Digital Society (2022) 1:10
https://doi.org/10.1007/s44206-022-00011-5

ORIGINAL PAPER

Why AI is a Threat to the Rule of Law

Sebastian Rosengrün[1]

Received: 1 November 2021 / Accepted: 14 July 2022 / Published online: 9 August 2022

Abstract
This paper will argue that recent developments in AI technology and its role in digital capitalism threaten the rule of law. AI (or the companies who control it) promotes and monetizes free speech, political competition, and other aspects of democracy, while our societies have been shifting towards a "rule of code," i.e., a system in which source code is able to put meaningful restraints not only on any individuals and institutions within a society, but also on law and the State. Based on Lawrence Lessig's "Code is Law," this paper will draw a more elaborated picture of "regulating AI" according to which AI is not only something that is to be regulated but also something that actively regulates individual and institutional behavior. From this background, it will be argued that, given the interdependence of governments and big tech corporations, free and open societies need to regain control over source code and the critical digital infrastructure to avoid being regulated by private companies that develop, control, and promote AI.

Keywords Artificial intelligence · Regulation · Rule of law · Digital capitalism

1 Introduction

There is vivid debate on how to regulate AI. Many countries have recently proposed legal frameworks, most prominently the Artificial Intelligence Act proposed in 2021 by the European Commission as a regulatory framework for AI technology within the European Union. The debate on AI regulation, however, often underestimates that AI itself has regulatory effects on the legal system and thereby endangers the rule of law as a foundation of many contemporary states including all democracies—something that ought to be considered when discussing any regulatory attempts on AI technology. To be put briefly, this paper argues that AI technology is a threat to the rule of law and outlines paths of how to regain control.

✉ Sebastian Rosengrün
sebastian.rosengruen@code.berlin

[1] CODE University of Applied Sciences, Berlin, Germany

Section 2 will clarify the rule of law as a fundamental legal concept and differentiate between a substantive and formal understanding and show that the rule of law is necessary for any democracy to flourish. Section 3 builds on these definitions and introduces Lawrence Lessig's (2006) central thesis according to which source code, social norms, and the market have similar regulatory power as the law. Section 4 focuses on AI and its role in contemporary digital capitalism and argues that, as a result of Tech Exceptionalism and recent developments in Legal Tech, many Western societies are about to shift towards a rule of code, i.e., source code is about to become the main regulator of individual and institutional behavior that regulates all other regulators including law. Finally, Sect. 5 will suggest that the only answer to this problem is that free and open societies must regain control over source code to prevent being regulated by it. While not presenting an ultimate solution, it discusses a few hints at how this can be achieved. Especially the Chinese attempts toward digital sovereignty, together with China's controversial attempts toward the rule of law, will provide an insightful foil for comparison.

2 The Rule of Law

The rule of law is a fundamental legal concept according to which "law is able to impose meaningful restraints on the state and individual members of the ruling elite" (Peerenboom, 2002, p. 2; cf. Bellamy, 2016; Bingham, 2011). The European Commission for Democracy Through Law (Venice Commission) lists some core features of a rule of law (German: *Rechtsstaatlichkeit*; French: *Etat de droit*): (i) legal certainty, (ii) prevention of abuse (misuse) of power, (iii) equality before the law and non-discrimination, and (iv) access to justice (cf. Council of Europe, 2016). Some of those features go beyond how some legal scholars understand "rule of law." The debate distinguishes between a substantive and a formal understanding. Substantivists argue that the rule of law is somehow connected to morality, e.g., by guaranteeing access to human rights for everyone (cf. Bingham, 2011, p. 66–84). In contrast,"[u]nder the formal understanding, a society may properly claim fidelity to the rule of law even if its legal regime is substantively quite brutal" (Pettys, 2012, p. 114). The rule of law, here, "says nothing about how the law is to be made: by tyrants, democratic majorities, or any other way" (Raz, 2016, p. 80), neither does it say anything about what the law entails. A law discriminating against members of an ethnic or religious minority, for example, would violate feature (iii) presented by the Venice Commission (and contradict a substantivist understanding, e.g., proposed by eminent British judge Tom Bingham, cf. Bingham, 2011), but such a discriminating law does not contradict a formal understanding of the rule of law, as, e.g., proposed by Israeli philosopher Joseph Raz (2016): Discrimination, in this case, is not arbitrary, but "justified."[1]

While dictatorships and totalitarian regimes might invoke a (formal) rule of law, too, it is impossible for a democracy to flourish without it: The rule of law is a

[1] Not in any moral sense, of course, but in the legal sense of "acting according to *jus*" (Lat. "law").

necessary, but not a sufficient condition for democracy (cf. Bingham, 2011, p. 6). The concept of democracy, in this paper, is used in its most general sense, referring to "a method of collective decision making characterized by a kind of equality among the participants at an essential stage of the decision-making process" (Christiano & Bajaj, 2022). By challenging the rule of law, AI technology is a serious threat to democracy, too—at least indirectly: AI technology clandestinely undermines the foundation of any democratic society, while leaving some democratic decision-making processes untouched, at least on the surface level. People can still make free decisions about their governments and their futures, as long as their free decisions will not challenge the (commercial) interests of companies controlling AI (and dictators can still tyrannize their populations by law, as long as they will not challenge those interests either.)

By claiming that AI is a threat to the rule of law, this paper argues for a shift of perspective when discussing regulation and societal risks of AI. In order to elaborate my argument, it is necessary to broaden the concept of "regulating AI" by building upon American legal scholar Lawrence Lessig's central claim that "Code is Law" (2006, p. 1).

3 Towards a Broader Picture of Regulation

In his groundbreaking work *Code and Other Laws of Cyberspace* (Lessig, 1999), and its updated version *Code: Version 2.0* (Lessig, 2006), Lessig describes the regulatory power of source code over the digital sphere (what he calls "cyberspace"). This is followed by an in-depth analysis of regulation. For the offline world, Lessig (2006, pp. 120–137) identifies four main regulators of human and institutional behavior: market, norms, architecture, and laws. While humans are free to make their own life decisions, they are often prevented from doing what they want, e.g., because they do not have enough money to afford their wishes (=regulation by the market), they are afraid to be frowned upon by their friends and neighbors (=regulation by social norms), there are physical or technical obstacles (=regulation by architecture), and, of course, there are many legal restrictions (=regulation by law). The same regulators also apply to cyberspace where source code is the digital equivalent of architecture.

How a website or an app is designed (and design is always implemented in its source code) regulates the behavior of its users. If a dating platform, for example, requires users to upload a profile picture, then their success will depend on how they look like. If their users must select favorite books, movies, or sexual preferences from a list, then the default answers from those lists will affect their choices for a potential date—which would be different if they would ask their users to fill in other categories. Also in the offline world, how things have been designed regulates what people can and cannot do, how they perceive the world, and how they socially interact. Thaler et al. demonstrate how decision-makers act within an "environment where many features, noticed and unnoticed, can influence their decisions" (2010) and how those environments are created by so-called choice architectures (see also Thaler & Sunstein, 2008; Verbeek, 2005). From an ethical point of view, technology ought not to be seen as just a neutral tool—an insight to be found, e.g., in the works of Karl Marx, Ernst Kapp, Hannah Arendt, and made explicit, among others, by the historian of technology Melvin Kranzberg who claims—within his influential, so-called Kranzberg laws—that "[t]echnology is neither good nor bad; nor is it neutral" (Kranzberg, 1986, p. 545; cf. Heichele, 2020; Loh, 2019, pp. 205–207; Rosengrün, 2021, pp. 114–120). Lessig conveyed this thesis into the debate on digital technologies:

> Codes constitute cyberspaces; spaces enable and disable individuals and groups. The selections about code are therefore in part a selection about who, what, and, most important, what ways of life will be enabled and disabled. (Lessig, 2006, p. 88)

The first conclusion to draw from this is that "Regulating AI" is a two-sided concept: While scholars often focus on how AI can be regulated by legislation, it is highly underestimated that source code is a regulator itself even though there has been a lot of research on the social implications of AI and big data, most of it related to algorithm-based decision-making, targeted advertising, and digital capitalism (cf. Fry, 2019; Mau, 2019; O'Neil, 2017; Staab, 2019; Zuboff, 2019). Social implications are often presented as an undesirable application of a technological tool in the hands of malicious agents (companies, governments, etc.). Zuboff, e.g., wants to "hunt the puppet master, not the puppet" (2019, p. 14), suggesting that AI is only problematic because it is abused for behavior prediction and control in surveillance capitalism (see Sect. 3). This slogan appears to be convincing, but completely ignores the regulating power of AI technology (=regulation by code, according to Lessig): Algorithms have tremendous social implications (and regulate human and institutional behavior) if they were not used to exploit "every aspect of every human's experience" (Zuboff, 2019, p. 9) and decision-making based on them was not racist, sexist, or otherwise inhumane.[2] Whether a person will find a job, receive a loan, or rent an apartment is nowadays regulated by a few lines of source code, also what music they listen to, what books they read, and—at least some people believe that—what political party they vote for. Where regulation by AI tools (as fallible or imprecise as they are, see Sect. 4) is not practically forced upon everybody (e.g., when applying for a loan or rent), it at least requires awareness and technological understanding, but also an active decision by the individual, to avoid them.

Understanding that source code is a regulator of human behavior itself is crucial to gain a more nuanced picture of regulation. Its offline equivalent, architecture, is often overruled by legislation and jurisdiction, i.e., by law-making and the interpretation of the law by courts. Law, in any country that has established the rule of law, is the regulator that regulates all other regulators: Beyond the theoretical debate introduced in Sect. 2, rule of law (at least according to the formal understanding of the notion) essentially means that the other three regulators (market, norms, and architecture) can only unfold their regulating power over spheres that are not regulated by law. While it depends on a country's legal tradition, whether there is a

[2] A problematic misconception in this context is to assume that algorithms are racist, sexist, or otherwise inhumane. Institutions (people, companies, governments, etc.) who use algorithms for decision-making are (cf. Rosengrün, 2021, pp. 90–102).

stronger focus on jurisdiction (in common law countries) or on legislation (in civil law countries), law usually regulates the market (e.g., by what goods are legal and what prices vendor could charge for them) and architecture (e.g., building codes require public buildings to become wheelchair-accessible) and while social norms can have a certain influence on legislation and jurisdiction, law has a significant influence on social norms, too.

The second conclusion to draw from this picture of regulation is that human and institutional behavior is never unregulated. If there is no regulation by law, other regulators provide rules (written or unwritten) that will affect life choices. If, for example, health insurance was not regulated by law, it would only be affordable for a significantly smaller group of people than today, and those who suffer from chronic diseases (or have any sort of critical genetic disposition) would not be able to sign a policy at all. In other words, without legal regulation, the market (driven by profit-maximizing insurance companies) would take over the role of law and would regulate who will receive an offer for health insurance and how much they need to pay for it. There is no law forbidding anyone to sign a health insurance contract, there would undoubtedly be a social norm encouraging everyone to do so, and there are no obvious architectural constraints. But people who cannot afford health insurance will still have very limited health care choices.

Lessig draws the same picture of regulation for the digital sphere: the Internet, in its beginning, was acclaimed by many of its users as a sphere of freedom which has not and cannot be regulated by the state. This belief is symbolically represented in John Perry Barlow's widely known *Declaration of the Independence of Cyberspace* from which Lessig quotes:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. (Barlow, 1996; cf. Lessig, 2006, pp. 1-8)

Because of the absence of regulation by law in the early days of the internet, source code soon became the most important regulator of the digital sphere, culminating in Lessig's dictum "Code is Law" (see above). Confronted with the objection that, for many legal scholars, the concept of regulation is strictly limited to state regulation (= regulation by law), Lessig simply points out that this is precisely why a broader picture of regulation is necessary (cf. Lessig, 2006, pp. 136–137; Hildebrandt, 2018). What certain groups, institutions, and enterprises currently do has the same regulating effects on human and institutional behavior (they control it by some sort of—written or unwritten—rules) as what the state does when it regulates human and institutional behavior by law, which is why what those groups, institutions, and enterprises do should also be viewed as regulation.

When thinking about how to regulate a technology, one needs to be aware that technologies like AI are regulators themselves that unfold their regulating power whenever there is no regulatory framework provided by the State. Source code in general and AI technology in particular, however, are not only a regulator of human and institutional behavior among others, but also took over from law the role of the regulator that regulates all other regulators, including law, as will be discussed in the next section.

4 Digital Capitalism and the Rule of Code

That AI regulates all other regulators essentially means that societies have shifted (or are currently shifting) from "rule of law" towards "rule of code." While this might sound like a controversial claim at first, some examples will shed light on the tremendous regulatory power of current AI technology (respectively the companies who control its source code).

If Google or Amazon change their search algorithms, they regulate the market as exemplified by grocery suggestions. A few lines of source code decide which products and shops billions of people will find and what they will be paying for it. With announcing mobile-first indexing in 2020—something they have been working on for many years (cf. Mueller, 2020)—Google tacitly announced a significant change of market regulation: it suddenly became difficult for small businesses, restaurants, and craftspeople to be found by their potential customers unless they understood the importance and have the financial resources to implement a mobile-friendly version of their website. Amazon's algorithms, in determining what products will be displayed first, influence the sales revenue of thousands of third-party vendors, but also the prices people pay and the products they find. It has similar effects as if supermarkets reorganize their shelves to put other products on display, just that Amazon's market dominance is much bigger than that of any supermarket chain in the offline world. Not only because of their regulatory power over the market, Google (and others) influences social norms, too. Publishers focus on SEO in order to achieve a higher Google rank with their articles, which immediately affects how articles are written: Many journalists choose to implement the right keywords rather than to write proper, well-researched stories that will not be found on Google. Empirical studies show how social media like YouTube, Facebook, Instagram, and Tiktok influence, change, and generate social norms and affect social behavior (cf. Turkle, 2015, 2017), not even to mention the effects on the understanding of human nature and social life imposed on us by smart home devices, social robots, and virtual realities.

To clarify a possible misunderstanding: tech corporations like Google and Amazon *have to* decide what shops, websites, and products they display at "eye level." Their algorithms would also regulate markets and social norms if products on display were always the ones with highest quality, fairest production chain, least environmental damage, and most affordable price. This paper does not criticize any particular regulation, but rather the fact that such regulatory power is executed by a small group of companies within the monopolistic logic of what scholars call "digital capitalism" (Betancourt, 2015; Schiller, 1999, 2014; Staab, 2019) that has, most famously, been revealed by venture-capitalist Peter Thiel (cf. Thiel & Masters, 2014).

In the words of Mark Zuckerberg, this regulatory power could be described as follows: "Facebook is more like a government than a traditional company, [and] we're really setting policies" (quoted after Foer, 2017). How problematic this is becomes clearer when looking at how AI (respectively the tech corporations who control AI) is transforming contemporary societies more and more into a rule of code. While regulation by AI is manifold, recent developments in Legal Tech and the widespread belief in Tech Exceptionalism and its resulting concentration of power are the two most significant threats to the rule of law and require thorough explanation in the following paragraphs.

Legal Tech refers to any "algorithm-based technology in legal matters" (Buchholtz, 2020, p. 176). This involves, among other things, algorithm-based decision-making in law-enforcement and jurisdiction, the debate on electronic personhood, and the effects smart contracts and algorithm-based business models have on the legal system (cf. de Bruyne & Vanleenhove, 2021; Hildebrandt, 2018; Wischmeyer & Rademacher, 2020). Algorithms already play a big role in US jurisdiction, e.g., in setting bail, calculating prison sentences, and deciding about early releases (cf. Jung et al., 2017), and in law enforcement (cf. Rademacher, 2020). Legal tech enterprises (in Germany, e.g., flightright.de, geblitzt.de, and wenigermiete.de) offer applications to handle minor legal cases "such as disputes over flight compensation or traffic accidents" (Buchholtz, 2020, p. 179) (semi-)automatically, which could be seen as a chance to make legal protection available to anyone but might also overburden legal systems with a significant increase in minor lawsuits: Legal protection in minor cases (like speeding tickets) is a lucrative business model for legal tech enterprises leeching on state compensation (= taxpayer's money) for legal fees. Google's chief economist Hal Varian, already in 2010, pointed out how "computer-mediated transactions […] [f]acilitate new forms of contract" (Varian, 2010, p. 2). Today, smart contracts are written, observed, and enforced by the support of AI technology. Other concrete legal challenges include the debate on liability of autonomous machines, copyright, and taxation.

All those challenges are currently debated with a strong tendency towards tech exceptionalism, i.e., the political view that digital technologies "have been powerful engines for economic growth, personal expression and disruptive change" (Thune, 2013, cf. Betancourt, 2015; Doctorow, 2020; Jones, 2018; Popiel, 2018) and big tech corporations, therefore, require considerate legislation and jurisdiction, especially in regards to competition law and anti-trust, but also data protection and tax law. Tech exceptionalism is the result of heavy lobbyism paired with a public debate being awestruck by the rapid development of digital technologies over the last decades. Morozov describes this phenomenon by introducing the concept of a "Surveillance Dividend," referring to "the idea that the Internet of Things and Big Data and the inevitable disruption of the entire universe by a handful of Californian start-ups will yield economic abundance, political emancipation, universal prosperity" (2014). Considerate legislation and jurisdiction with regards to AI and related technologies are a worthwhile investment because those technologies are presented and viewed—here in the words of Google officials Eric Schmidt and Jared Cohen—as bringing "untold benefits to the citizens of the future" (Schmidt & Cohen, 2013, p. 35).

Remarkably, also a significant part of contemporary AI criticism feeds into tech exceptionalism and the presented threat to the rule of law. To elaborate on this, it is helpful to distinguish between apocalyptic and realistic risks currently debated with regard to AI. Apocalyptic risks are often expressed in connection with Artificial

General Intelligence, the technological singularity and posthumanism, and include, e.g., the fear that an evil superintelligence will rise to power, violently establish a dictatorship, and subdue (or even kill) humanity. While those far-fetched scenarios—often pushed by tech entrepreneurs like Elon Musk and Ray Kurzweil—should not be anybody's concern (cf. Rosengrün, 2021, pp. 67–81), their widespread discussion not only causes great uncertainty in the public debate on the nature of AI, but also influences the agendas of lawmakers and courts accordingly. Among the realistic risks feeding into tech exceptionalism, there is, most prominently, the criticism by Shoshana Zuboff who argues that AI is the most important means of production in "surveillance capitalism"—a "new instrumentarian power that asserts dominance over society and presents startling challenges to market democracy" (Zuboff, 2019, preface). AI is used to ultimately control human behavior by predicting precisely how humans behave and how manipulating the input variables for human behavior will affect behavioral outcomes. Tech corporations, thereby, endanger the "Right to the Future Tense" (Zuboff, 2019, pp. 328–347), i.e., the fundamental idea that every human being should have the right to make their own life choices—a core value of any democratic society. However, it is questionable that machine learning in combination with big data will ever be accurate enough to achieve such an ultimate behavior prediction. While Zuboff might be right in assuming that this is the propagated goal of surveillance capitalists, it is naïve to assume that human psychology could be accurately predicted by feeding an AI with superficial data points (cf. Doctorow, 2020; Vinsel, 2021; Weizenbaum, 1976).

Presenting AI tools as a threat to free democratic decision-making, however, makes this technology appear much more powerful than it is (cf. Doctorow, 2020; Weizenbaum, 1976). While AI tools can be used to analyze and predict human behavior to a certain extent, it is important to note that this does not require magicians specialized in "sorcerous acts of mind control" (Doctorow, 2020): If a person constantly searches for advice on how to buy a car, anybody could conclude that this person might be a potential customer for a company selling cars. But the business of online advertisement, similar to book and movie recommendations, relies on humans believing that algorithms have this sort of magical powers and could be used (or abused, given Zuboff's criticism) to confront them with the factually best products (be it books, cars, or political news or election campaigns).

Especially the widespread belief in AI's magic powers (no matter whether it is justified or not) strengthens the public belief in tech exceptionalism and leads to a "metric society" (Mau, 2019) in which the social and personal sphere of individuals will be quantified, measured, recorded, and calculated—even though it is questionable whether the analysis of this data does make any sense. A prominent—as well as shocking—example of a democratic institution blinded by AI's magical powers is to be found in the "Smart City Charta," issued 2017 by the German Federal Ministry of the Environment, Nature Conservation and Nuclear Safety and the German Federal Ministry of the Interior, Building and Community. In this document, they give a platform to Finnish futurist Roope Mokka's vision of a "[p]ost-voting society" in which "behavioral data can substitute democracy as the societal feedback system" (BBSR and BMUB, 2017, p. 43, my own translation). A similarly shocking vision about the future of democracy is expressed by computer scientist Alex Pentland who argues for a mathematical, predictive science of society that "[…] has the potential to dramatically change the way government officials, industry managers, and citizens think and act" (2014, p. 191; cf. Zuboff, 2019, pp. 416–444).

From the background of tech exceptionalism, code regulates law because algorithms are so dominant in our everyday life that not only private people, companies, and NGOs, but also political leaders and whole state infrastructures are dependent on the services Google, Amazon, Facebook, Apple, and Microsoft (the so-called GAFAM companies[3]) offer to them and therefore heavily affected by their lobbyism. In September 2020, for example, Facebook overtly and publicly uses their market power as a threat to European legislators to influence data protection legislation (cf. Gilbert, 2020). This paper suggests that controlling a technology equals controlling the people and institutions relying on this technology. In a hypothetical situation in which only a few companies produce hammers, but everybody (including political institutions) feels a desperate need to drive nails into their walls, those companies would have complete control over who gets to buy a hammer and what price they will be paying for it. Western state infrastructure, political leaders, and parties rely on GAFAM's AI technology in military and surveillance (cf. Doctorow, 2020; Staab, 2019), public administration and bureaucracy, and, also, political campaigning. Due to this dependency, AI is first and foremost a threat to the rule of law, whereas Western societies shift towards a rule of code.[4]

Despite their recent efforts to regulate AI, digital markets, digital services, and data governance, this threat also applies to the European Union. While discussing concrete policy proposals (like the Artificial Intelligence Act from 2021 and the White Paper on which this regulatory attempt is based) goes beyond the scope of this paper, there are general tendencies that ought to be mentioned here: Both documents start with the assumption that AI "is a fast evolving family of technologies that can bring a wide array of economic and societal benefits across the entire spectrum of industries and social activities" (European Commission, 2021, p. 1), echoing instead of rejecting tech exceptionalism. The European Commissions, for example, concretely suggests equipping "law enforcement authorities with appropriate [AI] tools to ensure the security of citizens" (European Commission, 2020, p. 2), i.e., predictive analysis by machine learning and biometric surveillance technologies (for which there are detailed descriptions of potential use cases). The proposal also explicitly states that this "Regulation shall not apply to AI systems developed or used exclusively for military purposes" (European Commission, 2021, p. 39) which are discussed (in a similar spirit of tech exceptionalism) in separate documents. While addressing concerns regarding AI in connection with a substantivist

[3] Google here refers to Alphabet Inc., Facebook to the recently firmed Meta Platforms Inc.

[4] While this paper addresses the issue from a Western (or even European) perspective, it goes without saying that the concept of a Western perspective in itself is rather fuzzy and the presented interdependence between governments and tech corporations is, of course, not only a Western phenomenon. See Sect. 5 for a discussion of the contrasting Chinese perspective.

understanding of the rule of law,[5] the Ad Hoc Committee on Artificial Intelligence by the European Council also suggests that "[w]hen used responsibly, AI systems can be used to increase the efficiency of governance, including legal institutions such as the courts, as well as law enforcement and public administrations" (Council of Europe, 2020, p. 12).

Zuboff prominently argues that "privacy policies are more aptly referred to as *surveillance policies*" (Zuboff, 2019, p. 250, emphasis in original), i.e., agreeing to the privacy policies of a service does not protect one's privacy, but just to the contrary allows the service provider to use surveillance technology according to their specific terms and conditions. There is a similar argument to be made about policy proposals on the regulation of AI (or any other) technology: Providing such a detailed legal framework for their questionable applications does not outlaw those applications, but just to the contrary, defines concrete conditions under which corporations are allowed and even encouraged (funded by the state) to develop those questionable tools. Most questionable AI tools (including algorithm-based decision-making processes) are developed by those big corporations the proposals pretend to regulate. This leads to an even stronger dependence both with regards to law-making and especially law enforcement and, consequently, to a further undermining of the rule of law (in its formal understanding).

As paradoxical as this might sound, at least on the surface level, this threat to the rule of law seems to be compatible with modern democracy—even though, without the rule of law, what remains from democracy is a disempowered and empty shell (see Sect. 2). For Western tech corporations, the only reason to engage in digital capitalism appears to be the money there is in it. The GAFAM companies aim to control/own those markets not because they follow a broader political agenda but instead seem to aim for capitalist profit only. There are no indicators to believe that tech companies would actively work against democracy in the foreseeable future. Just to the opposite: the money in what Zuboff calls the "behavioral futures markets" (2019, p. 10) (i.e., the market of behavior predictions based on machine learning and big data) stems from targeted advertisements paid for by both commerce and political parties, believing in AI's magic powers and the benefits of a metric society, while they are competing for customers and voters. Even in a "post-voting society" (as envisioned in a document issued by the German government, see above), a societal feedback system is only necessary as long as there is political competition and as long as political parties believe that accurate AI-based behavior predictions are as accurate as promoted by tech corporations.

Within contemporary democracies, the relevant platform providers will profit as long as political competitors are willing to pay for manipulating voter behavior and the spread of fake news (see, e.g., the Cambridge Analytica scandal, Wylie, 2019), but also simply for political campaigning. Some form of political competition and

[5] They mostly address the problems of discrimination and inequality in algorithm-based decision-making which are not directly addressed within this paper, but are widely debated as threats to democracy, (e.g., in O'Neil, 2017; Fry, 2019). See also Rosengrün, 2021, pp. 133–152.

"democratic" decision-making, therefore, will always be in their commercial interest. Ironically, this profit is often paid for by tax money. Big tech corporations usually even market themselves as "an important tool for the freedom of expression" (Gilbert, 2020, quoting a Facebook spokesperson), which makes sense as providing this tool is what they monetize on. Political competition (which they also monetize on) and the slowness of democratic decision-making even help the GAFAM companies to flourish, and no matter what political parties will be elected, they are powerful enough to ignore state legislation and jurisdiction.

5 Hints at How to Regain Control

As outlined in Sect. 2, the rule of law is a necessary foundation of any democratic, free, and open society. Individual and institutional behavior, however, is regulated not only by law but also by source code, social norms, and the market, as shown in Sect. 3. When discussing recent AI technology, this paper concluded that source code is about to take over from law the role of being the regulator regulating the other regulators. This phenomenon was described as a shift toward a rule of code culminating in the central argument that AI is a threat to the rule of law (Sect. 4). While this paper cannot provide an in-depth solution, becoming aware of this threat already is essential to regain control. However, since awareness often does not lead to concrete action, especially when it is unclear what appropriate action should look like, this paper shall conclude with a few general hints at how to regain control.

To break the regulatory power of contemporary AI, democratic societies need to regain control over source code, according to the presented broader picture of regulation (see Sect. 3). For this, it is necessary to establish digital sovereignty (cf. Pohle & Thiel, 2021), i.e., societies need to invest in their own digital infrastructure independent from the GAFAM companies.

A controversial example of how to establish such an independent digital infrastructure is China (cf. Heilmann, 2018; Lee, 2018). China currently puts a substantial financial and political effort into building independent operating systems, chip technology, storage media, and internet infrastructure in order to become independent from American tech corporations. It does what is necessary for any sovereign country in the long run: trying to stay in control over what things regulate to prevent being regulated by them. It is less known that China has put similar efforts into establishing the rule of law in the last decades, at least in the formal understanding of the notion (see Sect. 2). Legal scholar Randall Peerenboom highlights "China's march toward rule of law" (2002, p. 6) as a "remarkable progress," transitioning from rule by law into "a system in which law is able to impose meaningful restraints on the state and individual members of the ruling elite, as captured in the rhetorically powerful if overly simplistic notions of a government of laws, the supremacy of the law, and equality of all before the law" (Peerenboom, 2002, p. 2). Of course, China's efforts toward rule of law ought to be discussed with a skeptical distance towards their political goals which is why it is “difficult for many modern Westerners in particular to imagine rule of law being embedded in a nonliberal context” (Peerenboom, 2002, p. 27): Mentioning the Human Right Situation in Xianjing, and how China uses their digital sovereignty and technological advances there (and elsewhere, e.g., by building their infamous Social Credit System) to surveil, control, manipulate, and oppress their citizens, conflicts with a more substantivist understanding of the rule of law in China.[6] But while the primary goal of implementing the rule of law in China is “state-strengthening rather than the protection of individual rights” (Peerenboom, 2002, p. 27), the Chinese legal reforms, starting in the 1980s, also provide Chinese citizens protection against arbitrary executive decisions by corrupted local authorities.

China’s attempts to reach digital sovereignty and state-strengthening by focusing on the rule of law should be seen as a best practice for what every free and open society needs to aim for. However, how China uses its digital infrastructure is, of course, a worst practice. While it is essential for any sovereign society to preserve the rule of law by controlling its digital infrastructure, it is essential for every free and open society to ensure that its digital infrastructure *will not* be abused to surveil, control, manipulate, and oppress humans living in or out of that society. The only effective guarantee that nobody will ever abuse digital infrastructures is to build/design them such that they *cannot* be abused: This includes (but is not limited to) a strong focus on open-source software, data parsimony, security, and net neutrality, especially in public infrastructure, and, from a legal perspective, strict enforcement of taxation law, competition law, and anti-trust regulation for tech corporations. Another important step towards empowering people is an education system focussing on “technoliteracy” (Pullen et al., 2010) and humanism—to enable people to understand what digital technologies are and to enable people to use this knowledge to make informed critical judgments about those technologies and their social impacts. This would also mean to demystify tech exceptionalism and the magical powers of AI, especially with regards to behavior predictions, and a broad societal understanding that AI is “just” mathematics executed on electronic circuits (see Sect. 4).

While recent European attempts to build their own digital infrastructure (e.g., the GAIA-X project) are an important step towards independence from American tech corporations, the problem with American tech corporations like the GAFAM companies is not that they are American, but that they are, as this paper suggests, powerful enough to threaten the rule of law both in America and Europe and anywhere else. Building European versions of powerful, monopolistic companies monetizing on surveillance and AI-based behavior predictions (as sometimes suggested) will be counterproductive when, as argued above, giving people control over what regulates them must be the goal of any free and open society.

Funding Open Access funding enabled and organized by Projekt DEAL.

[6] For a controversial analysis of China’s more recent efforts to establish the rule of law, (c.f. Zhang & Ginsburg, 2019; Cohen, 2019).

Data Availability I do not analyze or generate any datasets, because my work proceeds within a theoretical and mathematical approach.

Declarations

Conflict of Interest The author declares no competing interests.

References

Barlow, J. P. (1996, February 8). *A declaration of the independence of cyberspace*. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

Bellamy, R. (Ed.). (2016). *The rule of law and the separation of powers*. Routledge.

Betancourt, M. (2015). *The critique of digital capitalism: An analysis of the political economy of digital culture and technology*. Punctum Books.

Bingham, T. (2011). *The rule of law*. Penguin.

Buchholtz, G. (2020). Artificial intelligence and legal tech: Challenges to the rule of law. In T. Wischmeyer & T. Rademacher (Eds.), *Regulating artificial intelligence* (pp. 123–142). Springer.

Bundesinstitut für Bau-, Stadt- und Raumforschung (BBSR) & Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (BMUB) (Eds.). (2017). *Smart city charta: Digitale transformation in den Kommunen nachhaltig gestalten*. https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/bauen/wohnen/smart-city-charta-langfassung.pdf?__blob=publicationFile&v=7 (last access: 29 Apr 2021). Still available: https://www.smart-city-dialog.de/wp-content/uploads/2019/12/smart-city-charta-langfassung.pdf (originally published under ISBN: 9783879942039).

Christiano, T., & Bajaj, S. (2022). Democracy. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy* (Spring 2022). Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/spr2022/entries/democracy/

Cohen, J. A. (2019). Law's relation to political power in china: A backward transition. *Social Research: An International Quarterly*, *86*(1), 231–251. https://muse.jhu.edu/article/725995

Council of Europe (Ed.). (2016). *Rule of law checklist* (CDL-AD(2016)007rev). European Commission for democracy through Law (Venice Commission). https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2016)007-e

Council of Europe (Ed.). (2020). *Feasibility study* (CAHAI(2020)23). Ad hoc committee on Artificial Intelligence (CAHAI). https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da

de Bruyne, J., & Vanleenhove, C. (Eds.). (2021). *Artificial intelligence and the law*. Intersentia.

Doctorow, C. (2020, August 26). How to destroy surveillance capitalism. *OneZero*. https://onezero.medium.com/how-to-destroy-surveillance-capitalism-8135e6744d59

European Commission (Ed.). (2020). *White paper on artificial intelligence: A European approach to excellence and trust* (COM(2020)65final). https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

European Commission (Ed.). (2021). *Proposal for a regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts* (2021/0106(COD)). https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

Foer, F. (2017, September 19). Facebook's war on free will. How technology is making our minds redundant. *The Guardian*. https://www.theguardian.com/technology/2017/sep/19/facebooks-war-on-free-will

Fry, H. (2019). *Hello world: How to be human in the age of the machine*. Black Swan.

Gilbert, D. (2020, September 21). Facebook says it will stop operating in Europe if regulators don't back down. *Vice*. https://www.vice.com/en/article/889pk3/facebook-threatens-to-pull-out-of-europe-if-it-doesnt-get-its-way

Heichele, T. (2020). Das Spannungsfeld von Mensch, Technik und Natur aus Sicht der Philosophie. Von Ackerbau und Viehzucht zum Anthropozän. In T. Heichele (Ed.), *Mensch—Natur—Technik. Philosophie für das Anthropozän* (pp. 47–66). Aschendorff.

Heilmann, S. (2018). *Red swan: How unorthodox policy-making faciliated China's rise*. The Chinese University Press.

Hildebrandt, M. (2018). Algorithmic regulation and the rule of law. *Philosophical transactions of the royal society A: Mathematical, physical and engineering sciences*, 376(2128). https://doi.org/10.1098/rsta.2017.0355

Jones, M. (2018). Does technology drive law? The dilemma of technological exceptionalism in cyberlaw. *Journal of Law, Technology & Policy*, *2*(Fall 2018), 249–284.

Jung, J., Concannon, C., Shroff, R., Goel, S., & Goldstein, D. G. (2017). *Simple rules for complex decisions*. Social Science Research Network. https://papers.ssrn.com/abstract=2919024

Kranzberg, M. (1986). Technology and history: 'Kranzberg's laws.' *Technology and Culture, 27*(3), 544. https://doi.org/10.2307/3105385

Lee, K.-F. (2018). *AI superpowers: China, Silicon Valley, and the new world order*. Houghton Mifflin Harcourt.

Lessig, L. (1999). *Code and other laws of cyberspace*. Basic Books.

Lessig, L. (2006). *Code* (version 2.0). Basic Books.

Loh, J. (2019). *Roboterethik: Eine Einführung*. Suhrkamp.

Mau, S. (2019). *The metric society: On the quantification of the social*. Polity Press.

Morozov, E. (2014, July 30). Like clueless guinea pigs. *FAZ.NET*. https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/digital-surveillance-like-clueless-guinea-pigs-13070758.html

Mueller, J. (2020, March 5). Announcing mobile first indexing for the whole web. *Google Search Central Blog*. https://developers.google.com/search/blog/2020/03/announcing-mobile-first-indexing-for

O'Neil, C. (2017). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Penguin Books.

Peerenboom, R. P. (2002). *China's long march toward rule of law*. Cambridge University Press.

Pentland, A. (2014). *Social physics: How social networks can make us smarter*. Penguin.

Pettys, T. (2012). Judicial retention elections, the rule of law, and the rhetorical weakness of consequentialism. *Buffalo Law Review*, *60*(1), 69. https://digitalcommons.law.buffalo.edu/buffalolawreview/vol60/iss1/3

Pohle, J., & Thiel, T. (2021). Digital sovereignty. In B. Herlo, D. Irrgang, G. Joost, & A. Unteidig (Eds.). *Design, 54*(1), 47–68. transcript Verlag. https://doi.org/10.14361/9783839457603-003

Popiel, P. (2018). The tech lobby: Tracing the contours of new media elite lobbying power. *Communication, Culture and Critique, 11*(4), 566–585. https://doi.org/10.1093/ccc/tcy027

Pullen, D. L., Gitsaki, C., & Baguley, M. (Eds.). (2010). *Technoliteracy, discourse, and social practice: Frameworks and applications in the digital age*. Information Science Reference.

Rademacher, T. (2020). Artificial intelligence and law enforcement. In T. Wischmeyer & T. Rademacher (Eds.), *Regulating artificial intelligence* (pp. 225–254). Springer.

Raz, J. (2016). The rule of law and its virtue. In R. Bellamy (Ed.), *The rule of law and the separation of powers* (pp. 77–94). Routledge.

Rosengrün, S. (2021). *Künstliche Intelligenz zur Einführung*. Junius.

Schiller, D. (1999). *Digital capitalism: Networking the global market system*. MIT Press.

Schiller, D. (2014). *Digital depression: Information technology and economic crisis*. University of Illinois Press.

Schmidt, E., & Cohen, J. (2013). *The new digital age: Reshaping the future of people, nations and business*. Knopf.

Staab, P. (2019). *Digitaler Kapitalismus. Markt und Herrschaft in der Ökonomie der Unknappheit*. Suhrkamp.

Thaler, R. H., Sunstein, C. R., & Balz, J. P. (2010). *Choice architecture*. Social Science Research Network. https://papers.ssrn.com/abstract=1583509

Thaler, R., & Sunstein, C. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. Yale University Press.

Thiel, P., & Masters, B. (2014). *Zero to one: Notes on startups, or how to build the future.* Crown Business.

Thune, J. (2013, June 18). *Old regulations inhibit new technologies*. The Hill. https://thehill.com/opinion/op-ed/306377-old-regulations-inhibit-new-technologies

Turkle, S. (2015). *Reclaiming conversation: The power of talk in a digital age*. Penguin.

Turkle, S. (2017). *Alone together: Why we expect more from technology and less from each other*. Basic Books.

Varian, H. R. (2010). Computer mediated transactions. *American Economic Review, 100*(2), 1–10. https://doi.org/10.1257/aer.100.2.1

Verbeek, P. -P. (2005). *What things do: Philosophical reflections on technology, agency, and design*. Pennsylvania State University Press.

Vinsel, L. (2021, February 1). You're doing it wrong: Notes on criticism and technology hype. *Medium.* https://sts-news.medium.com/youre-doing-it-wrong-notes-on-criticism-and-technology-hype-18b08b4307e5

Weizenbaum, J. (1976). *Computer power and human reason*. Freeman.

Wischmeyer, T., & Rademacher, T. (Eds.). (2020). *Regulating artificial intelligence*. Springer.

Wylie, C. (2019). *Mindf*ck: Cambridge Analytica and the plot to break America*. Random House.

Zhang, T., & Ginsburg, T. (2019). China's turn toward law. *Virginia Journal of International Law, 59*(2), 306–389.

Zuboff, S. (2019). *The age of surveillance capitalism. The fight for a human future at the new frontier of power*. Profile.