JeDEM 12(1): 1-24, 2020
ISSN 2075-9517
http://www.jedem.org
DOI: 10.29379/jedem.v12i1.604

Democratic Governance of Digital Platforms and Artificial Intelligence? Exploring Governance Models of China, the US, the EU and Mexico

Ingrid Schneider

Universität Hamburg, Department of Informatics, Ethics in Information Technology, Ingrid.Schneider@uni-hamburg.de

Abstract: The article addresses the digital transformation and new power asymmetries and challenges to democracy by the world's seven largest digital platforms. Four different governance models are examined: The Chinese authoritarian model, the libertarian US-model, the European regulatory model and the Mexican hybrid model. The challenges of digital sovereignty and democratic governance of platform capitalism are explored.

Keywords: Governance, digital platforms, sovereignty, democracy, data economy

Acknowledgement: This research has received co-funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie Grant Agreement No 873119, PRODIGEES (Promoting Research on Digitalisation in Emerging Powers and Europe towards Sustainable Development). The research is also embedded in the project GOAL (Governance of and by Algorithms) funded by the German BMBF. To both funders and all project partners I would like to express my appreciation and thanks.

Co-funded by
the European Union

1. Introduction

The story of the political economy of the digital transformation is often told as a rivalry between two states, sometimes even as a new cold war for geostrategic spheres of influence. The 2019 UNCTAD Report on the Digital Economy states: "The economic geography of the digital economy does not display a traditional North-South divide. It is consistently being led by one developed and one developing country: the United States and China. For example, these two countries account for 75 percent of all patents related to blockchain technologies, 50 percent of global spending on IoT and more than 75 percent of the world market for public cloud computing. And, perhaps most strikingly, they account for 90 percent of the market capitalization value of the world's 70 largest digital platforms. Europe's share is 4 per cent and Africa and Latin America's together is only 1 per cent

(UNCTAD 2019: xvi). This article aims at taking a broader approach by including Europe and Mexico into the picture thus broadening the horizon towards the varieties of digital capitalism. The paper has a descriptive dimension in exploring different governance models which have emerged. Moreover, it also has a normative dimension, namely whether and how to tame the new digital economic powers in a democratic way. Its special focus is dedicated to the aspects, whether and how digital platforms can be democratically regulated.

To this purpose, it is necessary to analyze first, which governance models of the digital transformation have emerged over the last decade and to consider their opportunities and risks for democracy. Special attention will be paid to large digital platforms which have gained dominance. I will present two dominant governance models, the US and China. Furthermore, I will explore Europe's struggle for digital sovereignty and analyze how Mexico addresses de digital transformation and whether and to what extent it follows one of these models.

In referring to democracy, of course there are different theoretical versions of liberal, pluralistic, or deliberative models of democracy. The shortest definition is that in Lincoln's famous 1863 Gettysburg address, "government of the people, by the people, for the people". According to political scientist Larry Diamond (2008), democracy consists of these four key elements: (a) A political system for choosing and replacing the government through free and fair elections; (b) The active and inclusive participation of the citizens in politics and civic life, including a lively public sphere and independent media; (c) Protection of the human rights of all citizens and (d) A rule of law, in which powers are separated and the laws and procedures apply equally to all citizens.

At least according to European understanding, it has been generally acknowledged that basic or constitutional rights are at least indirectly valid also between private parties, such as citizens and private corporations. Thus, democracy is not restricted to the relationship between the citizens and the state. The state has some oversight and supervisory duties. Therefore, civil rights are not only defensive rights to protect citizens *from* the state, but also positive rights to be protected *by* the state.

The structure of this article will start with some introduction into the current digitalization process and relate to some concerns about distortions of democracy in the digital transformation. Then, some characteristics of digital platforms will be defined. For the geopolitical arena, it will present first, some features of China's digital transformation model and contrast it secondly, with the digital platform model developed in the US. Third, the European digital regulatory model will be explained. Fourth, it will explore which road Mexico is embarking on. Finally, some conclusions will be drawn.

2. Digitalization and Democracy

Digitalization today is penetrating all spheres of social life, from cradle to grave and in all societal sectors. If asked, most people may associate digitalization first and foremost with changed patterns of communication. People using cellphones and looking at their screens are a familiar sight in many countries, cultures and across different social milieus. Many people embrace the digital opportunities and enjoy it as convenient and often entertaining. This is also true for many people in the Global South, even though the digital divide is still prevalent and other socio-economic gaps have not vanished. Of the seven billion people on planet earth, five billion have a mobile phone, but only three billion have toilets with good sanitary conditions and two billion don't have access to clean drinking water. At present, one third of the world's population active on the internet is under 18 years old (UNICEF, 2017).

All sectors, agriculture, industry and services are currently undergoing a digital transformation process in which data is becoming a crucial asset. These acts of digital usage create lots of data traffic and transnational data flows. Many people are hardly aware that this traffic requires a large physical infrastructure in the background, like satellites, radio towers, undersea cables and broadband cables. The use of all the internet services – streaming, searching, working, chatting – creates an ever increasing amount, tera-, peta-, exa-, and zettabytes of data, to be stored in large data centers, so-called server farms. If cloud services are used, the location of citizen's data can be in another territory and will thus be subjected to the laws and jurisdiction of another nation state.

In the first decades of the internet, many believed that it would almost automatically be a force of and for democracy. New methods of data analytics, like Big Data, artificial intelligence (AI) and Machine Learning have been perceived as fostering progress and welfare. In 2013, the MIT Technology Review titled on its cover page "Big Data will save politics". However, only 5 years later, its cover contradicted by titling "Technology is threatening our democracy. How can we save it?" (Lichfield, 2018). Also in 2018, a new word entered Silicon Valley's lexicon: the "techlash", or the risk of consumer and regulatory resistance to big tech companies. The tide seems to have turned. So what happened? And why does there appear to be such a shift in the general sentiment and public opinion? In the context of this article and its focus on digital platforms, I can only point to some keywords.

In the beginning, social media were regarded as a welcome broadening of the public sphere which would promote free speech, attention and resonance for everyone and thus become a tool of participation and force for democratisation. Some political scientists proclaimed a move from the spectator to the participatory democracy. And indeed, social media is useful to mobilize people, to create alternative sources of information, networks, and enable protests.

In the meantime, however, what we see is a strong fragmentation of the public sphere. Quality newspapers are in decline. People are not always friendly to each other but create hate speech, shitstorms, and cyberbullying on the internet. Social media platforms are accused of creating filter bubbles and echo chambers, in which the users only receive information which confirms their already existing beliefs. The spread of "fake news", mis- and desinformation, conspiracy theories, or even radical propaganda is on the rise, especially in times of election and crisis like the Covid-19 pandemic and it is increasing social polarization. Hence, many scholars and policy-makers call for more digital literacy and media competences (Hendricks & Vestergaard, 2019).

At present, there is a race between developed countries to take the lead in Artificial Intelligence and many states have started digital agendas and pursue national AI strategies. These will lead to even stronger transformations in all social spheres. Big Data and Artificial Intelligence can be defined shortly as “the collection and aggregation of large masses of (publicly, commercially, proprietarily and/or illicitly available data and its analysis, largely in the form of correlation, pattern-recognition and predictive analysis" (Saetnan/Schneider/Green 2018: 6). However, Big Data and AI are not only technologies that employ new statistical and probabilistic tools for analysis, they are also driven forward by normative arguments, the involved actors' beliefs, as well as economic and political interests (Kitchin 2014). They have socially transformative and “mythological” aspects, namely “the widespread belief that large data sets offer a higher form of intelligence and knowledge that can generate insights that were previously impossible, with the aura of truth, objectivity and accuracy“, as danah boyd & Kate Crawford have put it in their seminal article (2012, p. 665).

Many people think that computers are more neutral than humans in making automated decisions. However, there is more and more scientific evidence showing that algorithms are not neutral. Human prejudices, stereotypes and bias enter the training data and algorithms and are being reproduced. As data analyst Cathy O'Neil in her book “Weapons of math destruction” (2017) has demonstrated, Big Data often increases inequality, reinforces social gaps in education and access to health, and threatens democracy. Data aggregation and analytics allows for the profiling and categorization of users. It harbors potential for discrimination and stigmatization, for instance in applying for credit or buying real property. Vulnerable people might have to pay more for car, health and life insurance, or have less chances of employment. These processes are analysed as social sorting and individualization of risks (Lyon 2003). All in all, this may threaten basic human rights and societal ideals of equity and solidarity, such as equal access to health services; predicting and individualizing risks may become discriminatory and undermine the insurance principle (Barocas & Selbst, 2016; Schneider & Ulbricht, 2018; Orwat 2019).

Access to personal data can also be used for political purposes and manipulation. As the Cambridge Analytica case has shown, Facebook via an API gave at least 60 phone and other device makers access to data of 87 million users and their friends. These data were used not only in the 2016 US election campaign by advisors for Donald Trump and in the UK Brexit vote. Cambridge Analytica has influenced more than 100 elections in 30 countries, based on data mining and data analytics. In Brazil, the spread of disinformation and conspiracy theories on WhatsApp groups contributed to the election of Jair Bolsonaro as president (Schlereth, 2018; Cadwalladr, 2019; EDPS, 2018; Ghoshal, 2018; House of Commons, 2019).

Many states are taking part in social media manipulation or even employ internet shutdowns when protests occur, as did 33 countries in 2019 (Internet Society, 2019). It may be no wonder that contemporary headlines ask questions like “Can Mark Zuckerberg Fix Facebook Before It Breaks Democracy?” (Osnos, 2018) and that even Chris Hughes, a former co-founder of Facebook wrote: “It's Time to Break Up Facebook” (Hughes, 2019). Google has also been accused by its own employees of doing work they see as unethical, such as “Project Maven” a contract with the U.S. Department of Defense to track people and vehicles in video footage captured by drones, which raised fear among engineers that the technology would be used to single out targets for killing. There were also misgivings around the consideration to reenter the Chinese market at the cost of censoring search results on behalf of the Chinese government. Several staff people were fired for organizing protests (Scheiber& Conger, 2020).

Many of the concerns for democracy are summed up in a recent Pew Study (2020) from the US, which concluded that many experts are rather pessimistic about the implications of the digital transformation. About half of the experts (49%) interviewed predicted that humans' use of technology will weaken core aspects of democracy and democratic representation between now and 2030, due to the speed and scope of reality distortion, the decline of independent journalism and the impact of surveillance capitalism. Digital illiteracy and the collapse of quality journalism may create an ill-informed public which easily falls prey to disinformation. In short, they warn that technology empowers the already powerful and that technology "diminishes" the governed. Experts fear that information technology is easily weaponized to manipulate and distort facts, which affects people's trust in public institutions and each other. This might incite a downward spiral toward disbelief and despair. Moreover, many experts surveyed said they worry about the future of democracy because of the power of major technology companies and their role in democratic discourse, as well as the way those companies exploit the data they collect about users. A third part (33%) of the experts is more optimistic, they expect technology to strengthen democracy and democratic representation, as reformers may find ways to fight back against "info-warriors and chaos". Only 18% of the experts expect no significant change in the next decade (Pew Research Center, 2020). Even if readers might not be as pessimistic as many of these experts, it is certainly worthwhile to analyze the power of digital platforms which I will do in the next chapter.

3. Digital Platforms - Definition and Characteristics

Let me start with some analytical considerations on digital platforms. "The world's most valuable resource is no longer oil, but data" (The Economist, 2017) is a common saying. Platforms extract and process data. However, the oil metaphor is contested, as data is neither scarce nor a rival resource, as it can be used by many without being diminished. However, de facto ownership of data has definitely turned into an intangible asset of firms. In analytical terms, according to Nick Srnicek (2017, p.47), digital platforms have the following characteristics:

- Platforms are digital infrastructures that enable two or more sides to interact, such as customers, advertisers, and service providers.
- Platforms produce network effects: The more users, the more valuable that platform becomes for everyone else. (Therefore, for instance, most people are on WhatsApp, Facebook, and Instagram, not on Telegram, Signal or Threema, because they can reach most other people on these messengers and social media platforms.)
- Platforms often use cross-subsidisation: one arm of the platform company provides a service or good for free, another arm – often the advertising section - creates revenues to compensate for the costs of the free services. In return, customers provide heaps of data to be profiled for targeted advertising.

The rules of service and product development are set by the platform owner.
In particular, the latter aspect of Nick Srnicek's analysis has to be emphasized, as he adds: "In that respect, platforms 'embody a politics' as they not only gain access to data but also 'control and governance over the rules of the game" (Srnicek, 2017 p. 47). In a nutshell, it can be stated that new business models of the digital economy are disruptive and have an impact on democratic culture.

“Tech culture prizes speed, scale, efficiency, convenience, a disregard for the law (… ask forgiveness not permission) and a dislike, if not hatred, of government” (Pew Research Center, 2020 p. 11). Mark Zuckerberg asked his employees to "Move fast and break things", and many other start-up companies have followed suit. Most internet companies and app revenue models rely on tracking online activity and selling ads. Hence, value chains from data and big data analytics became a source of power for large platforms. Economic mechanisms such as network effects lead to the oligopolisation of platforms or even to digital monopolies: “Seven ‘super platforms’ – Microsoft, followed by Apple, Amazon, Google, Facebook, Tencent and Alibaba − account for two thirds of the total market value [of the 70 largest digital platforms]” (UNCTAD, p. xvii). The growing dominance of digital platforms has global implications. According to the 2019 UNCTAD report, the combined value of the platform companies with a market capitalization of more than $100 million was estimated at more than $7 trillion in 2017, thus 67 per cent higher than in 2015. Some global digital platforms have achieved extremely strong market positions in certain areas. Google for instance, has some 90 percent of the market for Internet searches. Facebook accounts for two thirds of the global social media market, and is the top social media platform in more than 90 percent of the world’s economies. Amazon boasts an almost 40 percent share of the world’s online retail activity and its Amazon Web Service accounts for a similar share of the global cloud infrastructure services market (UNCTAD, p. xvii).

Thus, in many digital technological developments, “the rest of the world, and especially Africa and Latin America, are trailing considerably far behind the United States and China. Some of the current trade frictions reflect the quest for global dominance in frontier technology areas" (UNCTAD 2019, p. xvi). This also creates gaping power asymmetries between platforms and users, as it decreases consumer choice. Not to use certain platforms is not an option if one doesn’t want to self-exclude from important parts of contemporary social and economic life.

Within only one or two decades, previous small platform companies turned into digital giants. The rapid rise of these seven “super platforms” can be explained by several factors. The first is related to the above mentioned network effects. The second is the platforms’ ability to extract, control and analyze data collected. More users mean more data and more data mean a stronger ability to capitalize on first-mover advantages and to outcompete potential rivals. Thirdly, once a platform begins to gain traction and starts offering different integrated services, the costs to users of switching to an alternative service provider start to increase. These factors have led to the rapid rise to dominance of these large platforms (van Dijck, Poell & de Waal 2018; UNCTAD 2019, p. xvii).

Issues concerning 'digital sovereignty' arise, since data generated by the citizens, businesses and organizations of a particular state are a major economic resource in the digital economy, which can be harnessed to create economic value. These are related to control, access and rights over the data at the global level and the extraction and appropriation of the value that could be generated from refining them (Bendiek/ Schallbruch 2019: 6). Under the current regime, the platform that collects the data from the users is the one that controls and monetizes such data. As a result, big digital platforms have an advantage in terms of capturing data-related value (Pew Research Center 2020, p. 11).

4. China's Digital Transformation and AI Model

China has become very ambitious, the rising star in Artificial Intelligence and wants to become the digital and economic world champion. Xi Jinping, the President of the People's Republic of China has set the goal of China replacing the USA as world market leader by 2025 (Hausstein & Zheng, 2018). China has its own platforms: Alibaba is similar to Amazon, WeChat is the messenger like Whatsapp, and China's search engine is Baidu, similar to Google. WeChat, owned by Tencent, has more than one billion active users and together with Alipay (Alibaba), its payment solution has captured virtually the entire Chinese market for mobile payments. Meanwhile, Alibaba has been estimated to cover close to 60 per cent of the Chinese e-commerce market.

These platforms and their data are closely integrated in China's Big Data and digital tech strategy, as heaps of data are needed for machine learning, AI and training of neural networks. China also invests heavily in face recognition and biometrics. One of the key areas in which investments are being made is – in addition to military applications – the total monitoring of the population. Already now, several hundreds of millions of monitoring cameras are hanging from buildings and light masts. These are increasingly being equipped with "smart" monitoring technology and integrated into comprehensive systems, such as the social scoring system.

By this year 2020, China wants to introduce a nationwide Social Credit System. In some regions like Shanghai and Rongcheng, different pioneer models have already been in place for some years (Ohlberg & Lang: 2017). Local governments and agencies have been piloting aspects of the system, which will eventually attribute to every Chinese citizen a personalized score that includes all the data collected on their behavior. In short, the idea is that every citizen will have an individual "social score" or "social credit". "Good" behavior will result in bonus points, "bad" behavior in deductions of the points received on the individual score account. The social credit system aims to incentivize "trustworthy" behaviour through penalties as well as rewards. According to a government document about the system dating from 2014, the aim is to "allow the trustworthy to roam everywhere under heaven while making it hard for the discredited to take a single step" (Kuo, 2019).

The data for this system originates from many areas: It comes from the employer, from banks and distributors, from the house administration and also from governmental agencies. What enters the score are correct tax payments, loan repayments, paying bills and court judgments. But also social inputs like adherence to traffic rules, family planning limits, filial piety (like visiting and caring for your parents) and criminal records are included in the score. Moreover, data from large digital platforms like Tencent and Alibaba are also included in the system and contribute to the allocation of points, such as credit card bills, shopping habits, and the reliability of information posted and reposted online, for instance on WeChat. Another thing to be measured is the interaction with other internet users – who if spreading false information or criticizing the government will receive deductions in the score. If you interact with friends with low scores, this will also negatively affect your own (Strittmatter, 2019).

In terms of output, a high or low score will affect social opportunities like eligibility to loans, high school, jobs and travel. The individual score decides on who gets an apartment or a work place.

Other penalties for individuals include being barred from buying insurance, real estate or investment products. Citizens with a low score are placed on black lists for social credit offences and cannot travel on planes and express trains any more. By the end of 2018, according to the Chinese National Public Credit Information Centre, would-be travelers were banned from buying flights 17.5 million times and citizens were prevented 5.5 million times from buying high speed train tickets (Kuo, 2019).

In many Chinese cities, jaywalking is already immediately responded to by the naming and public shaming of the person who crossed at a red traffic light. The ubiquitous video cameras equipped with facial recognition software enable the individual attribution of rule violations. In addition, these and other sensors provide an enormous amount of data that AI systems are trained with. Many advances in the field of artificial intelligence are based on general surveillance, being it state-sponsored or by data acquired from private platforms. Finally, in some regions the social scores are also made public in order to distinguish especially "good" citizens and to identify socially "negative" elements (Strittmatter, 2019; Ohlberg & Lang, 2017). Most extensive surveillance methods are executed in the Xinjiang province where the Muslim minority of the Uighurs is kept under repressive digitized control (Zand, 2018; ICIJ, 2019; Buckley & Mozur, 2019). Furthermore, the Covid-19 pandemic has been used by Chinese authorities to invigorate surveillance by obliging citizens to wear a contact tracing app which tracks their location and grants or denies access rights to many facilities of the outside world (Giesen, 2020; Böge, 2020).

China justifies its system as a way to create harmony and social stability (Au & Kuuskemaa, 2019). In the Western world, it is regarded as the attempt to create a digital totalitarian state. To sum up, the Chinese governance model of the digital transformation is an authoritarian model of mass surveillance and aspired total control by the state. Here, platforms are not democratically controlled, there is a tight collaboration between states and platforms and these platforms are used by state authorities to control the citizens and to intimidate potential critics or opponents. China's ambition seems to create a digital panopticon, in which all the citizens are under permanent supervision and conform to this surveillance by self-censorship and internalized control.

5. The United States' Digital Platform Model

Let us move to the next, contrasting model. The US digital transformation model is a libertarian, free market model in which as yet hardly any governmental regulation of digital platforms is taking place. Disruption as exercised by these platforms is seen as positive both for innovation and economic growth and hence is fostered. Not least as a result of high finance and venture capital investments, low regulation and the so-called "Californian Ideology"(Turner, 2006 and 2017), most platforms are based in the Silicon Valley. In the business-to-consumer sector, a few US platforms dominate the markets in the western world.

Platforms, acting as intermediaries and data brokers have gained enormous power as economic titans and as gatekeepers. Some years ago, the German magazine "Der Spiegel" (2015) on its cover page declared the large platform owners to be the new "world government" – that is certainly highly exaggerated but it is interesting how platforms describe themselves. Eric Schmidt, former Executive

Chairman of Google (2011 – 2015) and Alphabet Inc. (2015-2019) wrote: "We believe that modern technology platforms, such as Google, Facebook, Amazon and Apple, are even more powerful than most people realize (...) and what gives them power is their ability to grow – specifically, their speed to scale. Almost nothing, short of a biological virus, can scale as quickly, efficiently or aggressively as these technology platforms and this makes the people who build, control and use them powerful too" (Schmidt & Cohen, 2013). Often, the Big Five Western internet companies Google, Alphabet, Facebook, Amazon, and Microsoft are clustered together by the acronym GAFAM. In the following, I will explore, what their main sources of power are.

The first source of power is their market value: Four of them, Alphabet, Amazon, Apple and Microsoft in 2019 have exceeded the "magical threshold" and have become worth more than $ 1trillion each. In February 2020, Facebook's market value was $620 billion (The Economist, 2020; Macrotrends, 2020). This means that each of these platforms are more valuable than any oil, pharmaceutical, bank, credit, airplane or film company (Schoen, 2018). And there seems to be hardly any end in sight: The Economist in February 2020 reported "a bull run over the past 12 months, rising by 52%" on the combined shares of the five GAFAM firms. These five big tech firms, worth $5.6 trillion make up almost a fifth of the value of the S&P 500 index of US shares. Just only the increase in the firms' combined value, of almost $2 trillion, is reported to be "roughly equivalent to Germany's entire stockmarket". The magazine stated this to be "an alarming concentration of economic and political power." (The Economist, 2020). At present, it is unclear whether this trend of big tech firms' supersized valuations will continue or whether investors have stoked a speculative bubble. Even though it seems as if the tech giants emerged unscathed by the Covid-19 pandemic, it is probable that the economic turndown during and after the Covid-19 crisis will negatively affect their revenues from advertisement.

A second source of platform power derives from the number of users: 2.9 billion monthly users makes Facebook the largest social app. With 1.6 billion users WhatsApp is the most popular messenger service. And with more than 1 billion users Instagram is the largest photo exchange site (Statista, 2020a). The number of people using one of the former services is larger than the population of almost any nation state. The social networks with the largest extensions, WhatsApp, Facebook Messenger, and Instagram are all owned by Facebook. This large audience makes the designers of these platforms and the algorithms they produce not only highly powerful but also puts a lot of responsibility on them. The question is how to program the algorithms and how to rank the content. It must be emphasized that these software design decisions determine what you see or you don't see on your timeline, what is ranked first on a search engine, which priority is given to the products offered and which videos are proposed to be watched.

The scope of users translates as an audience for advertisers, as this is how these platforms are making their revenue. On most of these platforms, users get services for free, but "pay" with their personal data, often without their own knowledge. Therefore, it is often said, "if you don't pay for the product, you are the product being sold". These more or less hidden data extracting and profiling practices have raised concerns about violations of privacy and clashes with human rights and civil liberties (EDPS, 2014, 2015; Zuboff, 2019). Platforms create detailed profiles of their users, their preferences, inclinations and weaknesses, to be exploited for targeted ads by advertisers. The platforms also exchange profile information data with commercial data brokers like Axciom and Oracle. Datasets given to third parties include for instance credit worthiness, taste preferences but also most sensitive health issues such as chronic diseases, tabacco, alcohol and drug (ab)use, or pregnancy and abortion issues (Christl, 2017).

A third source of power is the market dominance in smart phones engines and search engines. In December 2019, Android maintained its position as the leading mobile operating system worldwide, controlling the mobile OS market with a 74 percent share. Google Android and Apple iOS jointly possess almost 99 percent of the global market share (Statista 2020b). The Android smartphone operating system has a market share of two thirds (64%) both in the EU and in the US, whereas Apple's iOS has a 33% market share. In Latin America, the situation is even more pronounced: Google's Android operating engine dominates the market in Mexico with 86% of all cellphones, whereas Apple's iOS has a 14 percent market share. With respect to search engines, Google / Alphabet is dominating the European market even more strongly than in the US. Google as a search engine dominates 90 percent of the search market in the EU and 76 percent in the US. Both systems are crucial for the infrastructure of the internet (Statcounter Global Stats, 2020).

A fourth source of power is the acquisition of smaller players who could become rivals or have developed innovative technologies. Major acquisitions by digital platform companies include Facebook's acquisition of WhatsApp, Instagram and Oculus. Alphabet (Google) and Microsoft have invested in telecommunications equipment, Microsoft has taken over of LinkedIn, Skype and Nokia. Google has not only acquired Motorola but also the video platform Youtube, the advertising company Doubleklick and the smart home firm Nest (Statista 2020a). Major platforms have also made other large acquisitions in the retail industry, advertising and marketing industry and in non-residential real estate (UNCTAD 2019, p. xvii). Digital platforms heavily invest and spread also on to other sectors, such as transport, health, education, and media (van Dijck, Poell & de Waal, 2018; Zuazo, 2018).

To sum up on the US platforms, their market value, a giant user base, market dominance and high revenues from the advertisement market and large acquisition power translates in economic and geopolitical power in the western world. Sophisticated tax evasion schemes and extremely high revenues allow these companies also the power to lobby governments and to pay lawyers for strategic litigation cases (Schneider, 2018, p. 145f).

The US federal state as yet does hardly interfere and regulate. On the contrary, it has demonstrated desires to use the data collected by these private entities for its own political purposes. Even though president Trump seems to have some personal quarrels with some of the internet platform's top brass, such as Amazon's Jeff Bezos, the US economy profits heavily from the dominance of its platforms in large parts of the world. As has been revealed by the Snowden files, bulk data collected and processed by GAFAM are intercepted by the NSA and used not only to combat terrorism but also for economic espionage and gains in international diplomacy (Snowden, 2019; Schneier, 2015; Lyon, 2014; Greenwald, 2014).

Julie Cohen has argued that in the contemporary US "informational capitalism" it is not a political regulation which is taming platforms' power but it are the platforms themselves who are reshaping legal institutions, gradually “optimizing” them towards their own interests (Cohen, 2017 and 2019). Only recently, due to stronger discussion about a “techlash”, competition law inquiries have started. In September 2019, 50 attorney generals from US and territories launched a joint review into Google’s advertising and search practices to assess whether it has abused its dominance to stifle competition. Akin to that, the US Department of Justice launched a wide-ranging review of GAFA companies. And the Federal Trade Commission (FTC) is investigating possible antitrust violations (Giles, 2019). For the upcoming 2020 US elections, two of the candidates for the Democratic party's presidential nomination, Elisabeth Warren and Bernie Sanders, had even called upon “Breaking up Big Tech”. These calls resonated with some constituents but did not have a decisive impact on the Democratic party’s final nomination which chose Joe Biden running for president.

6. The European Union’s “Third Way” – a Quest for Digital Sovereignty

Europe and its platforms are dwarfed by the digital giants in the US and China and lagging behind in technical advances. And it is not only Europe but also the rest of the world, as it seems. So, are Europe, Canada, Japan, Australia, New Zealand and the Global South squeezed between the US and China and will only be able to choose between those two governance models to compete in the international digital competitive race? Europe is confronted with technology leadership by the US and China. Some policy-makers have even gone so far to speak of a new “Cold War” in digital predominance, referring in particular to the Huawei/ 5G case, in which the world seems to have only the choice between an US-American and a Chinese tech sphere (Bendiek/ Schallbruch 2019). This struggle for supremacy is not only related to technical standards but also to “geopolitical power projection through ‘technopolitical spheres of influence’” in which the development and usage of data and technologies thus “become part of a systemic competition” (Lippert & Perthes 2020: 2). The German foreign minister Heiko Maas in a 2019 speech referred to digital technological leadership as “a super power factor, a game changer”, affecting all other power factors: “Whoever has the best access to data controls the crucial raw material for machine learning. Those who set standards and own patents will hold the key to the competition between the major powers in the future. If there are additional breakthroughs, for example in computing capacity, the balance of power will shift again” (Maas 2019). Thus, European perceptions and attitudes are expressed in quotes such as that by Arnaud Montebourg, the (former) French Economy Minister who said in 2014: “We don’t want to be a digital colony of US Internet giants. What’s at stake is our sovereignty itself” (Stone & Silver 2015).

As a response, Europe has proclaimed a “Third Way”, a third, regulatory model of the governance of the digital transformation. “Digital sovereignty” has become a new keyword, not only for individual informational self-determination but also for states. Both the French President Emmanuel Macron and the German Chancellor Angela Merkel have referred to this term. It signifies that Europe should follow a path independent of both the US and China. Europe’s quest is to be capable of self-determination in the digital space, empowered to act and decide for itself. In a report for the French Parlament, Cédric Villani emphasized that the European AI strategy must be significantly oriented towards the goal of sovereignty (2018, p. 8,19,22,31,37, 47, 51, 106, 123). This is not only a matter of improving the competitiveness of the European economy, as the Data Ethics Commission

(2019) of the German Federal Government has stressed in its expert report. Rather, the digital strategy must be based on key ethical and legal principles, such as human dignity, self-determination, privacy, security, democracy, justice, solidarity and sustainability (Data Ethics Commission 2019: 43-48). In doing so, investment, research promotion and regulation shall be interrelated to assert "that the defining feature of European technologies be their consistent alignment with European values and fundamental rights" (Data Ethics Commission, 2019, p. 227). Therefore, the European idea of a digital society is "centred on the individual and the common good, at the same time. New technologies must, therefore, also be judged by whether they are conducive to democracy and whether their use respects human rights. Regulatory measures can make a decisive contribution to balancing the opportunities and risks of a technology with the interests of companies, consumers, the state and civil society" (Bendiek & Schallbruch 2019, p. 3). In this vein, a European Data Space initiative called GAIA-X was started in the end of 2019 which is supposed to become akin to a European data cloud, imagined as federated data infrastructure which aims at creating a European data and AI driven ecosystem and ensuring data sovereignty. Another recent project is the Open Search Foundation, a network of research centers which wants to establish a European, non-commercial search engine (Braun, 2020).

In the following, I will present the most important European regulatory initiatives in order to strengthen both privacy, fundamental rights, and international competitiveness. A core element is the EU General Data Protection Regulation (2018). But Europe also advances economic and ethical regulations with the EU Digital Single Market Agenda, antitrust inquiries and the trustworthy AI ethics initiative.

6.1. The EU's General Data Protection Regulation (GDPR)

The first field of the EU's regulatory intervention is data protection policy. The General Data Protection Regulation (GDPR, EU Regulation (EU) 2016/679) took effect from 25 May 2018 after a two year transition period. GDPR is not the first privacy regulation of the EU, as in 1995 already an EU Data Protection Directive (95/46/EC) had entered into force which was replaced by GDPR in 2016. The GDPR confirms and emphasizes principles such as informed consent of the data subject to the data collection and individual's right to transparent information, correction and deletion, as well as data minimization, purpose limitation of data collection and data safety to be adhered to by the data processors. Europe has also introduced the "right to be forgotten" which means a right of citizens to demand from platforms like the Google search engine to de-link outdated possibly stigmatizing or wrong information on them, causing reputational or defamatory harm. Data portability and interoperability of data is to be incentivized and fostered, demands the GDPR (EU, 2016).

Data protection authorities have gained enhanced enforcement powers. One of the sticks assigned to them via GDPR is the stricter framework of sanctions: Private companies violating the rules can be punished with a maximum fine of 20 million euros or up to four per cent of total worldwide annual turnover (whichever is higher) (Art. 83 (5) GDPR). Not least because of these potentially very high fines, GDPR is regarded as a global game changer, because this can make the executives of internationally active companies pay attention to data protection. To give an idea of the amount of possible penalty payments, four percent of worldwide turnover revenues for each of the five GAFAM companies could amount to possible penalties of several billion US-dollars. This potentially high fine – of which is uncertain whether it will ever be imposed – may work both as a carrot and a stick to incite GDPR compliance.

Compared with the US and China, the EU has the strongest data protection regime worldwide. And its reach has extended beyond Europe. The EU has codified the so called market location principle (lex loci solutionis): This means, EU data protection law also applies to companies based outside the EU with activity in the EU market, whenever data of EU citizens are processed or digital products offered in the EU. Moreover, GDPR principles are also enshrined into international trade agreements (Bendiek & Römer 2019). Both protect EU's citizens, the effect, however, goes beyond this, as it becomes international standard setting. This is often called "California effect" – or nowadays it has been coined "Brussels effect". The term "California effect" was introduced by David Vogel (1995) and refers to the strengthening of consumer, environmental and other standards towards the direction of political jurisdictions with stricter regulation. The name originally derived from new environmental regulations in California in the 1980s, proscribing rigid standards for car emissions. In order not to lose the (large) California market, the US automakers did not produce cars with two different standards, but generalized the stricter standards for the entire US market and a little later for the rest of the world. The same applies today to the comparatively strict European data protection law. For global companies like Google, Facebook or Amazon, leaving the lucrative European market is not an option. At the same time, it would be an extraordinary burden to them to organize their business according to two or more different sets of legal regulations. The inherent mobility of data flow requires de facto transnational regulation. For the time being, it seems to be far more efficient to implement the stricter European regulations on a global scale. This is called the "Brussels effect" – companies offering services and products in the EU have to comply with GDPR, and market participants in other jurisdictions join in. So all in all, the GDPR has extraterritorial effects and has become sort of a global baseline (Bendiek & Römer 2019; UNCTAD 2019, p. 135).

More generally, data protection legislation has become an international success story: To date, 120 countries have adopted comprehensive data protection and privacy laws to protect personal data held by private and public bodies. Another almost 40 countries and jurisdictions have pending bills or initiatives (Banisar, 2018). The US is one of the few countries which does not have a nationationwide, federal comprehensive data protection legislation. However, at least the California Consumer Privacy Act (CCPA), "a light version" of GDPR, took effect on January 1, 2020, and the states Nevada, New York, Texas, and Washington consider passing a similar bill.

6.2. Further EU Regulations: Tax and Competition Policy and AI Ethics

As it would go beyond the scope of this paper to provide details of further EU regulations, I will only shortly refer to some other measures taken or envisioned in Europe to tame the tech platform titans. A second field of regulatory intervention is tax policy. Europe wants to counter tax evasion strategies. The GAFAM digital platforms hardly pay any taxes outside of the US. Apple pays 1%, Google 3%, Amazon 5% on taxes abroad. The European Commission ordered Apple to pay €13 billion after it ruled that Ireland broke state aid laws: Apple paid a maximum tax rate of just 1%. In

2014, this was even less – Apple paid only 0.005% (which is €500 on €100.000 revenue). This happened although the usual corporation tax rate in Ireland is already very low, at only 12.5 percent (Schneider, 2018 p. 162-164). Further debates focus on a "digital tax", and there is also an OECD initiative about a global "minimum tax rate" for corporations. Spain announced in February 2020 that it will impose a digital tax of three per cent on the turnover of Google and other large platforms in the 2020s. France had also introduced such a digital tax in 2019 but withdrew it quickly because of US trade retaliation measures (Bayona, 2020).

A third field of regulatory intervention is competition policy. As mentioned above, this has also become an issue in the US. In Europe, policy interventions sound less radical than "breaking up big tech" but are possibly more stringent. The European Commission already imposed high punishments on Google in three cases for its abuse of market dominance. In the Google Shopping Case, Google was found to give its own comparison shopping service prominent placement and to demote rival services. Therefore, the Commission imposed a fine of €2.24 billion. In the Google Android Case, the Commission charged Google €4.3 billion for abusing its dominant Android mobile operating system by shutting down rivals. In the Google AdSense Case, Google was found to reduce choice by preventing third-party websites from sourcing search ads from Google's competitors and thus a penalty payment of €1.49 billion was inflicted (Schneider, 2018, p. 156-158). Further European investigations and regulatory initiatives relate to the data economy in which data is seen as a currency in the digital world and which aim at forcing large platforms to open their data troves for more or less mandatory data sharing (Crémer, de Montjoye & Schweitzer, 2019).

A fourth field of EU's regulatory intervention are rules for trustworthy Artificial Intelligence. In February 2020, the European Commission (2020) published a respective White Paper for further consultation. One of the proposals is to categorize risks associated with applications of AI. High risk applications such as face recognition in public spaces or use of AI in order to select candidates for job employment may in the future either be banned or put under very strict regulatory control. The White Paper is based on "Ethics Guidelines for Trustworthy AI", a report published by the European Commission's High-Level Expert Group on AI (2019). According to this, ethical design principles for AI should be incorporated in the software and in the usage of AI. Similarly, both the French Report by Cedric Villani (2018) and the German Data Ethics Committee (DEK 2019) already cited above emphasize in their expert recommendations for their respective governments that the European AI strategy had to be significantly oriented towards human-centric and value oriented AI. It remains to be monitored whether and how such noble principles on paper will be put into practice.

To sum up, Europe pursues a Third Way, as a form of self-assertion. Aimed at "digital sovereignty", it offers a regulatory model for the digital transformation which tries to enhance its international competitiveness and to provide safe data protection as well as protect fundamental rights for its citizens. Europe wants to become a trustworthy source of AI and digital services and thus become a reference model for other countries.

7. Which Digital Transformation Model in Mexico?

The digital transformation strategy is not only an issue in the industrialized world but also in the Global South, in particular for middle-income and newly industrialized countries. The example of Mexico as a rising power will provide some insights into how these states encounter the digital transformation, an area which to date is rather under represented and under researched.[1]

Mexico has a population of 131.5 million inhabitants, and has more than 110.7 million mobile phone subscribers. Two thirds of the Mexican population (88 million people), use the internet and almost all of them also use social media. On average, every Mexican spends eight hours per day in the digital world, of which more than three hours on social media, almost three hours on TV (streamed and broadcasted) and 1,5 hours on streamed music. For Mexico, the preferences in social media are similar to many other countries. In 2019, YouTube was the social network with most active user rates in Mexico (97%), followed by Facebook with 93%, then Instagram with 64%, Twitter with 57%, Pinterest with 40%, LinkedIn with 33% and Snapchat with 31%. Thus, Facebook alone reaches 86 million Mexicans (Yi Min Shum, 2020). Mexico, similar to European countries, does not have a national large digital platform with substantial market value or economic scope.

Throughout Mexico, there are numerous organizations and institutions studying AI, its applications, working on training talent and developing technological solutions for the market. From an academic perspective, the Mexican Society of Artificial Intelligence (SMIA) has existed for thirty years as a scientific community that seeks to promote the dissemination of research projects, teaching and linking the discipline. It is accompanied by the Mexican Academy of Computing (Amexcomp), which since 2015 has become a central reference for computer science and technology in Mexico. Communities of practice are for instance The Data Pub, which focuses on education and market awareness of Data Science and Machine Learning. Governmental publications include the report "Artificial Intelligence and Economic Growth: Opportunities and Challenges for Mexico", prepared by the Center for the Implementation of Public Policies for Equity and Growth (Cippec), which indicates that the accelerated adoption of AI-associated technologies could translate into an additional sustained growth of 1% of GDP overall over the next decade (Gómez Mont & Martínez Pinto, 2020). However, as yet, there is no explicit digital agenda and national AI strategy. The current Mexican government of President Andrés Manuel López Obrador has set the fight against corruption, poverty reduction and the reduction of inequality gaps as its main priorities. However, there are a number of initiatives and also existing legislation which show that Mexico is aware of the

[1] This chapter is based on two months of field research in Mexico-City in February and March 2020, employing the methodology of expert interviews, participatory observation as well as literature and document research. I am very grateful to all the interviewees for having dedicated their time as well as effort, and to the Instituto Mora for its hospitality in providing both space and inspiring discussions. The research is part of the EU-H2020 funded project PRODIGEES ("Promoting Research on Digitalisation in Emerging Powers and Europe towards Sustainable Development") which aims at transnational knowledge sharing on the intersection of digitalization and sustainability.

challenges of the digital transformation and proactively participates in becoming a Latin American reference and in developing perspectives and visions for its own digital model. This also includes awareness and counteraction to threats to democracy and privacy as posed by the digital transformation (Maqueo Ramírez & Barzizza Vignau, 2019).

At present, the Mexican model can be categorized as a hybrid model: In business issues, Mexico is very much aligned with the US, when it comes to data protection, its orientation is towards Europe.

Many Latin American countries have taken up data protection and privacy as a constitutional right and have passed respective data protection laws. In Mexico, privacy and data protection is protected in Article 16 of the Mexican Constitution. Privacy legislation is divided in two separate laws: The Mexican data protection law for the private sector dates from 2010 (Federal Law for Personal Information in Possession of Individuals / Ley Federal de Protección de Datos Personales en Posesión de Particulares or LFPDPPP). The data protection law for the public sector was passed in 2017 (Ley General de Protección de Datos en Posesión de Sujetos Obligados - General Law on the Protection of Data in the Possession of Obligated Subjects or LGPDPPSO). Citizen's rights to data protection rules for both sectors are codified as "ARCO" rules – rights to access, rectification, cancelation and opposition. In particular, the 2017 data protection law for the public sector has high standards which are similar to the EU's law and indeed were modeled according to the GDPR at the time of the EU's law being under preparation. The public sector law has very modern clauses, such as privacy by design and privacy by default and also demands techniques for the portability and interoperability of data.

Thus, Mexico's data protection legislation has high standards and it is advanced. Its weakness lies as yet in its ambit, as the most modern law is only valid for the public sector. The Mexican law for the private sector does not have an extraterritorial clause as has the GDPR and also lacks some other provisions. However, at present, there are seven reform initiatives in the Mexican Congress and another one in the Chamber of Deputies to reform the law for the private sector. Among them are proposals to establish a right to be forgotten, portability obligations for the private sector, opt-in clauses for informed consent and clauses on privacy by design and privacy by default.

What might be favorable for a stricter regulation also for the private sector is Mexico's ratification of Convention 108 of the Council of Europe in 2018. At present, this Convention 108 is the only binding international convention on data protection and it is open also for non-members of the Council of Europe. Mexico's Senate of the Republic has also signaled its willingness to reform the ley to be able to ratify Convention 108plus, which is the modernized version of this Convention and includes new principles and rules for the age of Big Data and AI. Mexico's accession to the Convention 108plus, however, will require previous changes in its national law. Therefore, this Convention may become a lever for improving data protection and fundamental rights for Mexican citizens. An important event in this regard was the International Forum on Personal Data Protection in Mexico-City on 30-31 January 2020. Another impetus will be the International Computers, Privacy and Data Protection Conference CPDP to be hosted in October 2020 in Mexico-City which will create more public attention and awareness among policy-makers.

As already mentioned, Mexico does not yet have an extraterritorial clause in its law. Therefore, platforms like GAFAM but also Uber and other companies operating in Mexico always argue their legal seat to be in California or in the Netherlands, so that they cannot be subjected to Mexican data protection law. Even Mexican domestic firms have threatened to shift their data centers to US territory, should data protection rules be enforced too rigidly. Such a market location clause as present in the GDPR (see above) could possibly be introduced in the upcoming legal amendment but the new free trade agreement USMCA might contravene such attempts, as its regulations on data localization prohibit the use of local computer facilities or the establishment of such facilities as a condition for doing business in the country. To date, on the one hand, both domestic and foreign companies engage in forum shopping for the least rigid privacy standards. On the other hand, however, Mexican firms selling to the European market have to comply with GDPR rules, which puts pressure upon them to adjust their respective standards and internal data handling rules (– the "Brussels effect").

With the INAI (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales), Mexico has a strong, autonomous organism for data protection which also has sanctioning power. However, compliance with and enforcement of Mexican data protection laws is facing a number of challenges. Among them, especially in the private sector, are the lack of knowledge about the legal implications of the processing of information, a weak data protection culture, little sensitivity in the case of abuse of information and ignorance of the legal mechanisms to enforce the privacy rights (Mendoza Enriquez 2018, p. 289).

As yet, there is not a strong public discourse about digital issues in Mexico but the civil societies forces are awakening, among them hackers, data scientists and human rights organizations. Mexico has several non-governmental organizations which defend digital rights from the civil society's perspective, like R3D (Network for the defense of digital rights), SocialTIC promoting digital technology for social goals and Articulo 19, defending freedom of expression and right to information. Current campaigns for net neutrality and open data create more awareness and public mobilization about such digital issues. Mexico is also part of the Ibero-American Data Protection Observatory and the respective Latin American network of mostly professional data protection lawyers. Hence, with respect to data protection, Mexico seems to be more inclined to take part in the European search for a "Third Way".

With respect to competition law, Mexico is taking a more cautious approach. The Mexican Federal Economic Competition Commission COFECE is observing the international discussion very closely and is up to date with international debates (COFECE, 2018 and 2020). However, it does not want to inhibit market entries for new start-up companies. It also does not want to deter companies from innovating and its commissioners think that some disruptive forces can well be favorable for some sectors, such as for instance fintechs for the oligopolistic banking sector.

To date, the first case in which Mexico's competition authority COFECE prohibited an acquisition was with Walmart which was blocked from buying Cornershop, a company providing an App for home-delivery services. According to COFECE, this would have given too much power to Walmart which already possesses market dominance in Mexico. In other cases, mergers were authorized by COFECE (see cases in COFECE 2020, p. 9-10).

To sum up, Mexico has an AI and digital transformation strategy but its concrete agenda seems to be still in its infancy. Mexico doesn't have a market huge enough to be capable of exercising credible threat potential to large digital platforms, as does Europe whose huge domestic market is also politically integrated. In contrast, the 2020 United States-Mexico-Canada Agreement (USMCA) is hardly linked to political regulations related for instance to data protection issues. Therefore, Mexico has a smaller carrot and stick potential to deploy than European countries when it comes to platform regulation. Moreover, large companies can easily evade Mexican data protection laws. The proximity of the USA as a neighbor and main trading partner also suggests that the economy is leaning and aligning itself accordingly. Hence, the Mexican model can be characterized as a hybrid model between the US and the European model, still seeking for its own path in digital transformation and AI strategy.

8. Conclusions

We live in a time in which a struggle for digital supremacy is fought with increasing harshness. Technological races and platform economics have created power asymmetries, new geostrategic tensions and threats to democracy on an international scale. The four key elements of democracy indicated in the beginning are challenged by the following, a) free and fair elections are threatened by disinformation campaigns and manipulative use of social media, b) participation of citizens is enabled but also potentially distorted by social networks and the decline of quality media, c) human rights and privacy are often intruded and d) digital platforms try to escape the (national) rule of law by forum shopping and other forms of escaping regulation. The dominance of big digital platforms, their extraction and control of data, as well as their capacity to create and capture the ensuing value, tend to further accentuate consolidation and concentration rather than reduce inequalities between and within countries.

In the context of international competitive races, these governance models have emerged:

- The first, China's authoritarian surveillance state model, sees technology as a means of control, of maintaining and gaining power. Mass surveillance and censorship, including the social scoring system are exercised on the domestic level, while at the same time expanding technological power in the external arena. Technology thus is at risk of becoming a totalitarian and hegemonic instrument.
- The second, the US libertarian market model, rejects almost any regulation as an encroachment on the freedom of the market, the right to open speech and to the autonomy and self-regulation of the digital economic sphere. Network effects and other mechanisms work in favor of dominance and oligopolization. Moreover, it is those who develop and enact disruptive digital technologies who draw the line at what is possible. Facts created in the digital economic thus create digital norms, what is technologically possible is perceived as allowed.
- The third model is the European regulatory model which wants to foster the positive potential of digitalization, aims at catching up in digital competitiveness but also cares about maintaining its social contract. The EU's Third Way of a quest for digital sovereignty aims at defending the social welfare state, democracy, the market system and liberal values and has emerged as a "regulatory superpower" in the digital terrain. GDPR, anti-trust law, AI ethics

and the fight against international tax evasion have shown teeth and become role models for other countries to foster innovative international governance approaches.

- The fourth, Mexican model is a hybrid model which is aligned with US business standards and practices but takes Europe as a reference model in data protection. In competition law, the Mexican approach is cautious and pragmatic. Mexico's academic digital community and legal system have high standards but implementation of the norms leaves room for improvement.

Whether digital platforms, in particular the GAFAM and Tencent/Alibaba tech titans and Artificial Intelligence can and will be democratically tamed by regulations, is a challenge for the future. That they should be so, is a normative impetus for the digital transformation. This task is to be encountered with imagination, human intelligence and human agency. In scholarly terms, it is important to watch out for further paths and models, thus contributing to the visibility of the varieties of digital capitalism, in which alternatives are certainly possible.

9. References

All URLs were last accessed on 6 July 2020.

Au, Lvender & Kuuskemaa, Mats (2019, November 1). Social control or a fix for a non-law-abiding society? Mercator Institute for China Studies, https://www.merics.org/en/blog/social-control-or-fix-non-law-abiding-society

Banisar, David (2018). National Comprehensive Data Protection/Privacy Laws and Bills 2018 (September 4, 2018), http://dx.doi.org/10.2139/ssrn.1951416

Barocas, Solon & Selbst, Andrew D. (2016). Big Data's Disparate Impact. 104 California Law Review, 671, 673-693. https://doi.org/10.2139/ssrn.2477899

Bayona, Eduardo (2020). El Gobierno dice que cobrará la 'tasa Google' este año pese a las amenazas comerciales de EEUU, Público, 18 February 2020, https://www.publico.es/economia/consejo-ministros-gobierno-dice-cobrara-tasa-google-ano-pese-amenazas-comerciales-eeuu.html

Bendiek Annegret/ Schallbruch Martin (2019). Europas dritter Weg im Cyberraum, SWP-Aktuell Nr. 60, Nov. 2019, https://www.swp-berlin.org/10.18449/2019A60/

Bendiek, Annegret/ Römer, Magnus (2019). Externalizing Europe: the global effects of European data protection, Digital Policy, Regulation and Governance, 21(1): 32-43, https://doi.org/10.1108/DPRG-07-2018-0038

Böge, Friederike (2020). Wehe, wenn das Handy rot leuchtet, Frankfurter Allgemeine Sonntagszeitung, Nr. 18, 3 May 2020: 6.

Boyd, D. and K. Crawford (2012). Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon. Information, Communication, & Society 15(5): 662-679.

Braun, Fabrice (2020). Union der Rechenzentren, Süddeutsche Zeitung, 25.Mai 2020: 21.

Buckley, Chris & Mozur, Paul (2019). How China Uses High-Tech Surveillance to Subdue Minorities, New York Times, 22 May 2019, https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html

Cadwalladr, Carol (2019, April 15). Facebook's role in Brexit — and the threat to democracy [video file]. TEDTalk. https://www.ted.com/talks/carole_cadwalladr_facebook_s_role_in_brexit_and_the_threat_to_democracy/transcript

Christl, Wolfie (2017). Corporate Surveillance in Everyday Life, http://crackedlabs.org/en/corporate-surveillance

COFECE (Mexican Federal Economic Competition Commission) (2018). Rethinking competition in the digital economy, Competition Advocacy Studies, https://www.cofece.mx/wp-content/uploads/2018/03/EC-EconomiaDigital_web_ENG_letter.pdf

COFECE (2020). Digital Strategy, https://www.cofece.mx/wp-content/uploads/2020/03/EstrategiaDigital_ENG_V10.pdf

Cohen, Julie E. (2017). Law for the platform economy, 51 U.C. Davis Law Review 133 (2017).

Cohen, Julie E. (2019). Between truth and power: the legal constructions of informational capitalism. New York, NY: Oxford University Press.

Crémer, Jacques/ de Montjoye, Yves-Alexandre/ Schweitzer Heike (2019). Competition Policy for the digital era. Final report, Brussels: European Commission, https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf

Data Ethics Commission (2019). Federal Ministry of the Interior, Building and Community, Federal Ministry of Justice and Consumer Protection. Opinion of the Data Ethics Commission. Berlin: DEK. Available at: https://datenethikkommission.de/wp-content/uploads/DEK_Gutachten_engl_bf_200121.pdf

Der Spiegel (2015). Die Weltregierung. Wie das Silicon Valley unsere Zukunft steuert. (Cover story), 28 February 2015.

Diamond, Larry (2008). The Spirit of Democracy. New York: Times Books

EDPS (2014). Preliminary Opinion of the European Data Protection Supervisor. Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy. March 2014.

EDPS (European Data Protection Supervisor) (2015). Meeting the challenges of big data: A call for transparency, user control, data protection by design and accountability.

EDPS (European Data Protection Supervisor) (2018). EDPS Opinion on online manipulation and personal data, 19.03.2018, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

EU (2016). Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (Regulation (EU) 2016/679 of 27 April 2016), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

EU Commission (2020). White Paper. Artificial Intelligence -A European approach to excellence and trust, COM (2020) 65, 19.02.2020, Brussels, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

European Commission, High-Level Expert Group on AI (2019). Ethics Guidelines for Trustworthy AI. Brussels: European Commission, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

Ghoshal, Devjyot (2018) Mapped: The breathtaking global reach of Cambridge Analytica's parent company, March 28, 2018, https://qz.com/1239762/cambridge-analytica-scandal-all-the-countries-where-scl-elections-claims-to-have-worked/

Giesen, Christoph (2020: Wir können Dich sehen, Süddeutsche Zeitung, 16/17 May 2020: 47.

Giles, Martin (2019). 50 US attorneys general have launched an antitrust investigation of Google, MIT Technology Review, 9 September 2019, https://www.technologyreview.com/f/614287/50-us-states-have-launched-an-antitrust-investigation-of-google/

Gómez Mont, Constanza/ Martínez Pinto, Cristina (2020). Inteligencia artificial: una mirada desde México, Nexos, 01/02/2020, https://www.nexos.com.mx/?p=46682

Greenwald, Glenn (2014). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. New York: Metropolitan.

Hausstein, Alexandra & Zheng, Chunrong (eds.) (2018). Industrie 4.0/Made in China 2025. Gesellschaftswissenschaftliche Perspektiven auf Digitalisierung in Deutschland und China. 8th ed. [ebook]. Karlsruhe: KIT.

Hendricks, Vincent F. & Vestergaard, Mads (2019). Reality Lost. New York, USA: Springer Publishing. Open Access: Springer.

House of Commons (2019). Digital Culture Media and Sport Committee. Disinformation and 'fake news'. Final Report. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf

Hughes, Chris (2019, May 9). It's Time to Break Up Facebook. New York Times, https://www.nytimes.com/2019/05/09/opinion/sunday/chris-hughes-facebook-zuckerberg.html

ICIJ (International Consortium of Investigative Journalists) (2019). China Cables: Who Are the Uighurs and Why Mass Detention? November 2019, https://www.icij.org/investigations/china-cables/china-cables-who-are-the-uighurs-and-why-mass-detention/

Internet Society (2019). Policy Brief: Internet Shutdowns, https://www.internetsociety.org/policybriefs/internet-shutdowns

Kitchin, Rob (2014). The Data Revolution. London: Sage.

Kuo, Lily (2019). China bans 23m from buying travel tickets as part of 'social credit' system, The Guardian, 01 March 2019, https://www.theguardian.com/world/2019/mar/01/china-bans-23m-discredited-citizens-from-buying-travel-tickets-social-credit-system

LFPDPPP (2010). Ley Federal de Protección de Datos Personales en Posesión de Particulares, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

LGPDPPSO (2017). Ley General de Protección de Datos en Posesión de Sujetos Obligados, http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Lichfield, Gideon (2018). Why the pessimists are winning, for now, MIT Technology Review, August 22, 2018, https://www.technologyreview.com/2018/08/22/140680/why-the-pessimists-are-winning-for-now/

Lippert, Barbara & Perthes, Volker (eds.) (2020). Strategic Rivalry between United States and China. Causes, Trajectories, and Implications for Europe, SWP Research Paper 4, April 2020, doi:10.18449/2020RP04.

Lyon, David (2003). Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination. Abingdon,UK: Routledge.

Lyon, David (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. Big Data & Society, 1(2). https://doi.org/10.1177/2053951714541861

Maas, Heiko (2019). Rede von Außenminister Heiko Maas zur Eröffnung der Konferenz FUTURE AFFAIRS - "Digital Revolution: Resetting global power politics?", 29 May 2019, https://www.auswaertiges-amt.de/de/newsroom/maas-future-affairs/2222076

Macrotrends (2020). Facebook Market Cap 2009-2020, https://www.macrotrends.net/stocks/charts/FB/facebook/market-cap, last accessed 18 May 2020.

Maqueo Ramírez, María Solange & Barzizza Vignau, Alessandra (2020). Democracia, privacidad y protección de datos personales. Ciudad de Mexico: INE.

Mendoza Enríquez, Olivia Andrea 2018: Protection of Personal Data in Companies Established in Mexico, Revista del Instituto de Ciencias Juridicas de Puebla, Mexico, Vol. 12, No. 41: 267-291.

O'Neil, Cathy (2017). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. London, UK: Penguin Books.

Ohlberg, M. Ahmed, S. and Lang, B. (2017). Central Planning, local experiments. The complex implementation of China's Social Credit System. https://www.merics.org/sites/default/files/2017-12/171212_China_Monitor_43_Social_Credit_System_Implementation.pdf

Orwat, Carsten (2019). Diskriminierungsrisiken durch Verwendung von Algorithmen. https://www.antidiskriminierungsstelle.de/SharedDocs/Downloads/DE/publikationen/Expertisen/Studie_Diskriminierungsrisiken_durch_Verwendung_von_Algorithmen.html

Osnos, Evan (2018). Can Mark Zuckerberg Fix Facebook Before It Breaks Democracy? New Yorker, 17 September 2018. https://www.newyorker.com/magazine/2018/09/17/can-mark-zuckerberg-fix-facebook-before-it-breaks-democracy

Pew Research Center (2020). Many Experts Say Digital Disruption Will Hurt Democracy, by Janna Anderson & Lee Rainie, 21 February 2020, https://www.pewresearch.org/internet/2020/02/21/many-tech-experts-say-digital-disruption-will-hurt-democracy/

Rudinow Saetnan, Ann/ Schneider, Ingrid/Green, Nicola (2018). The Politics of Big Data: principles, policies, practices, in: The Politics of Big Data: Big Data, Big Brother? (eds.), New York: Routledge: 1-18.

Scheiber, Noam/ Conger, Kate (2020). The Great Google Revolt, New York Times Magazine, www.nytimes.com/interactive/2020/02/18/magazine/google-revolt.html

Schlereth, Patrick (2018). Fakebook, D+C Development and Cooperation, 45(5-6), https://www.dandc.eu/en/article/worlds-largest-social-network-does-not-fight-fake-news-and-disinformation-convincing-way

Schmidt, Eric & Cohen, Jared (2013). The New Digital Age: Reshaping the Future of People, Nations and Business. London: John Murray.

Schneider, Ingrid (2018). Bringing the state back in: Big Data-based capitalism, disruption, and novel regulatory approaches in Europe, in: Schneider, I.; Rudinow Saetnan, A.; Green, N. (eds., 2018). The Politics of Big Data: Big Data, Big Brother? New York: Routledge: 129-175.

Schneider, Ingrid & Ulbricht, Lena (2018). Ist Big Data fair? Normativ hergestellte Erwartungen an Big Data, in: Heil, R./ Kolany Raiser, B./ Orwat, C. (eds.): Big Data und Gesellschaft. Eine multidisziplinäre Annäherung. Wiesbaden: Springer VS;

Schneier, Bruce (2015). Data and Goliath: The hidden battles to collect your data and control your world. New York, USA [et.al.]: W.W. Norton.

Schoen, John (2018). Here's how Amazon's $1 trillion market cap stacks up against the rest of the S&P 500, CNBC, 4 Sep 2018, https://www.cnbc.com/2018/09/04/heres-how-amazons-1-trillion-market-cap-stacks-up-against-the-rest-of-the-sp-500.html

Snowden, Edward (2020). Permanent Record. New York; Metropolitan.

Srnicek, N. (2017). Platform capitalism. Malden, MA: Polity.

Statcounter Global Stats (2020). https://gs.statcounter.com/ and https://gs.statcounter.com/os-market-share/mobile/mexico

Statista (2020a). https://www.statista.com

Statista (2020b). https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/, last accessed 18 May 2020.

Stone, Brad / Silver, Vernon (2015). Google's $6 Billion Miscalculation on the EU, Bloomberg Business, 6 August 2015, https://www.bloomberg.com/news/features/2015-08-06/google-s-6-billion-miscalculation-on-the-eu

Strittmatter, Kai (2019). We Have Been Harmonised: Life in China's Surveillance State. London: Old Street Publishing.

The Economist (2017). The world's most valuable resource is no longer oil, but data, 6 May 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

The Economist (2020). Big tech's $2trn bull run, 20 February 2020, https://www.economist.com/leaders/2020/02/20/how-to-make-sense-of-the-latest-tech-surge

Turner, Fred (2006). From Counterculture to Cyberculture. U Chicago Press.

Turner. Fred (2017). Don't Be Evil. On Utopias, Frontiers, and Brogrammers, Logic, Issue 3, December 01, 2017, https://logicmag.io/03-dont-be-evil/

UNCTAD (United Nations Conference on Trade and Development). (2019). Digital Economy Report 2019. Value Creation and Capture: Implications for developing countries. New York.

UNICEF (2017). Children in a Digital World. The State of the World's Children 2017. New York.

van Dijck, José/ Poell Thomas & Martijn de Waal (2018) The Platform Society. Public Values in a Connective World. Oxford: Oxford University Press.

Villani, Cédric (2018). For a meaningful artificial intelligence. Towards a French and European Strategy. Report, https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf

Vogel, David (1995). Trading Up: Consumer and Environmental regulation in a global economy. Harvard University Press. Cambridge, MA.

Yi Min Shum (2020). Situación digital y social media en México 2019, https://yiminshum.com/digital-social-media-mexico-2019/

Zand, Bernhard (2018). China's Xinjiang Region. A Surveillance State Unlike Any the World Has Ever Seen, Der Spiegel International, 26.07.2018, https://www.spiegel.de/international/world/china-s-xinjiang-province-a-surveillance-state-unlike-any-the-world-has-ever-seen-a-1220174.html

Zuazo, Natalia (2018). Los dueños de internet. Buenos Aires: Penguin.

Zuboff, S. (2020). The Age of Surveillance Capitalism. New York: Public Affairs.

About the Author

Prof. Dr. phil. Ingrid Schneider is Professor of Political Science and works since 2017 in the Centre for Ethics of Information Technology in the Department of Computer Science at the University of Hamburg. She focuses on the epistemic, political-economic and socio-political implications of digitization, Big Data, algorithms, artificial intelligence and platform industries. From 2002-2016, she was a senior researcher in technology assessment at the Research Centre Biotechnology, Society and Environment (BIOGUM) at the Universität Hamburg and worked on the democratic handling of ethical value conflicts and on Responsible Research & Innovation (RRI). She did research on technology assessment of numerous topics in the biomedical and informational sciences. In 2010 she completed her habilitation on the governance of intellectual property, and in 2014 she became a professor of political science at Universität Hamburg. In 2014 she had a guest professorship for political science at the University of Vienna, Austria. She has advised the German Bundestag and has acted as policy advisor to the European Commission, the European Parliament and other parliaments as well as the European Patent Office. She is a member of the Central Ethics Commission (ZEKO) of the German Medical Association, a member of the Executive Board of the EPIP Association (European Policy for Intellectual Property) and various scientific advisory boards.