Algorithms as Regulatory Objects

Abstract:

The recent dispersion of algorithms into the majority of social life makes algorithms the true analytical objects for sociology in the 21st century. The ubiquity of algorithms has led to increased public attention, scrutiny, and consequently, political regulation that is at the focus of this paper. I will show that such regulatory processes are not just aimed at *preventing* certain algorithmic activities, but that they are also *co-producing* algorithms. They determine, in very specific settings, what an algorithm *is* and what it *ought* to do. I will illustrate this by comparing two different European regulations of algorithmic practices: the regulation of trading algorithms in the German High Frequency Trading Act and in the Markets in Financial Instruments Directive (MiFID II) and the regulation of private data processing in the General Data Protection Law (GDPR).

Keywords: regulation, performativity, co-production, algorithms, automated decision making, algorithmic trading, regulation of algorithms, German High Frequency Trading Act, MiFID, GDPR

Making sense of and regulating algorithms

The recent dispersion of algorithms into the majority of social life makes algorithms the true analytical objects for sociology in the 21st century (Amoore and Piotukh 2016; Roberge and Seyfert 2016). Social attempts to make sense of algorithms can be found in a very different form of engagement with them, including designing, maintaining, selling, using and controlling them (Seaver 2014). I argue that political regulation, which will be the focus of this paper, plays a prominent role in the process of making sense of algorithms. I will show that such regulatory processes are not just aimed at *preventing* certain algorithmic activities, but that they are also *co-producing* algorithms. They determine, in very specific settings, what an algorithm *is* and what it *ought* to do.

Such conceptual framing is opposed to the common self-conceptualization of the law as "governmental social control" (Black 2010: 2). There are juridical debates about what it means when regulations *control* and *adjust* social conduct (Orbach 2012: 1). However, there is very little awareness that attempts to alter conduct also alter the nature of those whose conduct is regulated: subjects and objects alike. Rather than controlling and adjusting social practices, regulations are themselves social practices that co-produce the subjects and objects of social reality. Elucidating the more (co-)productive nature of regulation will help us better understand the mechanisms and effects of juridical practices. It will also help practitioners of the law to better understand and perhaps evaluate the impact of regulation, its positive and negative effects. My comparative analysis of regulatory texts shows how different definitions of the same object (algorithms) can lead to very different regulations and, consequently, to very different regulatory efficacies.

After introducing the concept of co-production, I will analyse two very different types of regulation and I will show how these legal texts co-produce the algorithms in two very different ways. I will also show how the definition of the algorithm is related to and perhaps derived from the notion of human subjects implied in the regulatory text.

I will focus on two regulations of algorithmic practices that have recently come into law in the European Union, the regulation of trading algorithms, as can be found in the German High Frequency Trading (HFT) Act and the Markets in Financial Instruments Directive (MiFID II) and the General Data Protection Law (GDPR). While the GDPR attempts to reconfigure algorithmic systems in accordance with expectations of digital literate subjects, the regulation of algorithmic trading systems enforces the expectations of strategically illiterate regulators onto the algorithmic framework.

Algorithmic regulation as social co-production

The question of what is an algorithm is a problem of observation but also one of production. It is not simply an epistemological question but also an ontological one. Studies of scientific knowledge have lucidly shown the productive aspect of observation (e.g. Knorr Cetina 1999). This productive aspect becomes even more pertinent when we talk about legal regulations, since regulations do not just produce scientific facts but produce and enforce social rules and norms. However, implied in this production of rules and norms is also a co-production of the object to be regulated, the co-production of *outcomes*. By adopting the idea of a regulatory co-production, the approach adopted in this paper will differ from other concepts in the sociology of law.[1] Specifically, I adopt a relational perspective, where social norms and legal rules are mutually co-produced (e.g. Lenglet 2019). In such a conceptual framework, the legal system is a performative co-production of social reality. In other words, the legal system does not simply regulate the movement, treatment and activities but rather performatively co-produces them.

However, simply stating a co-productive relation between knowledge and social reality might seem unbearably abstract. In addition, one might wonder through which specific relations knowledge and representations in fact co-produce social reality. How are they constituted?

The concept of co-production

The concept of co-production is part of a relational sociology that can be found in various disciplines such as Governmentality Studies (Bröckling, Krasmann and Lemke 2012), Actor Network Theory (Latour 1993), Science and Technology Studies (MacKenzie and Millo 2003, MacKenzie 2006, Callon 2007) and Social Studies of Finance (Muniesa 2014; Lenglet and Taupin [forthcoming]). It operates under the assumption that 'the ways in which we know and represent the world (both nature and society) are inseparable from the ways in which we choose to live in it' (Jasanoff 2006: 2). Performativity describes the effects that assumptions, utterances and theories have on the world. Fabian Muniesa has formulated the problem of performativity as 'making something explicit' (Muniesa 2014: 24). Crucially, making something explicit does not simply describe a process of finding the truth about something previously unknown: 'explicitness […] affects what is at stake in a truly inventive fashion, with no particularly

[1] The analytical perspective of the present article does not operate from a representational perspective where the legal system is the symbolic expression of underlying social norms and values (Durkheim 1969). Nor do I understand the legal system as a rational and legitimate type of social authority (Weber 1978). Further, this paper does not follow the perspective of social differentiation where the legal system is a social subsystem that operates according to its own logic (Luhmann 2008).

transcendental antecedent' (ibid. 24). It is this 'inventive' aspect of performativity that I will focus on in regulatory practices.

Very often, this inventive aspect consists in processes of classification and demarcation. Thus, Michel Foucault has defined the ways 'human beings are made subjects' as 'the objectivizing of the subject' (Foucault 1982: 777). According to Foucault, processes of objectivizing are based on 'dividing practices', e.g. classifying human subjects as the 'mad and the sane, the sick and the healthy', etc. (ibid.). Such processes of objectivization co-produce the human subject.

With regards to algorithms, scholars from Critical Data Studies use the approach of co-production to explain (digital) subjectivity, of processes of making (certain assumptions about) a subject 'explicit'. The performative mechanism consists in addressing a person. For instance, addressing somebody – by his/her gender, race, name etc. – means to create his/her subjectivity (Blackman et al. 2008: 2). In an algorithmically ordered world, it is the algorithm which creates a subject. For instance, an algorithm 'addresses' a person by their 'digital identity'. As users, we are addressed as somebody with certain interests and expected behaviours. These algorithmic expectations then become the template for demarcating and objectivizing digital subjectification (Kitchin 2014: 165).

The process of digital subjectification through algorithmic processing sheds light on the relational character between human subjects and algorithmic objects. Human subjectivity is co-produced by algorithmic processing. However, and this is crucial, algorithmic processes co-produce subjectivity as much as human subjectivity co-produces algorithms. For instance, veryday human practices change algorithmic processes, which is semantically expressed when it is said that algorithms 'learn' from human behaviour.

Instead of the everyday usage of algorithmic technologies, I am interested in the role of political regulation in the co-production of algorithms. How are algorithms being made explicit in regulatory texts and how are they co-produced? What dividing practices and practices of objectification are being utilized? What regulatory demarcations are created, e.g. between algorithms that are safe or risky, practices that are abusive or fair, spheres that are private or public, and so on. Consequently, which notion of digital subjectivity are they derived from or, vice versa, what type of digital subjectivity do they co-produce?

A brief overview of the two regulations discussed below shows us the different definitions of human subjects and algorithmic objects and the relation they have with each other. The primary aim of the GDPR is to regulate the handling of users' private data. Its primary understanding of the user is of a digital subject that is technically fluent, algorithmically literate, and that demands digital sovereignty (Schweitzer 2017). Implied in the definition of a digital subject is its counter image, an algorithm that automatically handles private data in a way that is intelligible to the user. Thus, the definition of the digital subject laid out in the GDPR not only co-produces the human user as a digitally literate subject but also the algorithm as an ‘intelligible’ algorithmic object.

In contrast, regulations of financial markets (the German High Frequency Trading Act and MiFID II) conceptualize trading algorithms as something that is mostly opaque to humans, especially to human regulators. In such regulations, the regulatory subject is explicitly and strategically staged as digitally illiterate, lacking expertise (in terms of qualification but also in terms of manpower). The co-productive power of this regulation does not lie in making the algorithmic processes intelligible to humans, but rather in forcing algorithms to ‘behave’ according to expected market behaviour.

I will talk about the consequences of these regulatory co-productions and their efficacies in the discussion below.

Objectivizing a regulatory object

Common definitions understand regulations as the management of existing risks: ‘Regulation is state intervention in the private domain, which is a by-product of our imperfect reality and human limitations. We have regulations only because “poisons” exist’ (Orbach 2012: 10). Such notions operate with essentialist assumptions: Poisons exist and their essence can be clearly identified. In addition, they define regulation only in a reactive sense, as a ‘by-product’ that aims to correct imperfect developments.

As I have said above, regulation is very often not just a by-product but a co-production. Such co-production of legal objects consists in processes of demarcation. Very often, what is poisonous does not exist in advance but is being legally produced: ‘Regulation explicitly or implicitly creates demarcations and boundaries that make objects appear hazardous or harmless, safe or risky, natural or unnatural, important or unimportant.’ (Lidskog et al. 2011: 112). For instance, toxic thresholds must be defined and their definition turns a grey area into a red line. Elisabeth Fisher has shown how chemical substances are co-produced by regulations in different ways and to varying degrees. Their specific regulation depends on many things including the purity of their quality, their market value, the risk they pose to humans and the environment, and so on. And with each iteration, the regulation changes the demarcation of the object itself: ‘Chemicals are indeed malleable regulatory objects’ (Fisher 2014: 171). Such co-productive effects make political regulation an inherently ontological activity.

The specificity of algorithms as regulatory objects

The same can be said about algorithms. Similar to chemical substances, they might be regulated in accordance with their inner quality (the intention contained in the code), the market value (proprietary objects) or the risk they pose to humans and the environment (e.g. tools for market manipulation or breach of privacy). However, there are differences between chemical substances and algorithms.

First, algorithms are not inherently malleable but are contextual. Strictly speaking, the term *algorithm* is already a co-productive reduction insofar as *an* algorithm is always also a multiplicity of algorithms (Morris 2015). An algorithm usually consists of clusters or chains of algorithms and the demarcation that makes these multiple algorithms into *one* algorithm is also part of the regulatory processes discussed in this paper. Second, they are highly dependable objects that can exist only in an algorithm-ready environment (Gillespie 2014). Third, they are interactional objects and their interactions can lead to unintended outcomes (Knorr Cetina 2013; MacKenzie 2019). Finally, they are highly opaque objects. This opaqueness is due to their contextual, interactional and proprietary nature (Introna 2011; Steiner 2017). It is also due to "the mismatch between mathematical optimization in high-dimensionality, characteristic of machine learning and the demands of humanscale reasoning and styles of semantic interpretation" (Burrell 2016: 2). In other words, machine learning algorithms are opaque to human beings because they are not made to explain their results to humans.

In the following I will discuss two different ways algorithms have been regulated, in financial markets and in data privacy. I have chosen these two cases because they are illustrative of two very different ways of regulating algorithms; regulations that operate with different notions of subjectivity and co-produce algorithms accordingly.

Regulating Financial Markets

Today, a case of regulating trading algorithms can be found in the Markets in Financial Instruments Directive (MiFID II) by the European Union. This European regulation was preceded by the German High Frequency Trading Act, the first regulation of Algorithmic Trading in the European Union and the precursor to MiFID II. German HFT Act was enacted on 15th May 2013 but was preceded by an intensive public debate that included very different notions of trading algorithms and how to regulate them.

In 2012, Peer Steinbrück, the social democratic (SPD) candidate for German chancellor wrote a working paper entitled 'Regaining trust: A new attempt to tame financial markets'. It defines High Frequency Trading as stock market trading among machines where 'algorithms buy securities in high volumes, in order to sell them again after a very short holding period in the range of milliseconds' (Steinbrück 2012 [my translation]). The paper links worries about the effects of HFT to a particular 'fear of algorithms with manipulative trading strategies'. This narrative of fear contains a decisive first step towards the regulation of algorithms. Not only does it create the regulatory demarcation between a manipulative and fair algorithmic strategy, but more fundamentally, it establishes the demarcations of the algorithmic object itself. In fact, the demarcation of a manipulative (dangerous) trading algorithm is only a derivative second step after *objectivizing the algorithm as a distinct object*. The following quote from Steinbrück's working paper outlines the regulatory move that demarcates the algorithm as a distinct object.

> The core of an effective regulation needs to be a public licensing procedure not just for trading firms, but directly for the trading algorithms themselves. Within this licensing procedure, the authority will assess the algorithm based on the trading strategy it is pursuing: dangerous trading strategies must be banned! … […] A specific algorithm would receive a distinct tag with which it identifies itself at the exchanges. Alterations of the algorithm would require a new license and a new tag. The distinct tag would ensure that only licensed algorithms trade, and it would make it possible to withdraw certain dangerous algorithms from the market, or stop automated trading altogether. (Steinbrück, 2012 [my translation]).

This process of creating the algorithm as a regulatory object includes the separation of trader/trading firm from trading algorithm, the attribution of intentions (strategies) to the algorithm, the identification through a distinct tag and, consecutively, the issuing of a public licence. Such a definition follows an intentionalist approach, where every algorithmic activity can be traced back to the strategy of the algorithm that has deliberately been implemented by its designers. The intentionalist approach is similar but not identical to essentialist approaches. *Essentialists* understand an algorithm as a distinct object or system (Croll 2016) that contains all its specifications in its inner core. A designated algorithm is somewhat independent from other algorithms. This approach defines the nature and the essence of this core as code. For outsiders, such systems usually appear as a black box. Regulatory demands related to the essentialist approach aim at reading and deciphering this code, a demand that is preceded by the general call for the opening of all black boxes of algorithms (Pasquale 2015) and to disclose the 'complete source code' (Scherer 2016: 397). In such notions, the algorithm changes only insofar as the code changes, in which case the algorithm would fall under a new regulation.

The *intentionalist* approach is similar but also decisively different from essentialism. The identity of the algorithmic object is not its codes but the 'strategy it is pursuing' (see Steinbrück above). Here, an algorithm is defined by its intentions but not by its essential specifications contained in the code. If the strategy of an algorithm changes, the identity of the algorithm changes. In that sense, the change in identity of an algorithm is not necessarily related to the change of the code, but can also take place if the environment changes. The most obvious case is a change in regulation that declares previously acceptable trading strategies as being manipulative. In such a case, the identity of the algorithm would have changed (from safe to manipulative) without a change in a single line of code.

At first glance, the licensing procedure described in Steinbrück's working paper from 2012 seems very similar to what was enacted in the 2013 German HFT Act: the requirement of the labelling of trading algorithms. However, it was only the first step towards the creation of a trading algorithm as a regulatory object. Not all suggestions in this working paper have materialized in the regulatory text. Rather, Steinbrück's paper is part of a process of coming to terms with an opaque object that necessitated demarcation.

The making of High Frequency Trading (HFT)

It is important to remember that the initial motivation for this regulation was a worry about market abuse, and the need to correctly identify the algorithms connected to abusive strategies. It is precisely the worry about a strategy that has proven difficult to regulate. The increasing complexity of market micro structure makes it exceedingly difficult to separate market abuse and risks. As Nathan Coombs, who has studied the origin of the German HFT Act in detail, writes, such difficulties are mainly related to the identification of intentions: '[E]ven if trades bear the hallmarks of manipulative activity, with the interactions in the order book of a financial exchange being so complex it is difficult to know whether or not they were the result of a deliberate strategy' (Coombs 2016: 285-86). In addition, market risk might emerge from algorithmic market activities that did not have inherent manipulative intentions. Furthermore, what might appear to be manipulative to some might simply be a software bug to others (Lenglet 2011; Seyfert 2016); and some risky algorithms might have emerged without previous intentions.

But resorting to essentialist and intentionalist types of regulation also turned out to be impractical. Essentialist and intentionalist regulations turned out to be unattractive for many reasons. First, the HFT industry is defined by a general 'culture of secrecy' (Gomolka 2011: 5). Trading algorithms are not open source, and firms are shielding their proprietary algorithms, resisting the disclosure of the strategies of their trading algorithms, let alone their source code. Second, because of the sheer amount of data that is characteristic for HFT, it is simply impossible to monitor all code. And third, there are the complexity issues mentioned above. The unpredictable feedback effects of algorithmic interactions throws in doubt the meaning of analysing the intentions and operations of individual algorithms. In addition, the respective market authorities lack the necessary expertise and number of personnel to supervise this newly emerging market technology. However, beyond the simple lack of expertise there is also a technical problem. The contextual and interactional nature of algorithms implies that an algorithmic activity is usually the combined activity of dispersed, dynamic and relational parts. To decide which system, sub-system, part, sum of parts or sub-parts, which cluster or chain of algorithms constitutes an algorithm is often an arbitrary decision and is usually taken by its designers for practical, contextual reasons. These constructions can change among firms, and what are multiple algorithms for some can be just a single algorithm for others. Such organizational differences make essentialist and intentionalist regulations very difficult. In fact, they all gesture to the necessity of the regulators to impose a particular definition of an algorithm onto all market participants.

Such a move can be identified in the making of the German HFT Act. The regulators decided on a completely novel way of defining an algorithm and they did so for the reasons mentioned above. The subtext of the law communicates the message that since we, the regulators, do not get access to the source code or the strategies of the algorithm, and since we are also not very interested in such access because we lack the expertise and personnel for the necessary oversight, we will tell you what we consider to be an algorithm or an algorithmic activity, and we will force you to re-sort your system according to our definition. Thus, the actual regulation is based on a move to simply turn the tables, where regulators strategically assumed the role of the *digitally illiterate*. This is what I call a *relational approach* to defining an algorithm.

The German HFT Act: a relational account

The *Act on the prevention of risks and abuses relating to high frequency trading* (Hochfrequenzhandelsgesetz) took effect on 7 May 2013 (BGBl I 2013/1). It contained additional guidelines to the adherence of this regulation. The relevant passage in this text defines a ‘trading algorithm [as] a well-defined, executable sequence of instructions with a finite length to perform trading, i.e. containing the definition of the order parameters as well as the entry, change and deletion of orders’ (Hessisches Ministerium 2014: 1). The type of financial instruments, the type of order (buy-sell), the quantity of the order, etc. are defined as order parameters. A sequence is defined as 'instructions determining the aforementioned order parameters and is to be distinguished from any other sequence of instructions' (Hessisches Ministerium 2014: 2). Decisively, the identity of an algorithm is defined as *the complete sequence of algorithmic decisions* that lead to the actual order. The regulatory text relates all events leading to the trading activity, including the information search, the decision-making process, the order execution etc., to *one* algorithm. For market authorities, all that matters is what happens in the 'order book'. An order book is the list of an electronic stock market that matches orders of market participants; an 'an exchange's […] electronic file of the bids to buy each stock and the offers to sell it' (MacKenzie 2018: 1644; see also MacKenzie 2019). The German HFT Act did not bother with codes and strategies of algorithms but decided to leave it up to the market participants to define a trading algorithm according to the effects it has on the (order books of) financial markets. The relevant questions are, what type of instruments are being ordered, what type of orders have been submitted to the order book (buy or sell), and what is the quantity. Consequently, a trading algorithm is re-constructed from the effects it has on the order book: from the parameters given in the order book. This is a novel way of defining an algorithm, of making algorithms specific regulatory objects within the law. The regulatory text leaves it up to the trading firm to ascertain how they organize their internal algorithmic operations. It is up to them to decide how to define this sequence, how to assemble algorithmic processes into one algorithm. Even more so, it leaves it to the discretion of the trading firm to differentiate manual (human) from automated (algorithmic) trades. All a firm has to do, is to attach a tag to what it has decided to call an algorithmic bid or offer. However, the regulation does oblige all market participants to store all trading data for a period of five years. That way, regulators leave it open to themselves to retrospectively challenge the non-/algorithmic demarcations by the trading firms. Thus, they can deliver judgment on their decisions when things go wrong, always re-constructing these algorithmic activities from what actually happened in the order book.

Consecutively, on 3 January 2018 the European Securities and Markets Authority (ESMA) enacted the *Markets in Financial Instruments Directive* and *Regulation* (MiFID II) that adopted many stipulations of the German HFT Act. It essentially incorporated the tagging rule of the German HFT Act. It stipulates that it is 'necessary to tag all orders generated by algorithmic trading' and defines it in the following way:

> 'algorithmic trading' means trading in financial instruments where a computer algorithm automatically determines individual parameters of orders

> such as whether to initiate the order, the timing, price or quantity of the order or how to manage the order after its submission (Article 4(1)(39)).

The tagging rule marks an epistemic shift from opening black boxes and the study of intentions to a relational account of algorithmic objects. While the focus on the code of an algorithm demarcates a clear frame of analysis, the tagging rule changes the identity of the algorithm. In the tagging rule, a number of algorithms, a series or a whole complex of algorithms can become 'one' algorithm: 'The tagging device was never intended to represent trading firms' algorithms as they "really are". The point was instead to generate information that would render visible the relational interactions between algorithmic strategies.' (Coombs 2016: 293).

In sum, the relational account for an algorithm differs from essentialist and intentionalist definitions insofar as it does not approach algorithms as pre-existing objects. Instead of defining the algorithm from its core (code) or intentions (strategy), it defines it from the *impact* it has on its environment (the order book). Even though the German HFT Act and MiFID II seem to have incorporated the idea of identifying algorithms as stated in Steinbrück's working paper, the tagging rule has introduced a definition of algorithms that is very different from what had previously been laid out in this paper. It leaves behind the idea of an algorithm with an inner code or intention. It also leaves behind the idea of the algorithm as a black box to be opened and regulated. Instead, the algorithm is what causes an effect on the order book, with the effects being precisely categorized (e.g. the specific parameters).

This novel definition will become especially insightful, if contrasted with the notion of the algorithm as a tool which materializes the intentions of a human subject. Such a notion can be found in the recently enacted General Data Protection Regulation of the European Union.

Regulating Fundamental Rights and Freedoms

Regulation 2016/679 (GDPR) of The Parliament and Council of the European Union (2016) took effect on 25 May 2018. As in the case of the German HFT Act and MiFID II it emerges as a result of a crisis related to recent technological developments and the increasing exploitation of private information. While market regulation in the German HFT Act and MiFID II are concerned with the integrity of market infrastructure, the GDPR has more humanistic intentions: 'The processing of personal data should be designed to serve mankind' (preamble, paragraph 4).

In this regulation, the definition of the algorithm is co-produced in accordance with the requirements of those whose data is automatically processed. Thus, in order to identify the specific definition of the algorithm within this regulation we need to reconstruct the definition of the digital subject that it is derived from.

At the core of this regulation is the digital subject and its relation to the natural person, whether or not our digital image sufficiently corresponds with our self-image as natural persons (Schweitzer 2017: 251). At which point does the algorithmic image of the digital subject turn into a violation of personal privacy, and when do individual users have a right for this image to be altered or deleted, e.g. publicly forgotten? The GDPR aims at giving natural persons the authority over this digital image. The GDPR aims to regulate the rights and authority of the natural person ‘to the processing of personal data by automated means’ (GDPR, preamble, paragraph 15).

Thus, the natural person shall have the right to consent ‘to the processing of personal data’ (Chapter 1, Article 4/11); the right to know about the collected data (Art 13-15); the right to have this data rectified (Art 16), deleted (Art 17), not processed (Art 21) and ported (Art 20); the right to obtain human intervention, which involves a right to ‘contest the decision’ by automated processes (Chapter 3, Section 4, Article 22, 1-3). In addition, the process of automatically collecting personal data has to be ‘transparent’ to the natural person and has to involve information of possible risks of such processing. Furthermore, the data subject has ‘the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.’ (Chapter 3, Section 4, Article 22, 3). Finally, the natural person has the right to have their digital image altered, to have their ‘personal data’ erased, and ‘the right to withdraw consent at any time’. (Chapter 3, Section 2, Article 13, 2). This right also applies to second usage of data, personal data that is used ‘for purposes other than those for which the personal data were initially collected’ (Chapter 3, Article 6, 4).

The GDPR regulates the digital subject by selectively enforcing certain aspects of the natural person onto the digital subject, giving the natural persons the right to have authority over these aspects. The GDPR establishes the right of the natural person along very specific aspects of its digital identity. The linkage is established by defining personal data as ‘any information relating to an identified or identifiable person (“data subject”).’ (Chapter 1, Article 4, 4). But these identifiable features are not classic features of the natural person. For instance, the right to object to the algorithmic processing of data is related to non-discrimination and profiling (Chapter 3, Section 4, Article 22, 1). However, profiling is not related to common aspects of the natural person such as race, gender, age, nationality etc. but to selective aspects of the digital subject, such as ‘personal preferences, interests, reliability, behaviour, location or movements’ (Chapter 1, Article 4, 4).

Digital subject and algorithmic object

As I have said above, what is at stake in this regulation is not just the right of the digital subject and the natural person but the simultaneous co-production of algorithmic object and digital subject (Carstensen et al. 2014). On the one hand, the regulation of how to automatically process personal data co-produces the digital subject. It co-produces the digital subject as a *digitally literate subject*. Implicit in this regulation is the notion of the technically-fluent subject that demands consenting algorithmic relationships and the right to object to such relationships.[1] The notion of a digital subject presupposes the willingness, digital literacy and expertise of the natural person to engage with their digital image. It connects political regulation to what N. Katherine Hayles has called the 'values of liberal humanism […] the right of a self to autonomy and freedom, and a sense of agency linked with a belief in enlightened self-interest'. All technology is to be designed to serve human subjects, understood as 'coherent, rational sel[ves] […] (Hayles 1999: 85-86).

This definition of the user as a digitally literature subject has co-productive effects for the algorithmic object. The GDPR co-produces the algorithmic object as the mirror image of the digital subject. It co-produces it as a tool that is, in principle, comprehensible to a technically fluent user. Thus, the regulation presupposes that algorithmically produced data can be accessed the same way that traditional information such as mailing addresses and age can be accessed. For instance, rights over information stipulate that the data subject has to be provided with 'information [about] the existence of automated decision-making, [and] meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject' (Section 2, Article 13(2f))**.** Such provision of information also includes the processing of data 'for purposes other than those for which the personal data were initially collected' (Chapter 3, Article 6, 4).

The algorithmic object co-produced in the GDPR is an epistemic object that is interpretable in principle. Those who are willing, technically fluent and digitally literate are able to understand algorithmic operations. For the GDPR, most faculties of cognition and action have to stay on the side of the enlightened subject. Such regulation creates conflicts with technologies that resume cognitive and active responsibility, where algorithmic objects and digital subjects can easily switch sides (Lange, Lenglet and Seyfert 2018).

First, producers of digital subjects such as social media companies create online identities that are not directly constructed out of public information such as age, ethnicity, gender, mailing address, etc., but constructed mainly from a digital user profile assembled from online behaviour. Social media companies construct the digital subject by what they paradoxically call *anonymous identifiers*. The anonymization process involves various steps, e.g. generalization – 'to remove a portion of the data or replace some part of it with a common value' – and adding noise to data sets (Google 2019).[2] Thus, (in theory) there is no direct relation between the digital subject and the natural person. However, such a relation can be established by the interference and imposition of meaning from and to this data. In its current form, however, this regulation fails to give human individuals any rights regarding the conclusions and interferences that are drawn from this data: 'data subjects have control over how their personal data is collected and processed, but very little control over how it is evaluated' (Wachter and Mittelstadt forthcoming: 4). It does not regulate the *effects* the algorithm has on the digital subject; the effects it is subjected to by an algorithmic process: 'for example the [algorithmic] decision not to grant residency or to fail someone at an exam, is not personal data' (Wachter and Mittelstadt forthcoming: 31).

Second, machine learning algorithms are not created in order to 'explain' the correlations they have discovered. They 'identify patterns and correlations that cannot be detected by human cognition' (Yeung 2018: 505). They lead to an inherent 'lack of interpretability' (Lisboa 2013: 17), because their processes do not 'explain' the correlations they discover. As Goodman and Flaxman put it: 'Putting aside any barriers arising from technical fluency, and also ignoring the importance of training the model, it stands to reason that an algorithm can only be explained if the trained model can be articulated and understood by a human' (Goodman and Flaxman 2017: 55).

However, the co-productive effects of the GDPR might be found elsewhere. Recently, attempts have been made to make unintelligible machine learning algorithms 'intelligible', i.e. to make their decisions 'explicit' to the digital subject. In this context, some have argued that regulations such as the GDPR itself have led to an increased research in and development of machine learning (Holzinger et al. 2018). While current machine learning algorithms do not explain their results, future algorithms might very well do so. The co-productive effect of GDPR might thus lie in the co-production of explainable and thus 'intelligible' machine learning algorithms. Such technologies would at the same time make it possible to evaluate and control the interferences that have been made from personal data.

Potentials and limits of the regulatory co-production

In this last paragraph I discuss the efficacy of these two regulations. Applying the conceptual framework of co-production shows us that regulations are far more efficacious then the notion of regulation as adjustment and governmental control suggests. Regulations do not merely limit certain activities but actively participate in the production of social reality. Such realization strengthens the role of regulation. It also makes it more complicated to assess their efficacy.

Undoubtedly, assessing regulatory success is difficult in general. Very often, the co-productive effects of regulations go beyond the mere implementation of regulatory requirements. For instance, Julia Black emphasizes that regulation is shaped by "regulatory conversations […] between regulators, regulated and others involved in the regulatory process" (Black 2002: 170). Thus, regulation might have performative effects that exceed successful technical implementation, e.g. by shaping public opinion, which might lead to new regulations in the future. In addition, a regulation can influence technological developments, such as explainable machine learning algorithms. Thus, my assessment can only be tentative and further research would have to be conducted in order to gain a more fine-grained picture.

In the case of the of the German High Frequency Trading Act and MiFID II, it is safe to say that the regulatory articulation did re-figure the algorithm according to the image of the regulation. It has been fully implemented. Regulators argue from the position of a strategically assumed digital illiteracy, imposing on algorithmic trading firms definitions and behaviour they expect from trading algorithms. Through the process of algo-tagging, trading firms were obliged to redraw the demarcations of algorithmic objects within their socio-technical systems. In addition, the behaviour of the algorithm has been framed according to the parameters defined within the regulation. Even though this process of algorithmic demarcation is – to a certain extent – left to the discretion of the firms, the fact that they need to store all trading data means regulators can retrospectively question these decisions. Regulators can demand access to this data, analyse this data according to their own classification, and have the regulatory power to retrospectively define trading activities as predatory, manipulative, etc. In addition, the regulators have the political means and will to enforce this regulation.

In comparison, the efficacy of the GDPR is much harder to assess. For many experts, this regulation does not have the same efficacy as the regulation within financial markets, at least not yet. Up to the time of publication of this article, experts grapple with a lack of implementation and political enforcement (Davies 2019). While small firms have mostly dutifully implemented these regulations, for instance by giving users the option whether or not they want to be tracked, the same is not the case for bigger companies such as Google and Facebook. They only give their users the option to waive their rights or not use their service at all. Given their market position, such a move amounts to blackmail, in which you can either accept any condition or face social isolation. In other words, these firms have bypassed this regulation (Forbrukerrådet 2018). Recently, several non-profit organizations such as Austrian-based *noyb.eu* and the French advocacy group *La Quadrature du Net* have filed complaints against several companies for violating Article 7(4) of the GDPR by threatening access to their services if users do not accept all types of data processing. It remains to be seen whether or not this will lead to the successful enforcement of this regulation.

However, the co-productive effects of the GDPR might be more related to the technological changes emerging from it. By co-producing the algorithm as interpretable object, the GDPR might nudge the industry towards the development of interpretable and explainable machine learning algorithms, simply because it grants natural persons this right to explanation. Such algorithms would simultaneously allow users to access the interferences these algorithms make when they 'process private data by automated means'.

Conclusion

The conclusion we can draw from these two cases is that regulation can be efficient. Both types of regulation have very different ways of co-producing the algorithmic object (and digital subject). They make very different assumptions about the digital subjects and algorithmic objects, each leading to differing ways of addressing the algorithm as an object with certain characteristics (its code), intentions (its strategy) and effects. In particular, the case of regulating algorithmic instruments in financial markets shows the political power of regulators and the efficacy of the regulation when things get too technologically complex or too proprietary and secretive. Algorithms are co-produced according to the will of the regulators, who strategically assume the role of the digitally illiterate. In turn, the GDPR constructs the algorithmic object as a mirror image of the digitally literate subject. The problem with this regulation is that (1.) is has not been sufficiently enforced and (2.) it gives digital subjects the right to have the processing of their personal data explained to them, when the algorithms processing their data are not technically capable of explaining their decisions. But the success of regulatory co-productions is hard to measure and their performative effects might lie in the future. First, the enforcement of this regulation is still work in process. Second, this regulation might influence future technology, thus potentially co-producing intelligible (machine learning) algorithms that make things explicit to us.

Acknowledgement:

I thank Marc Lenglet and the reviewers of *New Media & Society* for their valuable and generous comments on an earlier version of this paper. The final manuscript has greatly benefited from their critical engagement.

[1] A philosophical summary of this imaginary subject, implicit in the legal text, can be found in Anthony Gidden's *Magna Charta for the Digital Age* that he formulated during is time on the House of Lords Select Committee on Artificial Intelligence in the UK (Giddens 2018).

[2] That does not mean traditional aspects of the natural person are unrelated to the anonymous identification process. They can be re-constructed, for instance by interference. In fact, some researchers claim 'that Google has the ability to connect the anonymous data collected through passive means with the personal information of the user' (Schmidt 2018: 4). Thus, individual attributes about gender, race, political orientation etc. can be interfered from presumably 'anonymous' data (Kuner et al. 2012).

Literature:

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

BGBl I 2013/1 (Bundesgesetzblatt Jahrgang 2013, part I, no. 23), 14 May 2013, Bonn.

Black D (2010) *The Behavior of Law*. Bingley: Emerald Group.

Black J (2002) Regulatory Conversations. *Journal of Law and Society* 29(1): 163-196.

Blackman L, Cromby J, Hook, D, Papadopoulos D and Walkerdine V (2008) Creating Subjectivities. *Subjectivity* 22(1): 1–27.

Bröckling U, Krasmann S, Lemke T (eds) (2012) *Governmentality. Currents Issues and Future Challenges*. London: Routledge.

Burrell J (2016) How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms. *Big Data and Society*. DOI:10.1177/2053951715622512.

Callon M (2007) What does it mean to say that economics is performative? In: MacKenzie D, Muniesa F and Siu L (eds) *Do Economists Make Markets? On the Performativity of Economics*. Princeton, N.J. et al.: Princeton University Press, pp. 311-357.

Carstensen T, Schachtner C, Schelhowe H, Beer R (eds) (2014) *Digitale Subjekte: Praktiken der Subjektivierung im Medienumbruch der Gegenwart.* Bielefeld: transcript.

Coombs N (2016) What is an algorithm? Financial regulation in the era of high-frequency trading. *Economy & Society* 45(2): 278-302.

Croll A (2016) How to regulate an algorithm. In: *Pandemonio*, at https://medium.com/pandemonio/how-to-regulate-an-algorithm-c2e70048da3, November 16, (accessed 17 March 2019).

Davies J (2019) 'We've only just started': 1 year into GDPR, ad industry braces for more fines. In: *Digiday*, at https://digiday.com/media/weve-just-started-1-year-gdpr-ad-industry-braces-fines (accessed 27 May 2019).

Diakopoulos N (2014) Algorithmic accountability reporting: On the investigation of black boxes. In: *Tow Center for Digital Journalism*, Columbia Journalism School, https://www.cjr.org/tow_center_reports/algorithmic_accountability_on_the_investigation_of_black_boxes.php (accessed 17 March 2019).

Durkheim É (1969) *The Division of Labor in Society*. London: MacMillan.

European Securities and Markets Authority (ESMA) (2014) *Markets in Financial Instruments Directive* (MiFID II), 2004/39/EC, 12 June 2014.

Fisher E (2014) Chemicals as Regulatory Objects. *Review of European, Comparative & International Environmental Law* 23(2): 163-171.

Foucault M (1982) The Subject and Power *Critical Inquiry* 8(4): 777-795.

Giddens A (2018) A Magna Charta for the Digital Age. *New Perspectives Quarterly* 35(3): 6-8.

Gillespie T (2014) The Relevance of Algorithms. In: Gillespie T, Boczkowski P J and Foot K A (eds) *Media Technologies: Essays on Communication, Materiality, and Society*. Cambridge, Mass: The MIT Press, pp. 167–193.

Gomolka J (2011) *Algorithmic trading: Analyse von computergesteuerten Prozessen im Wertpapierhandel unter Verwendung der Multifaktorenregression*. Potsdam: Universitätsverlag Potsdam.

Goodman B and Flaxmann S (2017) European Union regulations on algorithmic decision-making and a 'right to explanation' *AI Magazine* 38(3): 50-57.

Google (2019) How Google anonymizes data. In: *Google Privacy & Terms* at https://policies.google.com/technologies/anonymization?hl=en (accessed 17 March 2019).

Hayles N K (1999) *How we became posthuman: virtual bodies in cybernetics, literature, and informatics*. Chicago & London: The Chicago University Press.

Hessisches Ministerium für Wirtschaft, Energie, Verkehr und Landesentwicklung (2014): 'Guidelines to the adherence to the requirement of the labelling of trading algorithms', https://wirtschaft.hessen.de/sites/default/files/media/hmwvl/guidelines_to_the_adherence_to_the_requirement_of_the_labelling_of_trading_algorithms_14-09-22.pdf (accessed 17 March 2019).

Holzinger A, Kieseberg P, Weippl E and Tjoa A (2018) Current Advances, Trends and Challenges of Machine Learning and Knowledge Extraction: From Machine Learning to Explainable AI. In: Holzinger A, Kieseberg P, Tjoa A and Weippl E. (eds) *Machine Learning and Knowledge Extraction*. Cham: Springer, pp. 1-8.

Introna L D (2011) The enframing of code: Agency, originality and the plagiarist. *Theory, Culture & Society* 28(6), 113-141.

Jasanoff S (2006) The Idiom of Co-production. In: Jasanoff S (ed) *States of Knowledge: The Co-Production of Science and Social Order*. London: Routledge, pp. 1-12.

Kitchin R (2014) *The Data Revolution: Big Data, Open Data, Data Infrastructures and their Consequences*. London: SAGE Publications.

Knorr Cetina K (1999) *Epistemic Cultures. How the Sciences Make Knowledge*. Cambridge and London: Harvard University Press.

Knorr Cetina K (2013) Presentation to Panel, Theorizing Numbers, paper presented at the *American Sociological Association annual meeting*. New York.

Kuner C, Cate F H, Millard C and Svantesson D J B (2012) The challenge of ‘big data’ for data protection. *International Data Privacy Law* 2(2): 47–49.

Lange A C, Lenglet M and Seyfert R (2018) On studying algorithms ethnographically: Making sense of objects of ignorance. *Organization*. DOI:10.1177/1350508418808230.

Latour B (1993) *We have never been modern*. New York: Harvest Wheatsheaf.

Lenglet M (2011) Conflicting codes and codings: How algorithmic trading is reshaping financial regulation. *Theory, Culture & Society* 28(6): 44 66.

Lenglet M (2019) Algorithmic finance, Its regulation, and Deleuzean Jurisprudence: A few remarks on a necessary paradigm shift. *Topoi. An International Review of Philosophy*. DOI:10.1007/s11245-019-09653-6.

Lenglet M and Taupin B (forthcoming) How to undo things with words? Regulation, transparency and the counter-performative effects of economics in the financial industry.

Lidskog R, Uggla Y and Soneryd L (2011) Making Transboundary Risks Governable: Reducing Complexity, Constructing Spatial Identity and Ascribing Capabilities. *AMBIO* 40(2): 111–120.

Lisboa P J (2013) Interpretability in Machine Learning – Principles and Practice. In: Masulli F, Pasi G and Yager R (eds) *Fuzzy Logic and Applications*. Cham: Springer, pp. 15-21.

Luhmann N (2008) *Law as a Social System*. New York: Oxford University Press.

MacKenzie D (2006) Is economics performative? Option Theory and construction of derivates markets. *Journal of the History of Economic Thought* 28(1): 29-55.

MacKenzie D (2018) Material Signals: A Historical Sociology of High-Frequency Trading. *American Journal of Sociology* 123(6): 1635-1683.

MacKenzie D (2019) How Algorithms Interact: Goffman’s ‘Interaction Order’ in Automated Trading. *Theory, Culture & Society* 36(2): 39–59.

MacKenzie D and Millo Y (2003) Constructing a Market, Performing Theory: The Historical Sociology of a Financial Derivatives Exchange. *American Journal of Sociology* 109 (1): 107–145.

Morris J W (2015) Curation by Code: Infomediaries and the Data Mining of Taste. *European Journal of Cultural Studies* 18 (4-5): 446-463.

Muniesa F (2014) *The Provoked Economy: Economic Reality and the Performative Turn*. London: Routledge.

Forbrukerrådet (2018): Deceived by design. How tech companies use dark patterns to discourage us from exercising our rights to privacy. Available at:

https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf (accessed 2 June 2019).

Orbach B (2012) What Is Regulation?. *30 Yale Journal on Regulation Online 1,* Arizona Legal Studies Discussion Paper No. 12-27. Available at SSRN: https://ssrn.com/abstract=2143385 (accessed 17 March 2019).

Parliament and the Council of the European Union (2016): 'Regulation (EU) 2016/679' (GDPR), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679 (accessed 17 March 2019).

Pasquale F (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.

Roberge J and Seyfert, R (2016) What are algorithmic cultures? In: Seyfert R and Roberge J (eds). *Algorithmic Cultures. Essays on meaning, performance and new technologies*. London: Routledge, pp.1-25.

Scherer M (2016) Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology* 29(2): 353-400.

Schmidt D C (2018) Google Data Collection. In: *Digital Content Next*, at https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf (accessed 17 March 2019).

Schweitzer D (2017) Die digitale Person: Subjektkonstruktionen im 'Recht auf Vergessenwerden'. *Österreichische Zeitschrift für Soziologie* 42(3): 237–257.

Seaver N (2014) Knowing algorithms, paper presented at *Media in Transition 8*, Cambridge, MA, http://nickseaver.net/papers/seaverMiT8.pdf (accessed 17 March 2019).

Seyfert R (2016) Bugs, Predations or Manipulations? Incompatible Epistemic Regimes of High-Frequency Trading. *Economy & Society* 45(2): 251-277.

Steinbrück P (2012): Vertrauen zurückgewinnen: Ein neuer Anlauf zur Bändigung der Finanzmärkte, working paper, September 2012, http://www.spdfraktion.de/system/files/documents/konzept_aufsicht_und_regulierung_finanzmaerkte.pdf (accessed 17 March 2019)

Steiner P (2017) Economy as Matching. Available at: https://halshs.archives-ouvertes.fr/halshs-01494492v2 (accessed 17 March 2019).

Wachter S, Mittelstadt B (forthcoming) A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*.

Weber M (1978) *Economy and society: an outline of interpretive sociology*. vol. 2. Berkeley et al.: University of California Press.

Yeung K (2018) Algorithmic regulation: A critical interrogation. *Regulation & Governance* 12: 505–523.