aspect of social control, policing refers to "the creation of systems of surveillance with the threat of sanctions for discovered deviance – either immediately or by initiating penal processes" (Reiner, 2010: 5). Within the multifaceted transformation of contemporary policing and security, the rise of

[1]Sciences Po Bordeaux, Centre Emile Durkheim, Pessac, France

Corresponding author:
Anthony Amicelle, Sciences Po Bordeaux, Centre Emile Durkheim, 11 allée Ausone, Pessac 33600, France.
Email: a.amicelle@sciencespobordeaux.fr

algorithms and big data analytics is a contrasted but transversal trend (Amoore and Raley, 2017), from police patrols (Benbouzid, 2019) to penal courts (Brayne and Christin, 2021), criminal intelligence and (trans)national security units (Bigo and Bonelli, 2019; Chan and Bennett Moses, 2017; Lyon, 2014). In the light of predictive machines developed in police, justice and intelligence, the holy grail of big data is often associated with the capacity of surveillance systems to create a new regime of anticipation of events (Aradau and Blanke, 2017; Christin, 2017; Kaufmann et al., 2019). Prediction is presented as the predominant operational principle of security intervention within and over society, and the ambiguous notion of big data is then used to emphasize "the crossing of a threshold of data quantity, complexity, and proliferation speed, beyond which we have no choice but to automate and speed up (in order to cope with the constant and ultra-rapid increase in volumes of data) the processes for transforming digital data into operational information" (Rouvroy, 2016: 10). For instance, the fast treatment of vast amounts of commercial, transactional and communication data to monitor people and things in motion for security purposes is increasingly enacted through computational algorithmic devices (de Goede, 2018), with "technologies of data processing and techniques of analysis that take some kind of input rendered in a machine-readable format, and generate human-readable ouput" (Bellanova et al., 2021: 129). As a critical modality of surveillance, the role of big data and algorithms is therefore investigated regarding its implications on policing practices as such, as well as on issues of efficiency, social sorting, discrimination, and the democratic governance of security (Brayne, 2017; Ferguson, 2017; Lyon and Murakami Wood, 2021; Shapiro, 2019).

On the other hand, the concept of algorithmic regulation has gained traction to characterize a new mode of coordination and control to produce social ordering, mainly in the field of economy (Andrews et al., 2017; Yeung, 2017; Yeung and Lodge, 2019). It refers to "decision-making systems that regulate a domain of activity in order to manage risk or alter behaviour through continual computational generation of knowledge by systemically collecting data (in real time on a continuous basis) emitted directly from numerous dynamic components pertaining to the regulated environment in order to identify and, if necessary, automatically refine (or prompt refinement of) the system's operations to attain a pre-specified goal" (Yeung, 2017: 6). Regulation relies on three components to seek compliance in legal markets: standard setting, supervision and enforcement (Gilad, 2007). In other words, any regulatory system articulates "the promulgation of targeted rules, typically accompanied by some authoritative mechanism for monitoring and enforcing compliance" (Woll, 2007: 813). The emergence of algorithmic regulatory governance is connected with the second component, surveillance. The aim is to complement if not supplement human oversight with big data surveillance devices to direct or at least inform decision-making to regulate behavior (Ulbricht and Yeung, 2022). As a result, algorithm-driven governance is expected to make a difference in the creation of new regulatory environments "where deviation from given standards and objectives can be detected and corrected in a way that has never been possible before" (Bellanova and de Goede, 2022: 104). Although detection of violations may be performed on a reactive basis, after their occurrence, there is also a move towards pre-emptive ambition on the basis of correlations within massive data sets (Yeung, 2017). Here too, regulation by and through algorithms is interrogated in terms of its justification, formalization, transformative potential, ultimate effectiveness, ordering effects, unexpected consequences and related degree of transparency and legal accountability (Burk, 2019; Eyert et al., 2022; Hildebrandt, 2018; Johns and Compton, 2022).

In accordance with such similarities and paralleled developments in policing and regulation, the article aims to further bridge the gap between literatures to respond to the calls for studying big data surveillance across institutional domains and social fields. To do so, it is focused on one case study that articulates algorithmic policing and regulation domains, in-between security and economic fields. This is the fight against illicit finance, i.e. "the global action against the financial flows that fuel crime and terrorism" (FATF, 2021). Over the last 30 years, the social fact of crime-related financial flows has been converted into an object of concern, public debate and global policy, involving "regulators, law enforcement and the private sector" across the world (FATF, 2019: 42; Nance, 2018). This has been reflected in the creation of an international organization (the Financial Action Task Force/FATF), new crimes (money laundering and terrorist financing), and new standards for the regulated financial system, "with more than 200 countries and jurisdictions committed to implementing them" (FATF, 2022). This transnational regulation – understood as "the organization and control of economic […] activities by means of making, implementing, monitoring, and enforcing of rules" (Benoît and Thiemann, 2021) – has led to the mandatory compliance of financial actors with unprecedented policing obligations. Indeed, the solemn appeal to follow the money has given birth to *financial policing*, that is the creation of systems of financial surveillance, coupled with the threat of sanctions for dirty money-related crimes. As a generic organizational imperative, surveillance is unsurprisingly at the heart of this original configuration of policing and regulation, with the articulation of differentiated universes of practices and rationalities, from economic and financial fields on the one hand, to penal and security fields on the other. To what extent does big data surveillance make a difference in the main global policy of crime-fighting and financial regulation?

Anti-money laundering and countering the financing of terrorism (AML/CFT) policy depends on the everyday surveillance of financial transactions that is operated by non-police, for-profit institutions, starting with banks (Helgesson and Mörth, 2019). They are at the frontline to deter any illicit use of the financial system and reporting information "to prevent, detect and disrupt money laundering, terrorist financing and the financing of proliferation weapons of mass destruction" (FATF, 2019: 25). From several employees to thousands are assigned to surveillance operation on a full-time basis depending on financial institutions. And "if a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions" (FATF, 2022: 19). In this context, big data surveillance programs have become commonplace across the banking industry over the last decade to monitor flows of money and detect suspicious ones. Moreover, this policing-related surveillance by algorithms is coupled with a form of regulation through and of algorithms. Banks' compliance with AML/CFT standards is increasingly monitored via the audit of such algorithm-driven automated detection of suspicious activity. This is especially true in North America, starting with Canada where federal authorities have imposed the so-called "compliance for intelligence and intelligence for enforcement approach" (Fintrac, 2014, 2017). It means that compliance is first and foremost monitored through the quality control of reporting practices based on big data surveillance. In other words, financial institutions are simultaneously agents of algorithmic policing and targets of algorithmic regulation. At the interface of economy and security, big data surveillance programs both appear as new policing and regulatory actants, as "boundary objects (Star and Griesemer, 1989) that make heterogeneous groups of actors cooperate and whose modalities of use differ according to the social worlds in which they circulate" (Méadel and Sire, 2017: 27).

Drawing on a fieldwork in a large North American bank, the present article takes stock of this algorithmic overlap between policing and regulation. It argues that the final result is policing and regulation of neither too much nor too little, which gives rise to automated and everyday mass surveillance while remaining as far removed from regulatory and crime-fighting ambitions as it is from dystopian visions of big data and algorithmic drama. Along these lines, the article is organized in five sections. The first section provides insights about my conceptual lens, fieldwork and qualitative research methodology. The second section sheds critical light on the social construction of the 'need' for big data surveillance as the imposition – and appropriation – of heteronomous principles within a specific field. The third part examines the transformative logic of new algorithmic device on surveillance systems. The fourth part relates to instrumentation as such, that is the set of problems posed by the choice of instruments (algorithms, methods of operation and so on) that allow surveillance and, by extension, policing and regulation to be made material and operational on a daily basis. The final part concentrates on the entry into service of the algorithmic device, focusing on its connection with a broader data infrastructure, embodying fields connections between security and economy.

Studying algorithmic devices *in situ*

Literatures on algorithmic regulation, policing and security all converge on the necessity "to examine algorithmic devices in situ," while recognizing that most studies fail to analyze such contexts of reception (Amoore and Piotukh, 2016: 3; Brayne and Christin, 2021; Ulbricht and Yeung, 2022). These algorithmic-like concepts direct empirical attention towards what Ulbricht and Yeung (ibid.: 14) define as "the ways in which computational systems are intentionally designed, configured, and implemented by those seeking to deploy them to further a particular social purpose, while helping to bring into view their multifarious and often hidden and/or unintended social and other impacts for individuals, groups, and society more generally." From organizational sociology to infrastructural perspectives (Bellanova and de Goede, 2022; Christin, 2017), the analytical focus on algorithmic devices within wider social, legal and technical contexts leads me to another concept, i.e. appropriation, understood as the "dynamic process of dialogue and reflection between an object and a space of activities producing usages either routinized or innovative" (Amicelle et al., 2015: 301). Studying a big data surveillance program in-the-making has required close attention to the process of appropriation of algorithms within a pre-existing IT infrastructure in the broader context of power relationships between different actors, multiscale institutional domains and fields, all crystallized during several months in one building of one organization in one country.

In Canada, 31,000 entities are legally bound by surveillance and reporting obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. Annually, they all together submit nearly 500,000 suspicious transaction reports and up to 30 million reports based on monetary thresholds to the dedicated federal authority – Fintrac – that is both an intelligence and a regulatory agency (Fintrac, 2021). Fintrac's related intelligence products are then disseminated for policing and security purposes to law enforcement and intelligence agencies. In this context, banks are by far the largest reporting entities as the source of over 85 percent of denunciations (Fintrac, 2016), with six domestic systemic banks, 22 other domestic banks, 24 foreign bank subsidiaries and 29 foreign bank branches (Department of Finance Canada, 2015).

My empirical material is precisely based on one significant financial institution, in which I followed during one year the implementation of a big data surveillance program for AML/CFT. This fieldwork mainly consisted in semi-structured interviews, ethnographic observations and the consultation of internal documents. Twenty professionals were interviewed among the nearly ninety people involved in the program deployment, from the director of bank's AML/CFT department as such (which went from a few employees to several hundred within a decade) to the IT manager, business analysts, programmer-analysts and the ultimate users. Each of them was selected for their representative role in the division of labor regarding the choice and deployment of the algorithmic device. All interviews were recorded with the participants' agreement and they last on average 60 minutes. The reliability of information was controlled via complementary strategies. Interviewees were systematically brought back to the description of specific steps and routine actions, starting with their evolving tasks and everyday work (Becker, 1998). Each new interview was cross-checked with the others and with ad hoc interviews in other banks in Canada to deal with any factual errors or cover-up attempts whilst having an overview of practices and related-social representations in the bank and across the banking industry (Pinson and Sala, 2007). Moreover, they were complemented by ethnographic observations, both on-site, in one building with most of the project teams at work, and on-line with weekly meetings between the main team leaders and managers. These on-line meetings were highly important for me to the extent that they were organized at the beginning of each week to provide updates on the progress of the project and reviewing the work objectives for the next days. Finally, I have accessed to internal documents about the project expectations, its timeline and the presentation of algorithms. The triangulation of information sources has allowed me to study the making of big data surveillance in all its complexity.

The need for big data surveillance

> In the era of 'big data', automated surveillance in our field has become inevitable. Although technology may never be able to completely replace humans when it comes to fighting the bad guys, the volume of information financial institutions need to process in order to do so, makes it impossible to 'follow the money' and identify criminals without automated surveillance systems. (ACAMS, 2018: 23)

Such a statement now goes without saying in the banking industry. It illustrates as much as it promotes the deployment of algorithmic devices at the heart of AML/CFT. It was made by a Canadian representative of the Association of Certified Anti-Money Laundering Specialists (ACAMS), operating in 175 countries. As in many other domains, the reference to big data is meant to emphasize the magnitude of digital traces generated by human activities. In this instance, data relate to financial transactions, whose aggregate volume can easily reach and exceed hundreds of millions per month for a bank with several million customers. This goes hand in hand with the development of big data analytics, with the promise of taking action on a series of phenomena and trends that would be difficult to grasp in any other way. Nevertheless, contrary to other policing and regulatory configurations, the predictive rhetoric exists but it is quite limited to terrorist financing (Bellanova and de Goede, 2022). The stated aim is rather to acquire "suspicion machines" (Amicelle and Grondin, 2021), as suspicion is clearly the predominant operational principle of proactive intervention within and over society via suspicious activity reporting. With this in mind, it is worth looking further into how the need to acquire such 'machines' is justified.

Many of the reasons given for justifying algorithmic devices overlap with the ones identified in other domains. This is the case with the quote at the top of the section, namely the need to deal with a considerable amount of information as a result of datafication. Recalling the "avalanche of printed numbers" in the early 19th century (Hacking, 2015), the current deluge of digital data would call for new instrumentation (Eyert et al., 2022). However, this practical necessity is itself the result of a regulatory one. Indeed, more stringent legal obligations against money laundering and terrorist financing has led to a series of changes in financial institutions. In this context, the director of the bank's dedicated internal department sums up the situation straight away: "The key point is accreditation. Since 2008, the legal regime has evolved in Canada. There have been reforms in certain areas, including what is known as continuous client monitoring in financial institutions. And the volume is far too great to do it with the human eye as was done until recently. So having an automated system is not a regulatory requirement, but you have a large volume, you can't do the job. And when we say continuous monitoring, the important thing is to make it clear that every business relationship, 100% of it, has to be monitored. […] We have [X] million individual customers, plus the professional profiles of companies, so let's say [X] million profiles. Then [X] million transactions per month. Then I tell you that you have to be sure to identify potential criminals and their obvious transactional. Your brain stops right there and says it's impossible to do it with the human eye. Still, we explored the idea, do I not sign up with [the technology vendor] and ask the frontline employees to improve all the manual and human controls already in place to meet the goal and get to the same level of surveillance. Imagine looking at [X] million transactions, [X] million profiles including corporate profiles, [X] million in all, it's impossible. Plus a human, no two humans look at it the same way" (interview 7, 2018). The

inevitability of big data surveillance was not simply because of the volume of data available, but also because of the regulatory requirement to process them for the purpose of total and continuous surveillance in the name of policing and security. Starting from this initial reason, the need for big data surveillance has imposed itself over any other alternative based on a twofold justification that is well known in the literature.

First of all, the "information argument" or efficiency argument is the one that has been put forward the most forcefully (Brayne and Christin, 2021; Christin, 2017: 3). According to the head of the bank's surveillance project, there is "a matter of efficiency because even if there were no budgetary limits and 3000 employees could come to work tomorrow morning, even then you can't do effective monitoring, even with an unlimited number of staff, because there are patterns of money laundering that cannot be detected by the human eye. So it's not just a question of compliance with the law, it's also a question of budgetary and operational efficiency" (interview 1, 2018). Along these lines, automated surveillance and detection systems would outperform human analysts, both in terms of gaining access to an unparalleled amount of data and making good use of it, and to do so within a shorter timeframe and at a lower cost.

This quest to optimize time and resources is all the more crucial for the representatives of an internal department who may seem to be "double agents" (Lenglet, 2012), paid by the bank but working for the security state. While the goal is to adapt quickly to legal and regulatory changes, they seek to do so by legitimizing their approach and their position within their organization. In the preparatory documents for the program, it is pointed out that "the anti-money laundering operations department is typically viewed as a cost center and it is important to monitor, justify and allocate those costs appropriately" (internal document 1: 14).

Secondly, the idea of operational efficiency and budgetary optimization has been compounded by the argument of objectivity and moral neutrality (Christin, 2017). The head of the team in charge of the automated suspicion alerts argues that "before the implementation [of the program], the anti-money laundering department was limited to the directors with their vision of what was a criminal, of what was an offence. Everyone comes with their own values and morals and every crime, every situation could be handled according to these different values. For example, some people thought that selling drugs was more problematic than other things. Well, at the time it was illegal [selling cannabis] but even today some people may find it punishable. So maybe cannabis production or massage parlors or dancers or stuff like is not morally acceptable but it doesn't reflect a suspicion of money laundering and we're here to make money, so you have to focus on what you really need to catch and disengage a little bit from morals and values. And with the rules [algorithms] you don't have a choice anymore, you follow everything that has been harmonized. […] That's what's been done with the advent of these technologies, to rely on industry-defined criteria, like money laundering patterns or money laundering risks, so something other than popular beliefs or stuff like that" (interview 6, 2018). This neutrality argument – based on algorithms that would be free from human exaggeration and uncontrolled discriminatory bias – was shared across the banking industry more broadly, as shown by the interviews in other banks.

Arguments of efficiency, optimization and objectivity have contributed to reinforce and rationalize a posteriori the need to invest in a 'suspicion machine' that was first thought of as a way to buy regulatory compliance. As major reporters, banks are regularly audited by regulators, with the potential for administrative and criminal sanctions and negative publicity in case they are found to be non-compliant. Criminal prosecutions are rare or even non-existent in Canada and fines are relatively low (a few million euros at the high end), but the reputational impact and economic consequences can be significant. As emphasized by one of the co-directors of the bank's AML/CFT department, "correspondent banks fill out risk assessment forms with one another: 'Do you have a compliance program, do you have a chief compliance officer, do you deal with this type of customer, etc.?' There's a lot of circulation between financial institutions, so we require the same thing that others require of us, everybody's watching each other. […] We have correspondent banking relationships in the United States, they are constantly watching us. We have people working full time here to deal with [a major U.S. bank], to assure them that we have what it is needed in place. They check and when you are in a business relationship with them they don't tolerate you dealing with activities that are prohibited or very risky in their country, otherwise the business relationship could end" (interview 1, 2018). In this respect, to be a good business partner means to be recognized as a proper policing institution. Regarding this – transnational – dynamic of "emulation" within the banking industry (Benoît, 2018), the director of the internal department says that they would have "probably done it anyway [without regulatory change]. But would we have done as much? Would we have created a team of [X] people, would we have spent so many millions over so many years if there wasn't a regulatory requirement and the possibility of a significant penalty? The answer is no. But would it have been zero? The answer is also no. Probably it would have been somewhere in between. Very difficult to say because it's a hypothetical situation. Because this is a regulatory requirement! And you have to respect it" (interview 7, 2018). With these conditions governing the need for algorithmic devices in mind, the next step is to look at the transformative logic of this new instrumentation.

From one surveillance to another?

How to make everyday mass financial surveillance possible at an unprecedented scale? It is the question that was posed within the bank under study, with the answer being algorithmic devices. Indeed, regarding surveillance as such, pre-algorithmic systems were both discontinuous and targeted.

On the one hand, surveillance was over-the-counter, limited to individuals showing up at branches and interacting with their bank advisors. All bank employees are required to be made aware of dirty money issues through in-house training. They are encouraged to be 'vigilant' and report unusual transactions to their colleagues from the AML/CFT department. During my fieldwork, there were an average of 40 alerts per week across the bank's branches.

On the other hand, this direct, face-to-face surveillance was rounded out by surveillance at a distance, with an exclusive focus on high-risk clients. This leads to the risk scoring of every bank account holder. It is based on a series of criteria such as professional occupation or elected position, sector of activity, the distance of your home or business from the bank branch, country of residence, activities or interests abroad, links with 'high risk' countries and individuals, types of accounts, financial products and services used, criminal record or connection with any suspicious transaction report in the past (Fintrac, 2017).

A dozen criteria were used in the bank to calculate each client's score on a risk scale. Risk scoring is synonym of what Sarah Brayne coined as "stratified surveillance: differentially surveilling individuals according to their risk score" (2017: 989). A high risk score implies deep surveillance, with individualized, manual reviews of financial activities at regular intervals. As such, fewer than 1% of clients were at high risk in the bank.

Moreover, face-to-face surveillance and surveillance at a distance refers to specific, differentiated approaches on suspicion. In the case of face-to-face surveillance, the initial suspicion formally depends on people's attitude on site, whether they behave more or less 'normally' in social interaction. "Potential red flags" are provided for this purpose by the dedicated federal authority (Fintrac), such as: "Client exhibits nervous behaviour; Client has a defensive stance to questioning; Client exhibits a lack of concern about higher than normal transaction costs or fees" (Fintrac, 2019). Various contextual elements can be added. For instance, far from the latin saying pecunia non olet, depositing "musty, odd smelling or extremely dirty bills" is considered to be "outside the normal conduct of [banks'] business" (ibid.). In my fieldwork, cash deposits that literally smelled of cannabis were categorized as a potential indicator of drug trafficking, especially if customers themselves smelled 'suspicious'. In the case of surveillance at a distance of the less than 1% high risk customers, the initial suspicion formally depends on people's transactional behavior in the light of their "financial profile" and other specific patterns (Fintrac, 2019). In this respect, the official "potential red flags" cover dozens of examples such as : "The transactional activity (level or volume) is inconsistent with the client's apparent financial standing, their usual pattern of activities or occupational information (e.g. student, unemployed, social assistance, etc.); Large and/or rapid movement of funds not commensurate with the client's financial profile; There is a sudden change in the client's financial profile, pattern of activity or transactions; Frequent and/or atypical transfers between the client's products and accounts for no apparent reason; Transaction is unnecessarily complex for its stated purpose; Immediately after transferred funds have cleared, the client moves funds, to another account or to another person or entity; Transactions involving any countries deemed high risk or non-cooperative by the Financial Action Task Force" (ibid.). Here, surveillance is operated manually by dedicated agents scrutinizing risky clients' accounts and transactions over a given period of time.

The logic of algorithmic surveillance differs in almost every way from these two logics of surveillance and suspicion that predate it and with which it now coexists. A preparatory document indicated that "by implementing a transaction monitoring solution, the goal is to cease most of this manual work and to consistently monitor all of our clients across the portfolio, not just those that are considered 'at risk'" (internal document 1). Along these lines, two main changes set this new surveillance apart. Firstly, it is a dramatic scaling up of existing surveillance with the ambition to monitor everyone, million clients daily, whether or not they show up, whether or not they have a high risk score. Secondly, it is the advent of transactional dataveillance since only transactional metrics and relations initially matter (Ruppert, 2012), without any other form of knowledge of the people. Transactional data take precedence over socio-demographic and historical data since an alert can be generated without the need to relate to "the person/entity profile" (Fintrac, 2019). That therefore gives rise to everyday, systematic, automated mass surveillance system in order to flag activities and people for denunciation. As in most cases of algorithmic policing and regulation, it is designed as a recommender system for human operators whose responsibility is to provide additional scrutiny on the basis of automated alerts before making any final decision (Bellanova and de Goede, 2022; Brayne, 2017; Katzenbach and Ulbricht, 2019). The fact remains that the move to big data analytics and automated alert-based assistance represents a major transformation in how surveillance and suspicion is performed. So what does the instrumentation designed to make unprecedented surveillance possible in the name of global crime-fighting and financial regulation policy look like ?

Algorithms under constraints of simplicity

> Little more than a set of step-by-step instructions that set out some conditions and consequences, these rules seemed far removed from the drama of artificial intelligence, big data and the opaque and inscrutable algorithm. (Neyland, 2019: 132)

The first finding – and empirical surprise – is the gap between my field research and the growing academic literature on algorithms in relation to policing, security and regulation. The latter and my own expectations about the complexity, opacity, and agency associated with new algorithms as a figure of power were largely challenged.[1] Beyond the primarily theoretical grounded nature of a significant part of studies, this gap is telling about the concrete articulation of differentiated universes of practices and rationalities around big data surveillance.

First of all, the expected complexity gives way to the relative simplicity of the algorithmic 'solution'. Like the other studied banks, the so-called big data surveillance program is made up of about 20 rules, in the form of IF/THEN conditions and actions regarding predefined transactional scenarios. In the light of the abandoned luggage algorithm ethnographed by Neyland (2019), each algorithm refers to specified, step-by-step sequences of operations, structured by initial conditions (IF questions) leading to consequences (THEN rules). "At its simplest, the 'IF' acts as a condition and the 'THEN' acts as a consequence" (ibid., 32). For example, IF a customer deposits or tranfers more than X thousands of dollars within X days, THEN an alert will be automatically generated.

There is nonetheless a distinction between "primary rules" and non-primary rules (internal document 4). The former are one-size-fits-all transactional rules, such as transferring specific amount of money from/to high-risk countries and/or high-risk institutions. By contrast, the latter refer to transactional metrics that can be fine-tuned with additional criteria. This involves, in particular, criteria to "segment" the population under surveillance (Yeung, 2017), at least between individuals and companies, and between companies according to their size and turnover. In this way, monetary thresholds for triggering an alert for the rule of cash deposit vary. A weekly deposit of several tens of thousands of dollars is expected from a company of a certain size, not from an individual. In addition, the rule is weighted according to risk scoring, with a lower monetary threshold for clients with a high score. In this case, a very high-risk individual would only need to deposit X thousands of dollars to trigger an alert, while a low-risk client could deposit more than twice that amount in the same time frame before triggering an alert based on the same transaction rule. With each rule setting a number of points that must be reached to automatically trigger an alert, high-risk customers have a head start. Beyond the customer risk score, a point value is assigned to various elements for each non-primary rule depending on certain scales, clients or population groups, such as the number of accounts and their 'age', the number of occurrences, the period of recurrence, the type of transactions, the existence of previous alerts, etc. In addition, the rule 'learns' to some extent. If human analysis shows that one or more alerts against a customer are unproductive, the number of points to be reached is increased.[2] Notwithstanding these different settings options, the program remains relatively rudimentary and perfectly intelligible, which is in part constrained and in part chosen.

According to the implementation project manager in the bank, such algorithmic device can be used to detect "all the transactional part of the indicators provided by Fintrac, but if you have the data. Because sometimes you don't have the data. For example, one of the indicators for money laundering, or rather for terrorist financing, is someone who buys an airline ticket and then empties his account, etc. Do you imagine how many things are needed to detect this patternIt requires a center that detects airline ticket purchases, a center that can detect that your [account] balance is at zero. It requires a combination of rules and it's complicated. It's not impossible, it's just that we already have difficulty modeling cash withdrawals and transfers between unrelated accounts because of the quality of the data available. […] Another example, for the credit card service, we asked to have a detection model, a rule, for human trafficking [related to prostitution] because it is one of the important issues in Canada and Fintrac puts a lot of emphasis on it. But it's complicated. You're going to have to watch for single credit card purchases to pay for multiple hotel rooms in a day, for group meals at fast food restaurants, etc. There are a bunch of indicators that Fintrac provides and they are good indicators, but being able to do something with them is going to require rules, it's going to require checking the banking part at the same time as looking at the credit cards, it's going to require a lot of business rules to be able to issue alerts to detect patterns like that. We can't afford to do that for every money laundering or terrorist financing risk. This one, me and [the director], is very important to us because we are talking about something, human trafficking, which is a major social problem, with lives behind it. So we want to focus on it and we would like to have a rule for that. But if it's going to cost us three million dollars and hiring 40 people, we can't afford to do that" (interview 1, 2018). This not only shows that morality and values are not disappearing with big data surveillance, especially for algorithms selection. It also includes key elements that were encountered throughout my fieldwork.

First of all, bank's IT infrastructure and related digital data are determined by their primary purpose, which is to provide a financial service. Secondary use for security and crime control purposes invariably comes up against

this original raison d'être, as the coding – sometimes quite old – was not designed for such function creep. And while some respondents expressed the idea of changing the central IT systems, they did so as wishful thinking, if not as a joke. The IT manager insists that they have "not gone back to the source because changing codes in the central systems is very, very expensive, and to make such a change you have to evaluate all the impacts and there you immediately begin with several million dollars just by starting to think about it and to go into these systems, with cascading impacts on all the satellite systems" (interview 4, 2018). As another respondent, co-leader of the automated alert analysis team, summed up wryly, "in general, the banking system and banking technology systems were not created to combat money laundering" (interview 6, 2018). From this perspective, the automation of surveillance is a socio-technical illustration of the structural difficulties involved in connecting finance and security fields for policing purposes. These difficulties are here infrastructural and, although not insurmountable, they require heavy investments by capitalist organizations for whom policing is neither their core business nor a source of profit. While budgetary constraints weigh on any public and private security agency, they are all the more significant for an internal department of a financial institution, which by definition occupies a subordinate position. These technical and budgetary constraints partly explain the simplicity of the algorithmic device.

However, in the light of those "constraints of simplicity" (Vayre, 2018: 85), instrumentation choices are also reinforced by the willingness to ensure algorithmic readability, comprehensibility and accountability in the face of regulatory authorities. One of the preparatory documents about the objectives of the program indicates that they revolve around a single, higher goal: "satisfying regulatory needs" (internal document 3). It emphasizes the importance to "create an environment and/or reporting that is readily available and easy to understand by the regulators. […] Not all examiners are familiar with the details of how solutions of this nature work. Examiners expect that financial institutions are able to show their work in a quick and clean approach. If they are unable to do so, there is a high potential for additional regulatory scrutiny and potential for uneeded findings" (internal document 3). This need for intelligibility and transparency does not fit well with the opacity of 'black boxes' whose precise functioning and calculations would be beyond the grasp of their users, or even their developers. Documenting everything, understanding everything in order to be able to explain and justify everything in front of the regulator was the mantra repeated over and over again for months. The relative simplicity of the selected algorithms was a resource rather than a constraint in this respect. The situation under study refers to a case of human-machine relation in which the algorithm tends to be treated as an "object" to be controlled, reduced to "'if-then' commands with predefined instructions or sets of actions" (Lange et al., 2019: 607). While the idea of mastering the algorithmic object did indeed accompany the entire automation project of surveillance, this does not mean that it went smoothly.

Policing and regulation of neither too much nor too little

> If one of the major concerns with algorithms is their opacity, then being able to look at our […] algorithm would be a step forward. However, as I have also tried to suggest thus far in this book, looking at a set of IF-THEN rules is insuffcient on its own to render an algorithm accountable. Algorithms combine with system architectures, hardware components, software/code, people, spaces, experimental protocols, results, tinkering and an array of other entities through which they take shape. (Neyland, 2019: 45–46; 49–50)

The big data surveillance program is a local and technical translation of a national legislation implementing a global policy in-between crime-fighting and financial regulation. It is also transnational, with a Canadian bank, an American technology vendor and a European technology integrator in charge of planning and supporting the implementation of automated surveillance. Furthermore, connecting the social control-oriented algorithmic device with the finance-oriented IT infrastructure mobilized nearly ninety people, some sixty men and twenty women over several months, including a project leader, a project manager, an administrative assistant, a writer, a technician, an agile coach (for the project supervision process), a database administrator, an infrastructure/information technology consultant, an infrastructure delivery manager, two designers, two business experts, two change management consultants, two detailed architecture consultants, two solution architecture consultants, three general architecture consultants, three development consultants, four business analysts, four application delivery managers, a dozen functional analysts, a quality assurance coordinator, and nearly 20 programmer-analysts from several different internal departments. Their mission was to ensure technically the fields connections at the heart of financial policing and regulation. Although an exhaustive analysis of the problems they faced is beyond the scope of this article, it is important to pay attention to the perspectives of those who (re)configure such a computational connection on the ground. It means looking back at some of the main points of tension they had to deal with and which illustrate the state of power relations at play.

In accordance with the history of the fight against illicit finance, the fundamental challenge was to bring together the different parties involved, in order to ensure that the

surveillance device could 'understand' the financial data infrastructure. One of the preparatory documents states that "[the device] requires that all data be mapped to a centralized database. […] [The bank] receives around numerous transactions daily from [X] different systems. Each system has its own set of transcodes used to identify the type of transaction. These transactions need to be unique and mapped to specific buckets within [the device] so that [the device] to utilize those transactions in their monitoring. […] If transactions are incorrectly mapped or missed, it may result in inaccurate alerting" (internal document). The first task carried out by the professionals involved was therefore to "understand the data in the system" (interview 4, 2018), that is, to identify and map all the computer codes related to each type of financial transaction in order to be able to translate them into a language adapted to the surveillance device. As in other domains of regulation, policing and security, this "translational work" is critical to render the world under surveillance and, by extension, fields connections computable (Bellanova et al., 2021; Ulbricht and Yeung, 2022). In this regard, one of the interviewees, a business analyst, summarizes the general feeling in the following terms, indicating that "it's a lot of work, it took a lot of time because you want to make sure at the end of the day that everything has been mapped. Because each [surveillance and detection] rule really works with a type of transaction [ATM withdrawal, deposit, domestic transfer, international transfer, debit, credit, etc.], but it has to be properly transcribed and the transaction has to be the right one, it has to be relevant to the rule. And there you have all kinds of errors with reversed codes, or codes that shouldn't be there, or codes that are questionable, stuff like that, and you have to make the matches. So yes, we go into each of the transactions, we have the details in [the device] and we make sure that the transaction matches the source. And we found mapping problems" (interview 3, 2018). This quote sheds light on the invisible and hard work that makes big data surveillance operations possible, starting with non-'seamless' data structuring and data integration as a sine qua non condition for algorithmic processing (Bellanova and de Goede, 2022; Brayne, 2017). The translation process was more generally one of "transcoding" a public policy in the literal – computer – sense of the term, with the "grouping and transferring of information into a different code. Transcoding consists in aggregating scattered information and practices, as well as constructing and presenting them as a totality; and finally transferring them to other registers pertaining to different logics in order to ensure their dissemination within a social field and outside it" (Lascoumes, 1996: 334–335). The operationalization of this requirement to understand, connect and adjust data and devices belonging to different domains and fields has run into many difficulties, highlighting the divergent rationales, practices, and interests at play.

When mapping financial codes (several hundred) and sub-codes (more than a thousand), respondents were faced with coding errors at every stage, as the same code may have been assigned to different types of transactions to reduce costs inherent to adding more codes to the central systems. They also dealt with a degree of informational precision that, although designed for the financial field, is far from optimal for policing and security. The codes tend to group together generic types of transactions that refer to different behaviors, operations and scenarios for the algorithmic device of surveillance. Moreover, the sub-codes used to differentiate them have been poorly documented to the extent that this level of knowledge was not necessary for the proper conduct of financial business. While this lack of documentation was partially addressed throughout the implementation process, interviewees had to contend with a fragmented IT architecture. "We realized, as we tested and delivered [the device] and then appropriating the data, that one of our problems is the consistency of the information. The information is bound to be somewhere, except that it flips from one system to another. And from one system to another there is information that is cut off. For example, let's take theoretical numbers, let's say there are 100 fields [rows of data] available on the customer and his transaction. System A has 50 of those fields and system B has 50 of those fields. But that switches to a system C that takes 25 from one and 25 from the other. And we [in the anti-money laundering department], in order to be able to look up that data, we have to go to the authoritative sources. So if we go to system C, we only have 50% of the data, not 100. And sometimes we might have needed data from system A or B. Then we unfortunately have to do a lot of data enrichment exercises in the project to be able to retrieve certain information. But the additional level of difficulty was that there was no unique reference key to be sure that the data we needed belonged to that transaction. So rules had to be put in place to determine the degree of probability that this additional data belonged to this transaction. So the level of certainty with which we will work for the enrichment of certain transactions is not always 100%. […] In short, we have problems with codes that group too many things together and we also have problems with transactions that are completed with information that may not be 100% accurate" (interview 1, 2018). Lastly, technical difficulties and architectural constraints are exacerbated by banking practices. Many tellers and financial advisors enter transaction codes manually – out of ignorance, habit, or for simplicity and speed – that do not necessarily correspond to the types of operations their customers requested. While this is without consequence for the clients, the impact on surveillance is immediate, with the massive production of false positives and false negatives. This is a broader illustration of the tensions if not contradictions of goals that are being pursued simultaneously. As summed up by one of

the interviewees, "we're always trying to make the customer experience easier, simpler, and we'd also like to make the process faster with as few questions as possible. But all of this goes against what we need with money laundering, which is to collect as much information about customers as possible to be able to track them and then understand their patterns of transactions, their habits" (interview 5, 2018).

All these accumulated difficulties and tensions were acutely felt during the real-life testing of the algorithmic rules, with a daily production of alerts that appeared at first to be unmanageable. Based on projections for comparable institutions, the team expected a few hundred alerts per day, when in fact thousands were triggered. While the team was aiming for an average false-positive rate of 80–85% per rule, the rate of "non-productive alerts," was well over 95% and close to 100% for some rules. There then followed a sustained period of experimentation and 're-calibration' of the algorithmic rules as part of an longstanding exercise of trial and error, in particular by tweaking the weightings and thresholds for triggering alerts, to reach the desired number. In addition to data quality issues as well as transcoding and interfacing processes, the result of this constant tinkering also depends on power relations, both on the financial side and the security side in-between policing and regulation. On the security side, with the federal financial intelligence unit, discussions focused on the possibility of raising the monetary thresholds associated with certain rules in order to reduce the volume of alerts. As one respondent summarized, "the proposal to Fintrac was to say look at the effort I'm putting into monitoring these transactions for small drug dealers who have $100s, wouldn't it be better to take our people [analysts] and have them work on alerts for big cases. But because we've reported on small amounts in the past, Fintrac doesn't want us to stop. […] They don't want us to stop, so we have to 'sell' them on it" (interview 3, 2018). On the financial side, discussions focused on the budgetary resources allocated to alert processing. Once the approximate number of analysts assigned to this new task had been determined by the senior executives of the bank, the next step was – backward – to "really make sure that we have the proper number of alerts so that it can fit into the process with the resources in place" (interview 3). This double power relationship structured the algorithmic surveillance in the making and it reveals the tension balance in which the internal department finds itself, that of doing enough to satisfy policing and regulatory expectations, but not too much to satisfy financial, business considerations. Neither too much nor too little seems to sum up thirty years of global policy at the interface of finance and security, with or without algorithms.

Conclusion

> Hence, every algorithmic system constitutes a highly contextualized vehicle to achieve complex organizational goals. (Bellanova et al., 2021: 138)

If big data surveillance is becoming routine organizational practices in a wide range of life domains, this is especially true for social control purposes, from the policing of illegal activities to the regulation of legal ones. It is no coincidence that both literatures on policing and regulation have paid exponential attention to the conjunction of big data and algorithmic devices for surveillance over the very last years. Surveillance is the pillar of both kinds of social ordering practices for detecting deviance from specific norms, whether it be for enforcing criminal law or regulatory compliance. Following a rather classic path in social sciences, the production of knowledge about big data-driven forms of surveillance has mainly started with theoretical if not speculative works before articulating conceptual perspectives with original and extensive fieldwork research. More recently, the logic of knowledge accumulation has led to converging calls for more systematic research to further examine algorithmic surveillance, always in context but across institutional domains and fields. This has started to result in fruitful comparative research, between field sites and around unifying concepts such as predictive policing and algorithmic security on the one hand, and algorithmic regulation on the other. Taking stock of this converging but still largely separate body of work, the article aimed at bridging the gap between literatures to contribute differently to the knowledge already accumulated on the algorithmic governance for policing and regulation. It is focused on one case study which has the distinctive but not unique feature of articulating algorithmic-related policing and regulation domains, in-between security and economic fields.

The global policy against illicit finance is built on the linking of differentiated universes whilst contributing to re-structure them at the same time, and the rise of big data surveillance is the illustration and the new driving force of this. On the one hand, as a fight against a wide range of dirty-money related crimes, it is based on a division of policing labour between heterogeneous institutional actors, with the surveillance part for financial institutions and the coercive part for law enforcement and intelligence institutions. On the other hand, as a financial regulation, it is based on the setting, monitoring and enforcing of international standards to manage any abuse of the financial system and altering the behavior of mostly private businesses to comply with this multiscale regulatory environment. In this context, algorithms and, by extension, big data surveillance are embedded in relationships of collusion and collision that shape them and that they are likely to impact and temporarily stabilize in return. From the need of big data surveillance to its ultimate deployment, unearthing the process of appropriation of algorithms makes visible this fluctuating, tensile equilibrium between competing goals at the core of a global policy configuration in constant transcoding and re-making locally. Here, big data surveillance is the common pillar for the simultaneous policing

of illegal activities by algorithms and regulation of legal ones through algorithms.

From this perspective, the imposition of heteronomous principles against illicit finance has significant consequences on the institutional order of the banking industry, with its major players as both algorithmic policing actors and algorithmic regulation targets. They must formally – appear to – be the compliant eyes and ears of the security state in order to continue to do financial business. Big data surveillance is part of the internalization of these security-related principles within this financial universe. But this does not mean that financial and security rationales at work are in any way indistinguishable, in spite of the convergence between policing and regulation around the formal motto of 'compliance for intelligence and intelligence for enforcement approach'. Again, big data surveillance operations are underpinned by dispositions, instruments and objectives that are always in tension and rarely complementary. And the final result is policing and regulation of neither too much nor too little, which gives rise to automated and everyday mass surveillance whilst remaining far removed from proactive crime-fighting and regulatory ambitions as it is from dystopian visions of big data and algorithmic drama.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Anthony Amicelle https://orcid.org/0000-0001-6735-4960

Notes

1. Algorithm is broadly defined here as "an abstract, formalized description of a computational procedure" (Dourish, 2016: 3). This "encompasses any kind of decision-making that passes data through a fixed and formal decision procedure, whether or not it results in a computer-automated decision" (Barocas et al., 2014).
2. An alert is deemed to be productive if the analyst in charge of processing it concludes that it is not an obvious error but a case that is sufficiently serious to be further investigated by a level 2 analyst with the prospect of suspicious transaction reporting.

References

ACAMS (2018) Best practices to successfully implement an AML monitoring system. *ACAMS Today* 17(1): 20–25.

Amicelle A and Grondin D (2021) Algorithms as suspecting machines: Financial surveillance for security intelligence. In: Lyon D and Murakami Wood D (eds) *Big Data Surveillance and Security Intelligence: The Canadian Case*. Vancouver: University of British Columbia Press, pp.68–87.

Amicelle A, Aradau C and Jeandesboz J (2015) Questioning security devices: Performativity, resistance, politics. *Security Dialogue* 46(4): 293–306.

Amoore L and Piotukh V (eds) (2016) *Algorithmic Life: Calculative Devices in the Age of Big Data*. London, New York: Routledge.

Amoore L and Raley R (eds) (2017) Special issue on securing with algorithms. *Security Dialogue* 48(1): 3–94.

Andrews L, Benbouzid B, Brice J, et al. (2017) Algorithmic regulation. *CARR, London School of Economics and Political Science Discussion Paper* (85).

Aradau C and Blanke T (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.

Barocas S, Rosenblat A, Boyd D, et al. (2014) Data & Civil Rights: Technology Primer, Data & Society Research Institute. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2536579 (accessed 30 June 2022).

Becker H (1998) *Tricks of the Trade: How to Think about Your Research While You're Doing It*. Chicago: Chicago University Press.

Bellanova R and de Goede M (2022) The algorithmic regulation of security: An infrastructural perspective. *Regulation & Governance* 16(1): 102–118.

Bellanova R, Irion K, Jacobsen KL, et al. (2021) Toward a critique of algorithmic violence. *International Political Sociology* 15: 121–150.

Benbouzid B (2019) To predict and to manage. Predictive policing in the United States. *Big Data & Society* 6(1): 1–13.

Benoît C (2018) Le pouvoir de régulation transnational d'une agence nationale. *Gouvernement et Action Publique* 7(1): 9–32.

Benoît C and Thiemann M (2021) Regulation. In: Pevehouse JCW and Seabrooke L (eds) *The Oxford Handbook of International Political Economy*. Oxford: Oxford University Press, pp.205–224.

Bigo D and Bonelli L (2019) Digital data and the transnational intelligence space. In: Bigo D, Isin E and Ruppert E (eds) *Data Politics: Worlds, Subjects, Rights*. London: Routledge, pp.100–122.

Brayne A and Christin A (2021) Technologies of crime prediction: The reception of algorithms in policing and criminal courts. *Social Problems* 68(3): 608–624.

Brayne S (2017) Big data surveillance: The case of policing. *American Sociological Review* 82(5): 977–1008.

Burk DL (2019) Algorithmic fair use. *The University of Chicago Law Review* 86(2): 283–307.

Chan J and Bennett Moses L (2017) Making sense of big data for security. *The British Journal of Criminology* 57(2): 299–319.

Christin A (2017) Algorithms in practice: Comparing web journalism and criminal justice. *Big Data & Society* 4(2): 1–14.

de Goede M (2018) The chain of security. *Review of International Studies* 44(1): 24–42.

Department of Finance Canada (2015) *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada*. Ottawa: Department of Finance Canada.

Dourish P (2016) Algorithms and their others: Algorithmic culture in context. *Big Data & Society* 3(2): 1–11.

Eyert F, Irgmaier F and Ulbricht L (2022) Extending the framework of algorithmic regulation. The Uber case. *Regulation & Governance* 16(1): 23–44.

FATF (2019) *Financial Action Task Force – Thirty Years*. Paris. Available at: https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/FATF30-(1989-2019).pdf

FATF (2021) *FATF Plenary, October 2021*. Available at: https://www.fatf-gafi.org/fr/publications/gafiengeneral/documents/plenary-october-2021.html

FATF (2022) *The FATF Recommendations*. Paris. Available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

Ferguson AG (2017) *The Rise of Big Data Policing*. New York: New York University Press.

Fintrac (2014) *Annual Report*. Ottawa.

Fintrac (2016) *Annual Report*. Ottawa.

Fintrac (2017) *Annual Report*. Ottawa.

Fintrac (2019) *Money laundering and terrorist financing indicators—Financial entities*. Ottawa.

Fintrac (2021) *Annual Report*. Ottawa.

Gilad S (2007) Regulatory enforcement. In: Bevir M (ed) *Encyclopedia of Governance*. Thousand Oaks: Sage Publications, pp.818–819.

Gill P (2002) Policing and regulation: What is the difference? *Social & Legal Studies* 11(4): 524–546.

Hacking I (2015) Biopower and the avalanche of printed numbers. In: Cisney VW and Morar N (eds) *Biopower: Foucault and Beyond*. Chicago: University of Chicago Press, pp.65–81.

Helgesson KS and Mörth U (2019) Instruments of securitization and resisting subjects: For-profit professionals in the finance–security nexus. *Security Dialogue* 50(3): 257–274.

Hildebrandt M (2018) Algorithmic regulation and the rule of law. *Philosophical of the Royal Society A* 376(2128): 1–11.

Katzenbach C and Ulbricht L (2019) Algorithmic governance. *Internet Policy Review* 8(4): 1–18.

Kaufmann M, Egbert S and Leese M (2019) Predictive policing and the politics of patterns. *The British Journal of Criminology* 59(3): 674–692.

Johns F and Compton C (2022) Data jurisdictions and rival regimes of algorithmic regulations. *Regulation & Governance* 16(1): 63–84.

Lange AC, Lenglet M and Seyfert R (2019) On studying algorithms ethnographically: Making sense of objects of ignorance. *Organization* 26(4): 598–617.

Lascoumes P (1996) Rendre gouvernable: de la "traduction" au "transcodage": l'analyse des processus de changement dans les réseaux d'action publique. In: CURAPP (ed) *La Gouvernabilité*. Paris: PUF, pp.334–335.

Lenglet M (2012) Ambivalence and ambiguity: The interpretative role of compliance officers. In: Huault I and Richard C (eds) *Finance: The Discreet Regulator. How Financial Activities Shape and Transform the World*. New York: Palgrave Macmillan, pp.59–84.

Lyon D (2014) Surveillance, Snowden and big data: Capacities, consequences, critique. *Big Data & Society* 1(2): 1–13.

Lyon D and Murakami Wood D (eds) (2021) *Big Data Surveillance and Security Intelligence: The Canadian Case*. Vancouver: University of British Columbia Press.

Méadel C and Sire G (2017) Les sciences sociales orientées programmes. État des lieux et perspectives. *Réseaux* 206(6): 9–36.

Nance MT (2018) The regime that FATF built: An introduction to the financial action task force. *Crime, Law and Social Change* 69(2): 109–129.

Neyland D (2019) *The Everyday Life of an Algorithm*. New York: Palgrave Macmillan.

Pinson G and Sala Pala V (2007) Peut-on vraiment se passer de l'entretien en sociologie de l'action publique? *Revue Française de Science Politique* 57: 555–597.

Reiner R (2010) *The Politics of the Police*, 4th ed. Oxford: Oxford University Press.

Rouvroy A (2016) *Of Data and Men. Fundamental Rights and Freedoms in a World of Big Data*. Strasbourg: Council of Europe.

Ruppert E (2012) The governmental topologies of database devices. *Theory, Culture & Society* 29(4/5): 116–136.

Shapiro A (2019) Predictive policing for reform? Indeterminacy and intervention in big data policing. *Surveillance & Society* 17(3/4): 456–472.

Star SL and Griesemer JR (1989) Institutional ecology, "translations" and boundary objects: Amateurs and professionals in Berkeley's museum of vertebrate zoology, 1907-1939. *Social Studies of Science* 19: 387–420.

Ulbricht L and Yeung K (2022) Algorithmic regulation: A maturing concept for investigating regulation of and through algorithms. *Regulation & Governance* 16(1): 3–22.

Vayre JS (2018) Comment décrire les technologies d'apprentissage artificielLe cas des machines à prédire. *Réseaux* 211(5): 69–104.

Woll C (2007) Regulation. In: Bevir M (ed) *Encyclopedia of Governance*. Thousand Oaks: Sage Publications, pp. 813–816.

Yeung K (2017) Algorithmic regulation: A critical interrogation. *Regulation & Governance* 12(4): 505–523.

Yeung K and Lodge M (eds) (2019) *Algorithmic Regulation*. Oxford: Oxford University Press.