

# Facebook: The criminal bank of social capital

- I like?



**Lisa Golla**  
**lgolla@uni-osnabrueck.de**  
**983700**



An essay for the course Digital Capitalism, Big Data and AI  
Paul Schütze, M. Sc.  
SS 2022

Cognitive science  
University Osnabrück  
Germany, Osnabrück  
September 2022

# Facebook: The criminal bank of social capital

## I. INTRODUCTION

Digital capitalism depends on the appropriation and exploitation of private data. Due to the fact that the data is collected by monitoring user's behavior, it has been defined as surveillance capitalism. A further key aspect is the monetization of the collected data in order to use that information for targeted marketing and advertising. What can be observed during that process is a rise of interest concerning digital platforms in governing the user's behavior to maximize profit [1], [2].

Facebook is one of the most representative and successful companies of digital capitalism, and manifests clearly a structure of government which will be shown and reasoned. During the course of this essay it will also be presented that in addition to the feature of governance, that is a characteristic element also for other digital platforms, Facebook's power to govern relies on the monopolistic control over so-called social capital. Moreover, as will be elaborated, the character of that bank of social capital reveals itself to be exploitative, monopolistic, and unscrupulous. Whereas Facebook's concentration of power can be considered as alarming, there is also another aspect which deserves some attention. Specifically, there is evidence that Facebook is extracting the private data of the user's in abusive and unlawful ways. While the process can be described as deliberate criminal strategy, it manifests in data crimes being defined in more detail section ?? In Particular, it will be discussed what patterns can be observed in the big tech companies, as well as why there is so little done yet connected to the challenges in this field emerging when trying to act against the crimes of digital capitalism. In parallel, the resulting structural effects are pointed out. The last part of the essay stresses the imperilment the commitment of data crimes and the government of social capital are causing.

## II. FACEBOOK AS A GOVERNING BANK OF SOCIAL CAPITAL

Fundamentally, the approach which will be explained in this paragraph considering Facebook as a bank of social capital is based on the paper "Facebook Rules: Structures of Governance in Digital Capitalism and the Control of Generalized Social Capital" by Ori Schwarz.

The first question in place is the following. Why is Facebook interested in governing? The answer is based on the shift in forms of capitalistic agglomeration. There is a rise of immaterial biopolitical production which denotes the production of the social life containing economic, political, and cultural aspects. Facebook is monetizing the produced social interaction into interpretable data which is captured and sold to advertisers. Basically, this describes the essence of Facebook quite well since 98.3% of the revues in 2017 have their roots in targeted

advertising [1]. What can be inferred from the monetizing process is that human interactions are serving as sources of profit. It is needless to say that users are active. Thereby, their individual behavior is able to influence the profit. In the context of surveillance capitalism as Zuboff [3] is defining it, one can say that Facebook is not only governing, rather it also manages and controls the social world for the purpose of maximizing profit. Moreover, the user is more than passive raw material. Rather, users become active in producing profit and thereof a need of governance emerges in order to make the user docile [1].

Since it was clarified why Facebook is interested in governing, it raises the question how private surveillance is legitimated. Actually, the internet is unsafe and proves to be dangerous in terms of spam, pornography, bullying, etc. Facebook is offering a 'Hobbesian contract' [1], to avoid the state of nature so to say. Therefore, the idea is to keep the digital spaces safe and legitimize private surveillance. So on the one hand, Facebook is 'protecting' [1] the users by providing a safe space, but, on the other hand, Facebook also governs and disciplines users. And this is done by the thread of exclusion. It is quite effective since Facebook offers a valuable benefit : it facilitates the accumulation, maintenance and mobilization of *social capital*. Social capital can be understood as the "capacity to effectively mobilize resources dispersed in one's social network" [1]. In that sense, one's social relations can be converted into resources. That happens for example when announcing a political activism event on Facebook. The more people know about it, the more valuable it is. It can be concluded that the number of followers can be seen as a measure of social capital since this number describes to which extent the resources can be mobilized. Hence, social connections are granting access to highly valuable information, political power, but also economic resources. In this system, Facebook is therewith providing a low-cost maintenance of larger networks.

The social capital which the users produce can be invested in Facebook which is operating analogously as a bank since the capital is maintained or increased in its value. As a consequence, Facebook is able to exert monopolistic control over generalized social capital which also allows it to govern the user [1]. Virtually, the power relies on the status Facebook gained as a central bank of social capital. The leading digital platform has therefore the power to devalue, freeze or confiscate social capital. Therewith, the position of power allows to perform economic, political, as well as socio-cultural influence by actively enforcing norms of behavior on the user. This form of government is coined by the thread of exclusion which is connected with being highly disadvantaged.

For example, if users are violating these established norms Facebook can remove your contents, or temporarily exclude users from certain features like posting. What is done in the end is preventing the dispersion of your resources leading to a decrease of your social capital. A norm could mean that you are not allowed to upload content related to pornography, or that it is forbidden to insult other users verbally. In doing that, Facebook is directly manipulating and regulating the social world, namely by restricting the social interactions on the platform on the basis of opportunistic and profit oriented standards. As the norms I listed were adopting a moral sense, Facebook can also restrict interactions arbitrarily, for instance to prefer a certain political party in allowing one party to display advertisement and to prohibit the same for the other.

How can the bank of social capital be described then? Facebook is extending the interest from management to regulation of social interactions across a variety of life spheres. The socio-cultural, economic and political dimension was discussed so far. The aim to be an universal mediator and regulator of social life which Facebook is trying to pursue [1], has to be viewed critically. The dominance of the digital platform becomes obvious also in terms of the necessary "point of passage" [1] Facebook provides for several spheres. The power position of Facebook, based on the status as a central bank of social capital, is an alarming concentration of power that should be taken seriously. Next to that monopolistic character, Facebook also has exploitative features. The internet corporation is targeting the user to exploit them as biopolitical producers whose immaterial labor can be captured and monetized into data. [1] There is a strong linkage between exploitation and governance. Whereas the exploitation is characterized by the capture and revaluation of social relationships, governance tries to control these relationships. Thereby, there are two different forms of surveillance used by Facebook. *Commodifying surveillance* simply puts actions into data, while *panoptic surveillance* describes the monitoring and disciplining of users to actively form and improve biopolitical production [1].

### III. FACEBOOK AS A COMMITTER OF DATA CRIMES

As we have seen so far, the bank of social capital turned out to be monopolistic and exploitative. In this paragraph, it will be discussed why one can denote Facebook as a criminal bank of social capital by showing Facebook's commitment to data crimes. This approach is based on the paper "Crimes of Digital capitalism" by J.S. Oleson and Aitor Jiménez.

As revealed in [2] the data of 85 million Facebook users were traded, commodified while violating their own terms and national as well as international laws. The given dimension of exploiting the user's data is attacking the privacy of the user seriously. What goes along with the violation of data privacy is a change in the way the user perceives and understands data privacy itself and democratic values. In a sense the notion is disrupted. Facebook is unscrupulous. The company obtains benefits from violating privacy laws [2], which means that it acts on the basis of a benefit-cost analysis regardless of an

ethical dimension as it seems. Thereby, Facebook is violating privacy laws regardless of the social harm it creates. The socially harmful behavior of Facebook and other Big Tech companies are still a current issue. A question arises. Why are there only a few legal actions taken to punish Big tech companies for violating privacy laws?

In order to answer the question it is necessary to analyze the patterns of Big Tech companies beforehand. There exists a structural relation between capitalism and corporate crime in the context of the digital economy. Along the following discussion it will be argued that the underlying pattern of Big Tech companies, which is socially harmful behavior only considering an opportunistic and profit-based perspective, should be criminalized. The described behavior corresponds to *data crimes*. Based on the given concept it involves two different kinds of crime inducing behaviors from which digital corporations are taking advantages from. *Privacy violations* and data mismanagement are the first kind of data crimes, as previously introduced. The second kind relates to the *breaking of competition rules*. Usually these 2 types of violation have been approached disconnected from each other. However, data capitalists exploited their control over data to seize control of market dominance and thereby a strongly interrelated connection emerges [2].

The control digital platforms gain over the data flows, is leading to a multi-faceted form of power [2]. Out of this, a need is demonstrated to regulate and reevaluate the data power originating of digital platforms to ensure data privacy. What can be inferred is that digital platforms are employing intentional criminal strategies which are strongly tied to their business model [2]. The elaborated criminal strategy is manifest in data crimes. As a result, the relationship between digital corporations and crime is *structural*. Big Tech companies have achieved dominant positions by actively violating data and competition laws in strategic ways [2]. Specifically, the data crimes itself are the data operations and extractions involving abusive, unlawful and exploitative behavior as demonstrated previously. The aim of data crimes is to reach socially harmful market domination out of this [2].

On a structural level, the effect is that citizen's rights are imperiled gravely. Due to the social harm and limiting of freedom which is caused by data crimes, its criminality is demonstrated. There is a need for declaring data crimes officially as crimes as they are by nature a form of criminality. On a westernized legal account, data rights are tied to human dignity. As a consequence, the violation of data privacy should be considered and treated as a human rights violation. Data crimes are a form of organized criminality which imperils not only citizen's rights, but also democratic values [2].

Data crimes are considered to be a current and sensible issue in digital capitalism. Why is it not stopped? Which challenges come with fighting crimes of digital capitalism? The basis for the argument that data crimes should be criminalized is that this process may make corporations criminally liable for data crimes and therefore may prevent further offenses. As explained in the paper [2], data crimes are by their nature

and structure part of an imperialist phenomenon, namely *data colonialism*. Data colonialism is “an emerging order for appropriation of human life so that data can be continuously extracted for profit” [2]. Along the course of extracting data and applying operations, the human beings become subjected to surveillance. Consequently, the autonomy of humans is undermined. What can be concluded from that thought is that it is not enough to criminalize data crimes at a local level in order to end digital corporate crime. Fundamentally, criminalizing data crimes would not only entail challenging the underlying capitalist legal structure of states but would also involve aborting the colonial structure of impunity in which criminal corporations operate.

Several challenges should be considered before any realistic criminalization of data crimes can be reached. Currently, the given legal framework and enforcement are not sufficiently fit or adapted to deal with a new era with Big-tech companies [2]. In the paper it is discussed that there are some institutional moves against big tech, with large fines that are imposed, however digital corporations offend again because they are making more profit than the fines are harming them. Facebook was condemned to pay a fine of 5,5 Billion Dollar for practices which include the obtaining of data without permission and allowing third parties to use Facebook’s data [2]. However, Facebook was repeating its patterns and the penalty was not able to achieve any success. Whereas, the Big tech companies are operating on a global scale, harming a huge spectrum of persons in their rights, it is clear that a need for a different system is demonstrated. The current legal framework and the ways of its enforcement used to fight data crimes are failing at having any success [2].

#### IV. CONCLUSION

Facebook has a position of power and is enjoying monopolism as a central bank of social capital. The digital platform is characterized by governing its users in order to maximize profit and thereby manipulates the social relations of the users directly. When capturing the user’s relations to monetize valuable resources out of it, exploitation is happening at a fundamental level. Facebook is abusing its users as biopolitical producers of immaterial labor. The power position is an alarming concentration of power which holds the risk of the misuse of power. The monopolized and exploitative character of Facebook can be added by the feature of unscrupulousness. As it was discussed, Facebook is violating privacy rights of users as well as abusing its power as a monopoly and breaking competition laws. To obtain the highest profit possible Facebook is not even stopping when it comes to social harm and violating privacy laws and attacking democratic values. Also, Facebook is not stopping when it comes to incredibly high fines, the digital platform is pursuing its goals. The behavior of Facebook can be described by the patterns of digital capitalism and committing data crimes. Facebook is actively suppressing its users, they do not have any influence on the rules or norms that are part of the platform, rather Facebook actively manipulates the user’s social interactions to obtain the highest

profit. In this essay I also illustrated that Facebook can be seen as a *criminal bank of social capital* which was described as monopolized, exploiting and unscrupulous. What is concerning are the imperilment and structural effects Facebook causes by its behavior. It was highlighted that Facebook threatens human rights, democratic values such as freedom, the privacy of the users, as well as the public notion of data privacy and democracy. Moreover, the current legal framework and the ways of its enforcement which is used to fight data crimes are failing at having any success. Another legal framework is needed which is adopted to the Big Tech era we are currently in.

Finally, a few open questions remain regarding the future. Will the governed accept their suppression eventually? Will it be possible to address the issue of committing data crimes in future? It remains open how future generations will understand data privacy and democracy. Will they be more aware of it or will there exist a blunting towards their notions. It is needless to say that this essay also stressed the importance for making critical reflections of Big tech companies and their crimes, and for making critical reflections of underlying patterns of digital capitalism more available for the public. Moreover, the insights of this essay raised another question for me personally. What exactly is the reason for such harmful and exploitative behavior? Power and greed? A system we’re passively subjected to? Isn’t this question casting doubt on the society’s capitalistic structure and set of values? The awareness and critical reflection of Big Tech companies being part of our society as well as their underlying patterns to maximize profit might be one of the major developments of our society for the surveillance capitalism we’re currently living in. Finding solutions to overcome its structural effects and harmful behavior, I propose, will be one of the most difficult challenges.

#### V. ACKNOWLEDGEMENT

Personally, I highly enjoyed the course, Digital capitalism Big data and AI, that was offered this summer term. I especially developed a lens through which I can detect patterns of digital capitalism which I’m also noticing in my daily life. The course raised my attention and created a feeling in me to inform more people about digital capitalism itself, and to raise attention. I hope that such courses critically reflecting the technological developments on a structural level will be offered also for future semesters. I realized that AI courses of our faculty are more focusing on the implementation and blunt application. For example, when I took the course Implementing artificial neural networks with Tensorflow nobody questioned that Tensorflow is a framework of Google and that its open source and providing a lot of material for free which may have hidden capitalistic intentions. Since I’m glad I developed a critical perspective to digital capitalism and its impact along the course, I hope that other students can also experience that progress and room for critical reflection.

## VI. PICTURES TITLE PAGE

Like Button

University Osnabrück Logo

### REFERENCES

- [1] Schwarz, Ori.(2019). Facebook Rules: Structures of Governance in Digital Capitalism and the Control of Generalized Social Capital. doi:DOI:10.1177/0263276419826249
- [2] Jiménez, Aitor and Oleson, J.C. (2022) "The Crimes of Digital Capitalism," Mitchell Hamline Law Review: Vol. 48: Iss. 4, Article 5. Available at: <https://open.mitchellhamline.edu/mhlr/vol48/iss4/5>
- [3] Zuboff, Shoshana. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. doi:<https://doi.org/10.1057/jit.2015>.