

Kosals, Leonid. Legitimation of innovation: The case of AI technology for facial recognition. In Radaev, V. and Kotelnikova, Z. (eds). 2022. *The Ambivalence of Power in the Twenty-First-Century Economy: Cases from Russia and beyond*. London: UCL Press. <https://doi.org/10.14324/111.9781800082687>, pp. 80-99

5

Legitimation of innovation: The case of AI technology for facial recognition

Leonid Kosals

Introduction

Social ambivalence is closely tied to both social change and resistance to social change (Hajda 1968, 25). As such, social ambivalence is an essential part and by-product of innovation. Innovation includes so-called creative destruction (Schumpeter 2010) – the emergence of some new products, technologies, organizational forms, institutions and so forth and, at the same time, removal of outdated elements of technological and social systems. This ‘embedded ambivalence’ is ramified in various parts of an organization and society, including social realms such as markets, enterprises, non-governmental organizations (NGOs), families, values and power relations.¹ Alongside positive technological change, this ramification produces uncertainty, social tensions and disorganization within these realms, in particular damaging the system of social values.

The focus of this chapter is the societal response to ambivalence in innovation. Apparently, the purpose of this response in all times and circumstances is to make favourable conditions for acceleration of the benefits of innovation and to neutralize its destructive aspects. However, in various countries with different socio-economic and socio-cultural settings, understanding of the positive outcomes and destructive effects may vary. What is perceived as unacceptable in some settings is considered quite normal in others, and vice versa. And these variations significantly depend on the system of values.

In his seminal book *Active Society*, Amitai Etzioni (1968) argued that if society is going to protect its core values from the destructive

aspects of technological change, it should actively change itself by undergoing societal restructuring. The focus of the book was on societal change as a response to the dark side of innovation, which can harm society, even if it is inactive. However, the book did not consider societal 'activeness' in the realm of innovation: the active societal response to the social selection and restructuring of the realm of innovation, which also serves to protect the core values of society, was not analysed properly. Meanwhile, if we look at the diffusion of various innovations in different socio-political and socio-cultural contexts, we can see that the same innovation can be accepted in some countries and rejected in others due to active changes being made to specific innovations in order to protect core values. Despite the fact that there have been many studies on the social aspects of innovation since the publication of *Active Society* (see the updated look on *Active Society* in [McWilliams 2006](#)), the link between core values and the social selection of innovation remains understudied.

Active Society came out at the beginning of the third industrial revolution, when information technologies started changing industry and society. The ongoing fourth industrial revolution has now renewed the research agenda for studies into the link between core values and technologies. At the core of the fourth industrial revolution is the transformation of the production process at industrial enterprises, the emergence of the so-called smart factory that will operate as a 'cyber-physical system'. This system is a set of computer-controlled processes and objects, including robots, which interact with the external environment, where software and physical elements closely intertwine and interact with each other in many ways automatically and without human intervention ([Mousterman and Zander 2016](#)). Such enterprises will be very flexible, paying much greater attention to individual customer requirements than traditional management. At the same time, due to its greater flexibility and customization, it can serve a much broader, global market than traditional industrial companies. These will be highly automated firms in which cloud technologies, big data, the Internet of Things, 3D printing and so forth will be widely used, with decentralized decision-making ([Shrouf et al. 2014](#); [Wang et al. 2016](#)). Artificial intelligence (hereinafter referred to as AI) is a kind of electronic brain of such enterprises, which is necessary to coordinate the functioning of various elements of a smart enterprise, as well as to provide a flexible interface when a person interacts with its various subsystems. In this capacity, it is an essential element of the fourth industrial revolution ([Skilton and Hovsepian 2018](#); [Benotsmane et al. 2019](#)). Therefore, for this research I have chosen AI technology as one of

the key elements of the fourth industrial revolution, often representing the bright side of the innovation.²

Meanwhile, AI technologies have their dark side, which is reflected in public opinion. On the one hand, there are acute, traditional (anti-) technological fears about the jobless economy, technological unemployment, inequality and so forth (Aronowitz and DiFazio 2010; Frey and Osborne 2013; Mokyr et al. 2015). The global COVID-19 pandemic, alongside the many widespread conspiracy theories, exacerbated these fears.

On the other hand, the empirical evidence does not support many of these fears, although some of them turn out to be well founded. For example, a recently published extensive study of the influence of robots on the labour market in 74 developed and developing countries in 2004–16 showed that robotization positively affects labour productivity and employment and negatively influences inequality in the sample as a whole: 'It further appears that increased robot adoption makes the rich become richer, although no evidence of so-called technological unemployment is witnessed' (Fu et al. 2021, 678). Additionally, robotization influences developed and developing countries heterogeneously: there is a positive effect on labour productivity and employment in developed countries but no significant evidence for such in developing states (Fu et al. 2021). This is evidence of embedded ambivalence in the influence of new technologies on society and its core values during intense processes of change, while the diffusion of innovation is at an initial and therefore fragile and contested stage. Therefore, it is still unclear what the balance sheet of pros and cons of innovation is and to what extent innovation harms the core values of society.

In this chapter, I offer several methodological lenses for the study of the legitimization of innovation as a useful tool for understanding why in some socio-economic contexts innovation is thriving, whereas in others it has been inhibited or even stopped. I argue that there are opposite responses to the embedded ambivalence in innovation from countries with various core values: democratic with high value of human rights versus non-democratic states where human rights are undervalued. The first group is represented by the United States and Canada, whereas China represents the opposite side. Russia is in-between these two opposite entities. Being 'between East and West',³ Russia has ambivalent core values, which makes it an especially interesting case for analysing innovation, as a study of 'double ambivalence', since innovation itself has a dual nature.

The chapter includes a literature review where the classic and modern views on legitimacy are considered. Then I describe the methodology of the case study to apply to AI facial recognition technology in comparative socio-economic and cultural contexts. This piece includes

the analysis of variations in the societal response to ambivalence in innovation in four countries: Canada, the US, Russia and China. The chapter ends with a discussion of the proposed case and my conclusions.

The literature review

The classic view on legitimacy, developed by Emile Durkheim and Max Weber, focused on the legitimacy of authority and the state. They researched the moral grounds of political authority, the state and state building to analyse the social roots of sustainable political order beyond force and violence to explain why individuals do or do not support law and order and political authority. As Weber argued, 'the basis of every system of authority, and correspondingly of every kind of willingness to obey, is a belief, a belief by virtue of which persons exercising authority are lent prestige' (Weber 1964, 382). As is well known, he identified three major sources of legitimacy: tradition, charisma and the legality of authority.

Emile Durkheim, who considered the state an 'organ of social thought',⁴ argued that to establish a social order, two-way relations should be in place whereby the people obey social order and the state 'tells them what is right'.⁵ At the same time, it is worth noting that he outlined the difference between the West and Russia in these two-way relations:

In the West, the state has succeeded in superimposing itself on political orders already in existence and divided among themselves by all sorts of conflicts of interest, and it has made it its business and *raison d'être* to merge them and unify them. In Russia, by way of contrast, it is unity that is more of a primary factor, and it is the state that has dispersed the population into distinct political orders; it is the former which has divided the inhabitants into categories and classes in order to give society a more solid base. (Durkheim 1998, 345)

In other words, according to Durkheim, in the West society is relatively autonomous from the state and they interact as equal entities at least, while in Russia the state plays the prime and leading role in shaping the social order. Potentially, this approach assumes that there can be various problems with legitimizing authority in Russia and that the role of moral grounds and citizens' obedience can be different from the West too.

In the twentieth century, Carl Schmitt played a prominent role in the study of legitimacy. He revealed and analysed the conflicted

relationship between legitimacy and legality in the 1930s (Schmitt 2004), which is of special importance for this research. Schmitt demonstrated the controversial relationship between the two concepts in that any social phenomenon can be simultaneously legal but illegitimate or illegal but legitimate. In turn, this conflict can generate social controversies in various political and economic structures, which can harm the core values of society and often may only be resolved after much social upheaval and loss of life. For example, the conflict between legality and legitimacy in the Weimar Republic that was the focus of Schmitt's study was only resolved by Germany's defeat in the Second World War.

Considerable research on legitimacy in disciplines such as political science, economics and management, law and criminology, public administration, anthropology and sociology has been carried out over the last few decades.

Sociological research on the legitimacy of innovation began relatively recently, mainly in the past two decades. In these studies, legitimacy is treated as a social process, where legitimacy can be acquired through social interactions by participants in the development, diffusion and use of a new product (technology, organizational form or services) among themselves and with the state and society, including local communities, city residents, NGOs and others (Johnson et al. 2006). In this chapter, this very process of acquiring (or not acquiring) legitimacy will be called legitimation. I categorize these studies into two groups. The first includes the legitimacy of innovation when a new market for a new product emerges (Navis and Glynn 2010; Markarda et al. 2016; Wang et al. 2019). The second focuses on the legitimacy of innovation in particular companies or any other agents (Blanco et al. 2013; Petkova 2018; Schoon and DeRoche 2019).

A good example of research in the first group is Navis and Glynn's study of the legitimacy of satellite radio technology in 1990–2005 (Navis and Glynn 2010). In order to understand how new markets emerged, the authors analysed the diffusion of the technology by means of qualitative and quantitative data. They revealed that the technology was legitimized in 2002 when it became widely available in the retail sector and its subscribership grew significantly. Overcoming the legitimacy threshold in 2002 led to the institutionalization of the technology. The self-presentation of the companies and the attention of the consumer then shifted from the shared, collective identity (as 'satellite radio' providers) to the individual firms. This helped some companies achieve a competitive advantage and, in particular, to occupy a more exclusive satellite radio category (for example, as a premier sports channel).

A good example of research in the second group is Petkova's study of the legitimation of digital technologies in the recently established e-commerce fashion industry (Petkova 2018). She showed how one of the newly established players in this industry struggled to achieve legitimacy in the eyes of traditional fashion companies as well as their peers in digital fashion. The author revealed that traditional fashion media companies that mimicked online their traditional offline practices but did not closely interact with their online peers failed. They relied on the pragmatic legitimacy of their offline parental companies and failed because of the lack of moral legitimacy in the realm of digital fashion. Interestingly, some major internet companies, possessing moral and pragmatic legitimacy in the digital space, failed in the digital fashion industry due to their lack of pragmatic legitimacy in traditional fashion. Meanwhile, the company in question, while achieving pragmatic legitimacy in the traditional fashion industry, established alliances with their peers in digital fashion that helped them achieve moral legitimacy in both worlds, traditional and digital fashion. As a result, being an outsider at the very beginning, the company later became one of the largest global e-commerce fashion retailers.

Sociological studies of the legitimacy of innovation have identified four stages of legitimation (Johnson et al. 2006). In the first stage, the innovation emerges in response to an existing unmet need, often at the local level. In the second stage, the innovation is adopted locally. It acquires support and a social licence to operate in a limited space, including a separate small group, organization or territory. In the third stage, the innovation starts to be diffused when it begins to be accepted by other local communities. Finally, in the fourth stage, the innovation is widely diffused when it becomes familiar to large social groups, jurisdictions, territories and states. At the same time, the legitimation of one or another innovation may not go beyond any of these stages. For example, it may stop at the second stage, that is, not go beyond the local community.

However, these studies failed to address the social mechanisms underpinning the legitimation of innovation having an ambivalent nature, in particular the role of the core societal values. What are the factors that influence legitimation in various political, socio-economic and socio-cultural contexts? Do core values play any role? These are the main research questions for the research presented in this chapter.

Research methodology

Depending on the focus of analysis, the literature distinguishes between different types of legitimacy, such as international legitimacy (Neuman 2018) or political legitimacy (Giannini 2018). Given the focus of our research, we will consider the legitimacy of innovation in three social contexts: the state, business and the population. While it is, of course, possible for legitimacy to be recognized in only one or two contexts, such as business and the state, the particular form of innovation must be recognized in all three contexts for it to acquire 'full' legitimacy. In some cases, 'partial' legitimacy may be enough for the successful diffusion of the innovation; for example, business legitimacy may be sufficient for a business-to-business niche innovation. In other situations, for example, if an innovative product is offered to the population and the population 'does not recognise' it, partial legitimacy can quite significantly slow down the diffusion of innovation.

With regard to the essence of the innovation process, I distinguish three types of legitimacy: cognitive, pragmatic and moral. The cognitive includes more or less complete and realistic information and knowledge about the content of the innovation. Pragmatic legitimacy is expressed in the belief that the innovation brings practical benefits (financial profits, improved satisfaction of a particular need, achievement of political goals, etc.). Moral legitimacy means that the innovation has a moral justification, helps to achieve higher social goals and does not violate moral norms but rather promotes social justice and the integration of communities and society as a whole, contributes to the improvement of people's lives, helps vulnerable social groups and so forth (Kumar and Das 2007; Bunduchi 2016; Petkova 2018). In other words, these three types of legitimacy reflect the extent to which different social groups have knowledge about new technologies, whether they believe that these technologies bring practical benefits and in what form, and also whether they harm society and its highest social goals. In this chapter, I plan to focus on both pragmatic and moral legitimacies.

At the same time, the acquisition of legitimacy or legitimation is a social process, that is, it unfolds over time, embracing the four aforementioned stages. All these stages are accompanied by social interactions between the actors in the development and implementation of the innovation between themselves and the external environment.

In this study I proceed from the assumption that the diffusion of the innovation (AI technologies) depends on its legitimation: if these

technologies are legitimate, then the social interactions of the agents contribute to the acceleration of the development and diffusion of AI technologies; if they are not, then social barriers arise in AI's path, which complicate or even halt its development and diffusion.

At the core of the problem under examination is *the ambivalent relationship between pragmatic and moral legitimacies*: pragmatic legitimacy can be achieved without the moral legitimacy associated with the threat of potential or real harm to higher social goals (morality, social integration, etc.), first of all, because of creative destruction. The speed and success of the diffusion of AI technologies as well as their real socio-economic effect and the trade-off between benefit and harm depend on how this conflict is resolved in a particular state, jurisdiction or territory.⁶

Nevertheless, the diffusion of illegitimate innovations (or innovations with contested/partial legitimacy) is possible if there is pressure from the state or influential non-state actors, which, in turn, can lead to various negative formal and informal social and economic effects and forms of dysfunction for individuals, organizations and society in general.

These cases are of particular interest for our research and therefore we are intentionally considering a case of diffusion of innovation with 'contested' legitimacy. Such cases explicitly highlight the role of core societal values in contrast to cases where legitimacy was achieved without significant controversy because in the former case the involved actors are certainly in the position of having made an actual choice. Concisely, it is the case when values matter.

To study the legitimation of innovation we chose the case study methodology. As John Gerring argued, comparing this methodology to the conventional quantitative approach, its strength lies in the opportunities for the analysis of the causal mechanisms: 'the opportunities for investigating causal pathways are generally more apparent in a case study format' (Gerring 2007, 48) and '[c]ase studies are thus rightly identified with "holistic" analysis and with the "thick" description of events' (Gerring 2007, 49).

Looking for a case of AI technology with 'contested legitimacy', I selected facial recognition technology, where the legitimacy of AI technology is challenged and its diffusion is controversial and faces opposition in society, especially its use by the police. I describe the legitimacy of this technology in North America, China and Russia, cases where there are acutely salient differences in the outcomes of the social mechanism for legitimation.

The case of facial recognition technology

Canada

The [Office of the Privacy Commissioner of Canada](#) (OPC) released the Joint investigation of Clearview AI report (Joint Investigation of Clearview AI, Inc. 2021) on its investigation of the activities of the US-based firm Clearview AI on 2 February 2021.⁷

Clearview AI offers police departments and other law enforcement agencies a computer-based AI facial recognition system. The data set for this software includes almost 4 billion computer images and related personal data, which were collected from social media and other open internet sources. Hundreds of law enforcement agencies throughout North America use this technology, although Clearview AI has suspended sales of the technology to private firms since mid-2020. This technology showed very high efficiency and some police officers who use it say it is helping to solve crimes:

In February (2019), the Indiana State Police started experimenting with Clearview. They solved a case within 20 minutes of using the app. Two men had gotten into a fight in a park, and it ended when one shot the other in the stomach. A bystander recorded the crime on a phone, so the police had a still of the gunman's face to run through Clearview's app. They immediately got a match: the man appeared in a video that someone had posted on social media, and his name was included in a caption on the video. 'He did not have a driver's license and hadn't been arrested as an adult, so he wasn't in government databases,' said Chuck Cohen, an Indiana State Police captain at the time. ([Hill 2020](#))

Although police in North America have used facial recognition technologies for almost two decades, they are restricted to government-generated data sets and, as a result, their capacity is much less than that of Clearview AI; even the FBI's database is ten times smaller ([Hill 2020](#)).

The aforementioned report argued that this technology violates the Privacy Act and cannot be used in Canada because the personal data included in the database were collected without the consent of citizens. Moreover, there was a requirement for Clearview AI to remove all information about residents of Canada and not to use it in Clearview AI products in other countries. Previously, about 50 organizations in Canada had used Clearview AI technology, but most of them suspended its use

after the OPC announced the launch of an investigation in mid-2020. The release of the report means a de facto ban on its use in Canada.

This is not the first time in Canada that the OPC has called for a ban on facial recognition technologies. The OPC released a report on their investigation of the Cadillac Fairview Corporation Limited (Joint Investigation of the Cadillac Fairview Corporation Limited 2020) at the end of 2020. The report concluded that Toronto-based Cadillac Fairview, one of North America's largest office owners, had built software in its information kiosks in 12 large malls that collects images of visitors without their knowledge and estimates their approximate age and sex, as well as other information. In total, they collected more than 5 million images of buyers. The report argued that this practice was contrary to the Privacy Act. The day after the report was released, Cadillac Fairview announced that it was removing the software in question from its information kiosks.

In Canada a considerable number of academic articles and reports as well as reports from human rights organizations have analysed algorithms and AI technologies, including facial recognition. Many of them included critical assessments of the dangers of these algorithms in terms of human rights violations,⁸ which also played a role in shaping public attitudes towards these technologies.

This, of course, does not mean that facial recognition technologies, and AI technologies in general, are prohibited in Canada. However, this suggests that they face a rather tough social filter, embedded in the public's fears that these technologies may cause them some significant harm. This filter prevents facial recognition technologies from being diffused as quickly as they would otherwise be if only economic and technological factors were at play.

The United States

The United States is characterized by a much wider variety of legal and enforcement practices. In particular, there is no federal privacy law that could limit the diffusion of AI facial recognition technologies to the same extent as in Canada. Facial recognition technologies such as Clearview AI are used in many US regions and cities but in some they are also restricted or prohibited. The social response to these technologies is strong and varied. In particular, the authorities of a number of states, individuals and companies, including Facebook, YouTube and others, filed lawsuits against Clearview AI. However, not all claims have been resolved in the courts. In some police departments, commercial facial recognition

technologies, including Clearview AI, are forbidden, for example, in the Los Angeles police department, one of the largest in the United States. Thus, the legitimization of facial recognition technologies in the United States is still in process and, while it is unclear what restrictions society wishes to place on them and what requirements society has of them, they are now in the process of being formed as a result of the discussion of lawsuits and public debates. At the same time, there is also a significant corpus of academic articles and reports from human rights organizations with critical assessments of these technologies.

The situation in North America by no means exhausts the diversity of the process of legitimization of AI technologies.

China

Unlike North America, China has almost no barriers to the diffusion of facial recognition technologies or any other AI technologies. There have been no human rights lawsuits, public criticism or opposition to these technologies, which, of course, does not mean that everyone in China supports them. It is known that in China they diffuse at a very high rate. For example, there were more than 100 million people using facial recognition technology for mobile payments in 2019, which, of course, facilitates and speeds up the payment process but comes with a loss of privacy (Kawakami and Hinata 2019). There are many uses for this technology in China, including its extensive use by the police and other law enforcement agencies, one example being the total surveillance and control system established in the Xinjiang Uygur Autonomous Region (Leibold 2020). It includes a whole range of modern technologies (voice and facial recognition, GPS tracking and other machine learning technologies) aimed at achieving the socio-political and ethno-cultural goals of total control and changing the behaviour and consciousness of an entire ethnic group.

Moreover, China actively exports electronic surveillance technologies to many countries: these Chinese technologies are now used by consumers in more than 80 countries (Greitens 2020). Of course, many of them, including Russia, are trying to diversify their supply and not depend solely on China (Kovachich 2020). It is unclear, however, to what extent it is not only the technologies that are exported, but also the accompanying socio-cultural norms and standards for their application.

PwC has predicted that AI technologies will make a 14 per cent contribution to the growth of the world economy in the period 2017–30, which is approximately 15.7 trillion dollars, of which China will be the

main beneficiary, gaining a 26 per cent share, while North America will achieve an average of just 14 per cent (Rao and Verweij 2017).

Russia

Facial recognition technologies are actively developed and used in Russia. For example, one of the world's largest urban video surveillance systems has been set up in Moscow (Kovachich 2020). In explaining their extensive investment in the system, the Moscow authorities argued that it would do a lot to fight crime in the city. However, no solid evidence has been provided about how successful and effective this system has been in fighting crime. People have reasonable doubts about establishing facial recognition in Moscow, which could be derived from the existence of the so-called *palochnaya sistema*, the quasi-centralized system of planning in operation in Russian law enforcement (Paneyakh 2014). This system incentivizes police officers who select which cases to pursue to reject those that are hard to solve. Very often, police officers refuse to register such 'hard cases' and address only offences that are easy to investigate and where it is easy to convict a perpetrator. As a result, people have a lack of confidence in the police and often do not report crimes at all. Therefore, the Russian criminal justice system is overwhelmed with latent crime, including offences that the police refused to register or that were not reported by the victims. And facial recognition technology cannot eliminate this institutional feature of the criminal justice system rooted in the peculiarities of Russian politics.

However, there is considerable evidence that this system is being used beyond regular crime fighting, firstly by targeting activists engaged in political protest.⁹ Secondly, the system was extensively used during the COVID-19 pandemic. The Moscow authorities as well as those of some other cities established a system of so-called social monitoring to trace people who had contracted the coronavirus based on facial recognition and then punish those who violated the rules. For example, in Moscow up to July 2020, more than 447,000 people were registered on the system, and nearly 94,000 penalties were imposed, mostly for leaving home,¹⁰ despite the technology's 20–25 per cent error rate; even in cases of technological errors, penalties have sometimes still been upheld by the courts.¹¹ In other words, the system was used not to fight crime but to control people's behaviour.

Moreover, a black market for offers to access the facial recognition system has emerged in Moscow (Kaganskikh 2019). Anyone willing to pay a small amount of money (200–300 US dollars) online can be granted limited access to the facial recognition system in Moscow to trace her/his business competitor, wife or husband and so forth.

This causes, among other things, public criticism, similar to that which exists in many Western countries from the standpoint of human rights violations. In Russia, lawsuits were also filed against these technologies on grounds of human rights violations based on the Federal Law of 27 June 2006 No. 152-FZ On Personal Data. However, all the decisions of the courts went against the plaintiffs.¹²

Thus, in Russia, the social filter, although it has some effect, is obviously weaker than in North America and, as a result, the video surveillance system continues to expand, without encountering salient obstacles that such technologies face in some other countries. For example, quite recently, at the height of the coronavirus pandemic, in December 2020, the Moscow authorities announced an auction to develop technology for the recognition of human silhouettes.¹³

Discussion: power with and without ambivalence

The case study of AI facial recognition technology shows that the acceptance and diffusion of innovations are not only dependent on technological, economic and legal factors. While it is, of course, important how well a particular technology works, how much profit it generates for a business and whether its application violates the law, it is also very important to understand the diffusion of innovations as a social process. It involves many actors with their own systems of values and motives, and it depends on the attitude of both society as a whole and various influential social groups, organizations and institutions, including human rights organizations, political parties, government agencies and others. Their position, assistance or opposition can have multiple consequences for the diffusion of a particular innovation. Possible consequences could be that the innovative products will turn out to be too expensive due to the introduction of additional regulatory standards (taxes, labour safety standards, etc.), may be slowed down due to the requirements of additional expertise and the provision of information on safety, for example, or stopped altogether.

Thus, it may turn out that the same technology can diffuse quickly and smoothly in one socio-political and cultural context (country or region), more slowly and with difficulty in a second, and be generally prohibited in a third.

Power is well embedded in the social interactions about the diffusion of innovation in a 'Foucauldian' way: it is everywhere (Foucault 1998). And every step the innovation takes along the path towards legitimation is the result of many encounters by the 'micro-powers', where sometimes those

interested in pushing innovation through and those interested in blocking it interact with each other. Of course, often the trajectory of their efforts can finally coincide, and then legitimacy is successfully achieved or happily blocked. There is no explicit ambivalence of power in such a case.

However, power is well embedded in creative destruction too. As such, power is an element of the embedded ambivalence of innovation since creative destruction is an essential side of the innovation process and some parts of the technological and social systems should be removed to provide legitimacy and diffusion of innovation. During power conflicts at legitimation, both agents of innovation and potential victims use their own powers. The former try to innovate, while the latter strive to protect their status. In the case of AI facial recognition technologies, the victims of creative destruction are large social groups who can lose their individual privacy and human rights.

After all, the outcomes of this struggle depend on core values.¹⁴ One of their dimensions is the role of human rights, support for which is high in democratic and low in non-democratic societies. In Canada, which, among our case studies, has the most stringent human rights laws including the Privacy Act, the social filter is the toughest, with many AI facial recognition technologies banned despite their potential economic benefits. In other words, although pragmatic legitimacy was achieved, the moral legitimacy of some facial recognition technologies failed. In the United States, where human rights are not so consolidated as in Canada, the moral legitimacy of the same technologies is contested, and their legitimation is still in process.

In China, with its socialist system of appropriate collectivist values without a pronounced idea of human rights for individuals, both pragmatic and moral legitimacies are achieved. As a result, the diffusion of facial recognition technologies is the fastest.

In the cases of Canada and China, there is no explicit evidence of the ambivalence of power, whereas the cases of Russia and the United States are more complicated.

Russia is an interesting case of a society with pronounced ambivalence in its core values. On the one hand, Russia has laws for the protection of human rights including the Federal Law on Personal Data. The contents of the Russian laws on human rights are not much different from those in the West, including North America. On the other hand, the authorities and courts in Russia often do not use these laws in the same way as in the West. This is because the gap between 'law in action' and 'law on the books' (Gould and Barclay 2012) is significantly larger in Russia than in the West. This gap is so big that one can talk of selectivity in Russian law enforcement.¹⁵

This is in line with the Russian legal tradition with its legal dualism, formalism, technicality and instrumentalism of the law (Hendley 2011; Borisova and Burbank 2018; Kurkchiyan 2018; Bækken 2019). This legal setting shapes the preconditions for the ambivalence of power while legitimizing facial recognition technologies: the Russian authorities maintain the Law on Personal Data and simultaneously push through the innovation with contested legitimacy, which may violate this law. The Russian authorities not only fail to initiate investigations, as in Canada, or conduct due process, as in the United States, but also, when citizens go to court, the authorities usually dismiss their claims or informally influence the judges to refuse a plaintiff's case. We could call this the Russian-style relationship between state and society, as Durkheim argued. However, in contrast to the late nineteenth and early twentieth centuries, this relationship has become saliently ambivalent because the society in Russia today has become more active than at that time. This understanding is rather in line with the critiques and further developments of Durkheim's analysis of Russia, as M. Gane argued, considering Durkheim's thesis that Russian society is rather the product of the state, and not vice versa.

This is not I think to be interpreted, as Horowitz has recently suggested, to mean that this inversion of state and society was 'the source of autocracy, an order based on coercion rather than on consent' (Horowitz 1982, 371) but to suggest 'the limits, the superficiality of the society thus created' (Gane 1984, 327). Moreover, Russian society, being in some sense relatively 'superficial', appeared as active, trying to protect its core values in its interactions with an authoritarian state in the case of the legitimation of facial recognition technologies.

As a result, the decision of the authorities to push the diffusion of facial recognition technology without full legitimacy has produced some negative effects. This means that, although pragmatic legitimacy is achieved in terms of political gain for the authorities, there is no full moral legitimacy and therefore there is no clear path for the diffusion of facial recognition technologies in Russia, as there is in China.

In the US case, where there is no ambivalence in society's core values, the source of the ambivalence in power, with regard to the legitimation of innovation, is the highly decentralized legal system and mechanism of law enforcement, with the lack of a federal law regulating personal data usage. As a result, the conflict between pragmatic and moral legitimacy is played out in protracted disputes between citizens (human rights advocates, NGOs) and the companies making facial recognition technologies. Both parties possess some 'micro powers'. The mosaic of clashes between such 'micro powers' in the United States

constitutes the ambivalence of power in the legitimation of facial recognition technology.

There is a kind of trade-off between pragmatic and moral legitimation, and one can be achieved at the expense of the other. Finally, this trade-off depends on the core values that define the criteria for pragmatic and moral legitimation. For example, human rights are among the criteria for moral legitimation in North America, in contrast to China. Hence, China will benefit from economic growth, although this is fraught with the risk of stoking social tensions if the values of Chinese society begin to change in the long run. In the other scenarios, if North America lags in terms of economic growth, it can accelerate new AI technologies without violating human rights, or perhaps they will be forced to downgrade human rights as a criterion of legitimacy. In Russia, for pragmatic legitimation, political gains for the authorities are a top priority, in contrast to economic gains and human rights in North America.

Conclusion

The legitimation of innovation has many dimensions. For example, it can include a legal component, the mobilization of existing laws (Black 1973), and in principle, the development of new legal norms can be initiated too. It can include certain actions by civil society, for example, criticism in the press or protests against a particular innovation, economic policy measures, including the direct stimulation by the state of some innovations, and so forth. However, it should be borne in mind that all these actions to one degree or another reflect the core values of society. So, a legal ban on the diffusion of a particular innovation on the grounds of human rights law reflects the value of human rights in society: if they are highly valued, the law is used; if not, then the corresponding legal norms either do not exist or are not applied. In other words, values act as a kind of ‘trigger’ that ‘turns on’ (or ‘does not turn on’) the action of various social institutions.

As a matter of fact, the legitimation of innovation works as a particular system of social immunity, which includes social filters that slow down the diffusion of innovation, adjust them or change them in line with societal values as well as, in certain cases, stopping their diffusion if society believes that they could cause significant social harm. At the same time, the structure of this social immune system can differ from society to society, depending on political, cultural and other institutions. The system of social immunity includes a set of criteria by which society is guided,

including values, when it ‘filters out’ some innovations and gives the green light to others. The ambivalence of power reduces the efficiency of social immunity and produces various negative social effects when powerful actors push through innovation with contested legitimacy. Although in principle it is known that the legitimation of innovation can have a positive economic effect, a deeper knowledge of these criteria and an understanding of how they ‘work’ will make it possible to better predict the successes and failures of the diffusion of various innovations in different socio-economic, political and cultural contexts.

Acknowledgements

The author appreciates the support from the Program for Basic Research of the National Research University Higher School of Economics (HSE University, Moscow).

Notes

- 1 I borrowed the term ‘embedded ambivalence’ from the paper written by Miller (2020), where ambivalence was analysed as an essential element of the problem under study.
- 2 The initial stage of the study was carried out with M. M. Yachnik and published in Kosals and Yachnik (2020a) and Kosals and Yachnik (2020b).
- 3 According to many scholars, although still debatable, the vision of Russia as a country ‘between East and West’ remains relevant in the Russian context and generates discussions to date: see, for example, Shlapentokh (2007), Ivanov (2008) and Korosteleva and Paikin (2021).
- 4 ‘Strictly speaking, the state is the very organ of social thought’ (Durkheim 1957, 51).
- 5 ‘What is needed if social order is to reign is that the mass of men be content with their lot. But what is needed for them to be content is not that they have more or less, but that they be convinced they have no right to more. And for this, it is absolutely essential that there be an authority whose superiority they acknowledge and which tells them what is right’ (Durkheim 1962, 242).
- 6 In the academic literature, there are a number of studies focused on the controversy between pragmatic and moral legitimacy, but not in the realm of innovation (Bowen 2019; Melé and Armengou 2016).
- 7 It is an independent agent of the Canadian Parliament (<https://www.priv.gc.ca/en/about-the-opc/>) that monitors compliance with the Privacy Act (1985, <https://laws-lois.justice.gc.ca/PDF/P-21.pdf>). The act regulates the rules for the collection and use of personal data in Canada.
- 8 See, for example, Citizen Lab (Munk School of Global Affairs and Public Policy, University of Toronto) report by Robertson et al. (2020) or Chiao (2019).
- 9 See, for example: Медуза. 6 ноября 2019 ‘Суд отказался запрещать систему распознавания лиц на улицах Москвы’ (Meduza, 6 November 2019 (интернет-издание, внесенное в список иностранных агентов в России), ‘The court refused to prohibit the facial recognition system on the streets of Moscow’). <https://meduza.io/news/2019/11/06/sud-otkazalsya-zapreshchat-sistemu-raspoznvaniya-lits-na-ulitsah-moskvy>.
- 10 See РБК. 22 июля 2020 ‘Власти Москвы назвали число штрафов за нарушение самоизоляции’ (RBC, 22 July 2020, ‘Moscow authorities called the number of fines for violation of self-isolation’). Accessed 26 January 2021. <https://www.rbc.ru/rbcfreeneews/5f18216a9a7947cc5b5f8423>.

- 11 See Открытые медиа. 21 июля 2020 'У системы слежки за москвичами погрешность — более 20%: штрафуют при неполном сходстве фото с оригиналом' (сайт издания заблокирован в России) (Open Media, 21 July 2020, 'The tracking system for Muscovites has an error of more than 20%: they fined if the photo is not entirely similar to the original'). Accessed 2 February 2021. <https://openmedia.io/news/n3/u-sistemy-slezhki-za-moskvichami-pogreshnost-bole-20-shtrafuyut-pri-nepolnom-sходстве-foto-s-originalom/>.
- 12 See, for example, Медиазона. 3 марта 2020 'Суд в Москве отклонил второй иск о запрете системы распознавания лиц' (интернет-издание, внесенное в список иностранных агентов в России) (Mediazona, 3 March 2020, 'Moscow court rejects second lawsuit to ban the facial recognition system'). Accessed 10 February 2021. <https://zona.media/news/2020/03/03/popova-isk>.
- 13 See Единая информационная система в сфере закупок. 7 декабря 2020 'Поставка программного обеспечения Видеодетектор для поиска силуэтов людей в кадре' (Unified information system in the field of procurement, 7 December 2020, 'Supply of Video Detector Software for Searching People Silhouettes in the Frame'). Accessed 15 February 2021. <https://zakupki.gov.ru/223/purchase/public/purchase/info/common-info.html?regNumber=32009771514>.
- 14 'Общественные ценности влияют на отношение к искусственному интеллекту и его юридическому оформлению' ('Social values influence attitudes towards artificial intelligence and its legal design') Симачев – Simachev 2019, 62.
- 15 See chapter 5, 'Selective law enforcement as a mechanism enforcing informal rules', in Bækken (2019, 107–26).

References

- Aronowitz, Stanley and William DiFazio. 2010. *The Jobless Future*. Minneapolis: University of Minnesota Press.
- Bækken, Håvard. 2019. *Law and Power in Russia: Making sense of quasi-legal practices*. London: Routledge.
- Benotsmame, Rabab, György Kovács and László Dudás. 2019. 'Economic, social impacts and operation of smart factories in Industry 4.0 focusing on simulation and artificial intelligence of collaborating robots', *Social Sciences* 8(5): 143. Accessed 5 January 2020. <https://doi.org/10.3390/socsci8050143>.
- Black, Donald J. 1973. 'The mobilization of law', *Journal of Legal Studies* 2: 125–49.
- Blanco, Belen, Encarna Guillamón-Saorín and Andrés Guiral. 2013. 'Do non-socially responsible companies achieve legitimacy through socially responsible actions? The mediating effect of innovation', *Journal of Business Ethics* 117: 67–83.
- Borisova, Tatiana and Jane Burbank. 2018. 'Russia's legal trajectories', *Kritika: Explorations in Russian and Eurasian History* 19: 469–508.
- Bowen, Frances. 2019. 'Marking their own homework: The pragmatic and moral legitimacy of industry self-regulation', *Journal of Business Ethics* 156: 257–72.
- Bunduchi, Raluca. 2016. 'Legitimacy-seeking mechanisms in product innovation: A qualitative study', *Journal of Product Innovation Management* 34: 315–42.
- Durkheim, Emile. 1957. *Professional Ethics and Civic Morals*. London: Free Press.
- Durkheim, Emile. 1962. *Socialism*. New York: Collier.
- Durkheim, Emile. 1998. *Contributions to l'Année Sociologique*. New York: Free Press.
- Etzioni, Amitai. 1968. *Active Society: A theory of societal and political processes*. New York: Free Press.
- Foucault, Michel. 1998. *The History of Sexuality: The will to knowledge*. London: Penguin.
- Frey, Carl Benedikt and Michael A. Osborne. 2013. 'The Future of Employment: How susceptible are jobs to computerisation?' Paper given at the *Machines and Employment* workshop, Oxford University, 17 September 2013. Accessed 3 February 2021. https://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf?link=mkw.
- Fu, Xiaoqing (Maggie), Qun Bao, Hongjun Xie and Xiaolan Fu. 2021. 'Diffusion of industrial robotics and inclusive growth: Labour market evidence from cross country data', *Journal of Business Research* 122: 670–84.

- Gane, Mike. 1984. 'Institutional socialism and the sociological critique of communism (introduction to Durkheim and Mauss)', *International Journal of Human Resource Management* 13: 304–30.
- Gerring, John. 2007. *Case Study Research: Principles and practices*. New York: Cambridge University Press.
- Giannini, Tyler R. 2018. 'Political legitimacy and private governance of human rights: Community–business social contracts and constitutional moments'. In *Human Rights, Democracy, and Legitimacy in a World of Disorder*, edited by Gerald L. Neuman and Silja Vooney, 209–33. Cambridge: Cambridge University Press.
- Gould, Jon B. and Scott Barclay. 2012. 'Mind the gap: The place of gap studies in sociolegal scholarship', *Annual Review of Law and Social Science* 8: 323–35.
- Greitens, Sheena Chestnut. 2020. *Dealing with Demand for China's Global Surveillance Exports*. Washington, DC: Brookings Institution. Accessed 10 February 2021. <https://www.brookings.edu/research/dealing-with-demand-for-chinas-global-surveillance-exports/>.
- Hajda, Jan. 1968. 'Ambivalence and social relations', *Sociological Focus* 2: 21–8.
- Hendley, Kathryn. 2011. 'Varieties of legal dualism: Making sense of the role of law in contemporary Russia', *Wisconsin International Law Journal* 29: 233–62.
- Hill, Kashmir. 2020. 'The secretive company that might end privacy as we know it', *New York Times*, 18 January. Accessed 20 January 2021. <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.
- Horowitz, Irving L. 1982. 'Socialization without politicization: Emile Durkheim's theory of the modern state', *Political Theory* 10: 353–77.
- Ivanov, Vyacheslav V. 2008. 'Russia between East and West? Remarks on comparison of cultures', *Russian Journal of Communication* 1: 113–26.
- Johnson, Cathryn, Timothy J. Dowd and Cecilia Ridgeway. 2006. 'Legitimacy as a social process', *Annual Review of Sociology* 32: 53–78.
- Kawakami, Takashi and Yusuke Hinata. 2019. 'Pay with your face: 100m Chinese switch from smartphones: Facial recognition technology spreads rapidly at the expense of privacy', *Nikkei Asian Review*, 16 October. Accessed 2 February 2021. <https://asia.nikkei.com/Business/China-tech/Pay-with-your-face-100m-Chinese-switch-from-smartphones>.
- Kollektiv avtorov (team of authors) (ruk. (headed by) Yuriy. V. Simachev). 2019. *Razvitie regulirovaniya: novye vyzovy v usloviyah radikal'nyh tekhnologicheskikh izmenenij*. Doklad. Moskva. [Regulation of the development: new challenges in the face of radical technological change]. Moscow: HSE University Press, 2019.
- Korosteleva, Elena and Zachary Paikin. 2021. 'Russia between East and West, and the future of Eurasian order', *International Politics* 58: 321–33.
- Kosals, Leonid and Maria Yachnik. 2020a. 'Rynek tekhnologij iskusstvennogo intellekta v Rossii: social'nye usloviya zarozhdeniya Stat'ya 1. Podhody k issledovaniyu i vydelenie granic rynka' [The market for technologies of artificial intelligence in Russia: social conditions of emergence. Article 1. The methodology of research and identifying the market agents], *Obshchestvennye nauki i sovremennost'* 2: 5–24.
- Kosals, Leonid and Maria Yachnik. 2020b. 'Rynek tekhnologij iskusstvennogo intellekta v Rossii: social'nye usloviya zarozhdeniya. Stat'ya 2. Razrabotchiki, potrebiteli i gosudarstvo: vzaimootnosheniya i perspektivy' [The market of artificial intelligence technologies in Russia: social conditions of origin. Article 2. Developers, consumers and the state: relationships and prospects], *Obshchestvennye nauki i sovremennost'* 3: 5–17.
- Kovachich, Leonid. 2020. 'Sdelano ne v Kitae: kak ustroena sistema videonablyudeniya Moskvyy' [Made not in China: how the video surveillance system of Moscow works], Moscow: Moskovskij Centr Karnegi. Accessed 5 February 2021. <https://carnegie.ru/2020/08/05/ru-pub-82419>
- Kumar, Rajesh and T. K. Das. 2007. 'Interpartner legitimacy in the alliance development process', *Journal of Management Studies* 44: 1425–53.
- Kurkchian, M. 2018. 'The distinctive features of Russian legal culture'. In *Constructing Legal Culture through Institutional Reforms: The Russian experience*. Report and Analysis of a Workshop Held at Wolfson College, Oxford, edited by M. Kurkchian. Oxford: Foundation for Law, Justice and Society.
- Leibold, James. 2020. 'Surveillance in China's Xinjiang region: Ethnic sorting, coercion, and inducement', *Journal of Contemporary China* 29: 46–60.

- Markarda, Jochen, Steffen Wirth and Bernhard Truffer. 2016. 'Institutional dynamics and technology legitimacy: A framework and a case study on biogas technology', *Research Policy* 45: 330–44.
- McWilliams, Wilson Carey (ed.). 2006. *The Active Society Revisited*. Lanham, MD: Rowman & Littlefield.
- Melé, Domènec and Jaume Armengou. 2016. 'Moral legitimacy in controversial projects and its relationship with social license to operate: A case study', *Journal of Business Ethics* 136: 729–74.
- Miller, Zinaida. 2020. 'Embedded ambivalence: Ungoverning global justice', *Transnational Legal Theory* 11: 353–81.
- Mokyr, Joel, Chris Vickers and Nicolas L. Ziebarth. 2015. 'The history of technological anxiety and the future of economic growth: Is this time different?', *Journal of Economic Perspectives* 29: 31–50.
- Mousterman, Pieter and Justyna Zander. 2016. 'Industry 4.0 as a cyber-physical system study', *Software and Systems Modeling* 15: 17–29.
- Neuman, Gerald L. 2018. 'Human rights, treaties, and international legitimacy'. In *Human Rights, Democracy, and Legitimacy in a World of Disorder*, edited by Gerald L. Neuman and Silja Voenekey, 51–72. Cambridge: Cambridge University Press.
- Office of the Privacy Commissioner of Canada. 2020. 'Joint Investigation of the Cadillac Fairview Corporation Limited', 28 October. Accessed 10 January 2021. <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/>.
- Office of the Privacy Commissioner of Canada. 2021. 'Joint Investigation of Clearview AI, Inc.', 2 February. Accessed 5 February 2021. <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/>.
- Paneyakh, Ella L. 2014. 'Faking performance together: Systems of performance evaluation in Russian enforcement agencies and production of bias and privilege', *Post-Soviet Affairs* 30: 115–36.
- Petkova, Iva. 2018. 'Digital Moda: Institutionalizing legitimacy in the fashion industry'. In *Engineering Legitimacy: How institutional entrepreneurs in e-commerce bring fashion companies into the digital age*, by Iva Petkova, 103–36. Cham: Palgrave Macmillan.
- Rao, Anand S. and Gerard Verweij. 2017. 'Sizing the prize: What's the real value of AI for your business and how can you capitalise?' PWC. Accessed 9 February 2021. <https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf>.
- Robertson, Kate, Cynthia Khoo and Yolanda Song. 2020. *To Surveil and Predict: A human rights analysis of algorithmic policing in Canada*. University of Toronto. Accessed 5 February 2021. <https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf>.
- Schoon, Eric W. and Courtney DeRoche. 2019. 'Legitimacy building in policy and practice: The case of US private military and security contractors (PMSCs) in Afghanistan'. In *The Sociology of Privatized Security*, edited by Ori Swed and Thomas Crosbie, 67–83. Cham: Palgrave Macmillan.
- Schumpeter, Joseph A. 2010. *Capitalism, Socialism and Democracy*. London: Routledge.
- Shlapentokh, Dmitry. 2007. *Russia between East and West: Scholarly debates on Eurasianism*. Leiden: Brill.
- Shrouf, Fadi, Joaquín Ordieres and Giovanni Miragliotta. 2014. 'Smart factories in Industry 4.0: A review of the concept and of energy management approached in production based on the internet of things paradigm', *2014 IEEE International Conference on Industrial Engineering and Engineering Management*, IEEE. Accessed 10 January 2021. <https://ieeexplore.ieee.org/abstract/document/7058728>.
- Skilton, Mark and Felix Hovsepian. 2018. *The 4th Industrial Revolution: Responding to the impact of artificial intelligence on business*. Basingstoke: Palgrave Macmillan.
- Wang, Shiyong, Jiafu Wan, Di Li and Chunhua Zhang. 2016. 'Implementing smart factory of Industry 4.0: An outlook', *International Journal of Distributed Sensor Networks* 12. Accessed 20 January 2020. <http://dx.doi.org/10.1155/2016/3159805>.
- Wang, Tao, Ting Zhang and Zhigang Shou. 2019. 'The double-edged sword effect of political ties on performance in emerging markets: The mediation of innovation capability and legitimacy', *Asia Pacific Journal of Management* 38: 1003–30. Accessed 4 February 2021. <https://doi.org/10.1007/s10490-019-09686-w>.
- Weber, Max. 1964. *The Theory of Social and Economic Organization*. New York: Free Press.