ppi 201502ZU4645
Esta publicación científica en formato digital es continuidad de la revista impresa
ISSN-Versión Impresa 0798-1406 / ISSN-Versión on line 2542-3185Depósito legal pp
197402ZU34

CUESTIONES POLÍTICAS

Instituto de Estudios Políticos y Derecho Público "Dr. Humberto J. La Roche"
de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia
Maracaibo, Venezuela

Vol.39 Nº 71
2021

Cuestiones Políticas Vol. 39, Nº 71 (2021), 609-620
IEPDP-Facultad de Ciencias Jurídicas y Políticas - LUZ

Human rights during the mass introduction of artificial intelligence and robotic systems into public life

DOI: https://doi.org/10.46398/cuestpol.3971.36

Dmitry Kuteynikov *
Osman Izhaev **
Valerian Lebedev ***
Sergey Zenin ****

Abstract

Purpose: This article considers legal approaches to implementing human rights during the mass exploitation of artificial intelligence and robotic systems in public life. Methods: Within the framework of this study, an emphasis is placed on the legal regulation of artificial intelligence systems and robotics used for remote biometric identification of a person and the creation of social credit systems. This study analyzes different models of legal regulation that are typical of certain countries and regions, including the UK, USA, China, and the EU. Results: In the UK, it is allowed to use real-time face recognition systems in public spaces but the set of scenarios and situations for their use is significantly limited by legislation and law enforcement. The legal regulation of these systems in each state is based on a constant dialogue between state and civil society. The use of artificial intelligence and robotic systems to create social credit systems is tested in some countries. Modern states have formed several approaches to the creation of such systems: some of them completely prohibit these systems, while others develop a technological and regulatory framework for the creation of national systems.

Keywords: human rights; robotics; social rating; state; civil society.

* Kutafin Moscow State Law University, Moscow, Russia. ORCID ID: https://orcid.org/0000-0003-1448-3085

** Kutafin Moscow State Law University, Moscow, Russia. ORCID ID: https://orcid.org/0000-0003-3777-8927

*** Kutafin Moscow State Law University, Moscow, Russia. ORCID ID: https://orcid.org/0000-0002-7642-1325

**** Tyumen State University, Tyumen, Russia; Kutafin Moscow State Law University, Moscow, Russia. ORCID ID: https://orcid.org/0000-0002-4520-757X

Recibido el 14/09/2021 Aceptado el 03/11/2021

Los derechos humanos durante la introducción masiva de la inteligencia artificial y los sistemas robóticos en la vida pública

Resumen

El objetivo del artículo fue considerar enfoques legales para implementar los derechos humanos durante la explotación masiva de inteligencia artificial y los sistemas robóticos en la vida pública. Se trata de una investigación documental que hace énfasis en la regulación legal de los sistemas de inteligencia artificial y robótica utilizados para la identificación biométrica remota de una persona y la creación de sistemas de crédito social. Además, este estudio analiza diferentes modelos de regulación legal que son típicos de ciertos países y regiones, incluidos el Reino Unido, EE. UU., China y la UE. Resultados. Como conclusión se muestra que, en el Reino Unido, se permite el uso de sistemas de reconocimiento, pero el conjunto de escenarios y situaciones para su uso está significativamente limitado por la legislación y la aplicación de la ley. La regulación legal de estos sistemas en un estado determinado se basa en un diálogo constante entre el estado y la sociedad civil. El uso de inteligencia artificial y sistemas robóticos para crear sistemas de crédito social se prueba en algunos países. Los estados modernos han formado varios enfoques para la creación de tales sistemas: algunos de ellos prohíben completamente estos sistemas, mientras que otros no.

Palabras clave: derechos humanos; robótica; calificación social; estado; sociedad civil.

Introduction

It would not be an exaggeration to say that the digital environment has become an independent sphere of society. The social relations arising in this regard are relatively new and do not always have established approaches to their regulation in legal science. On the contrary, the regulatory policy of many states is still searching for the most adequate and effective legal approaches (Gurinovich *et al*., 2020; Gurinovich and Smirnikova, 2021).

At first glance, such traditional constitutional rights as the inviolability of private life, the freedom of speech and expression, the right to information and some other rights fully embrace the emerging relations in the field of information technology. However, the legal means of ensuring and protecting such rights should also consider the specifics of these relations (Livingston and Risse, 2019).

At the level of states and private companies, technical means are developed and introduced into public life, based on the use of complex algorithms which are abstractly defined in the regulatory legal acts of different countries by the term "artificial intelligence".

Public administration in various areas, including law enforcement, uses technologies for collecting personal data of citizens (for example, digital pass systems to control the movement of a person, including in transport, as well as to differentiate citizens by the scope of their rights; video surveillance systems with face recognition technology, etc.). Many countries develop comprehensive government systems to control public life. Under such circumstances, an unprecedented amount of data is generated and is increasing exponentially, along with the potential risks of violating human rights.

1. Methods

We set the objective of analyzing the world's legal approaches to protecting human rights during the mass introduction of artificial intelligence and robotic systems into public life. This article studies approaches to the legal regulation of artificial intelligence and robotic systems for the remote biometric identification of a person and the creation of social credit systems.

The first task was to study the legal regulation of artificial intelligence and robotic systems for the remote biometric identification of a person in the UK, USA, EU, and China. The analysis of their legislation is conditioned by different ways to the regulation of the issue under consideration. The study of these approaches will reveal the best options for legal regulation.

The second task was to analyze the use of artificial intelligence and robotic systems to create social credit systems. The study identifies several approaches to the legal regulation of this issue that are typical of certain countries and regions. It also analyzes the impact of these systems on fundamental human rights.

2. Results

In recent years, the UK has developed legal regulation and law enforcement practice on the use of artificial intelligence and robotic systems in public life. Security authorities allow the use of real-time face recognition systems in public spaces, but scenarios and situations of their use are significantly limited by legislation and law enforcement practice. The legal regulation of these systems in each state is based on a constant dialogue between state and civil society.

The United States still has no federal laws on the use of artificial intelligence for biometric identification. State and local legislation go differently. In several states and cities, the use of the corresponding technologies is prohibited completely or significantly limited.

The EU has developed a draft Regulation of the European Parliament and the Council laying down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act). This draft is supposed to impose a ban on the use of artificial intelligence for the remote biometric identification of people in public spaces in real-time to protect law and order, except for three listed and defined situations when such use is necessary to achieve a significant public interest, whose importance outweighs the risks.

In China, there is no special regulation of this sphere. The use of these systems is described in civil legislation, as well as in legal acts on cyber security and data circulation. The development of these systems is controlled by the Chinese government. Due to the high centralization of power, there is a risk of violating human rights and ending up with the total surveillance of citizens without any legislatively established framework and restrictions.

The use of artificial intelligence and robotic systems to create social credit systems is not widespread in most countries. However, their legislations utilize several approaches: a complete ban on the creation of these systems or the formation of a regulatory framework for the deployment of nationwide systems. At the same time, the functioning of these systems will not correspond to universally recognized human rights and civil freedoms. Thus, it is necessary to prevent the creation and application of social scoring both at the national level and at the level of individual territories or spheres of public life.

3. Discussion: the use of artificial intelligence and robotic systems for the remote biometric identification of a person

One of the most sensitive spheres of public life, influenced by the implementation of the aforementioned technologies, has become relations associated with the establishment of legal guarantees for the protection of human rights to privacy in connection with the use of artificial intelligence systems for remote biometric identification. These systems are usually used by government agencies to ensure national security (the search and capture of offenders, the predictive analytics of crime) but there are other ways to use them in the public sector, for example, payments for public transport, public services, etc. These systems are being used in the private sector, especially in banking, retail, communications, and security.

In the UK, public and human rights organizations are against the use of real-time facial recognition by the police in public places after several citizens were apprehended for no reason (Woollacott, 2021).

From the legal perspective, the use of face recognition systems by the police did not have any regulation until recently. In 2019, human rights organization Liberty filed a lawsuit against the South Wales Police alleging that the police's use of facial recognition in public places violated the fundamentals of human rights, such as the Human Rights Act, the Data Protection Act and Equality Act (Gordon, 2021). The court ruled that, on the one hand, there was a sufficient legal basis to ensure the proper use of real-time face recognition systems and, on the other hand, that the police used these systems in full compliance with the existing law (Centre for Data Ethics and Innovation, 2020).

In 2020, Liberty appealed against this decision (R. (Bridges) v. Chief Constable of South Wales Police. The court ruled that the use of real-time face recognition systems by the police in some cases did not comply with law. The court reached the following conclusions (Biometrics and Forensics Ethics Group, 2021):

- The use of facial recognition systems violated the right to privacy protected by the Human Rights Act. The court found critical flaws in the legal framework that left too much regulatory leeway for employees.
- The use of face recognition systems violated certain provisions of the Data Protection Act. While considering the impact on data protection, it was impossible to properly assess the risks of violating the rights and freedoms of data subjects, and no measures were taken to eliminate these risks. Two groups of powers were also identified, within which state bodies have unacceptably wide opportunities for discretion: firstly, how persons are selected for observation lists; secondly, on what basis technical complexes equipped with face recognition systems are in a particular public space.
- The South Wales Police violated their responsibilities under certain provisions of the Equality Act because the police did not attempt to verify, either independently or through an outside review, that the software was free of potential race- or gender-based bias (The Court of Appeal of England and Wales, 2020).

Based on this judgment, amendments were made to the Surveillance Camera Code of Practice. Accordingly, system operators should plan their work based on 12 guiding principles, including limiting an exhaustive list of areas and scenarios for their use, transparency, the priority of human rights, and non-discrimination (Surveillance Camera Code of Practice, 2013).

In the UK, it is allowed to use real-time face recognition systems in public spaces but the set of scenarios and situations for their use is significantly limited by legislation and law enforcement. The legal regulation of these systems in a given state is based on a constant dialogue between state and civil society.

In the United States, there are no federal laws on artificial intelligence systems for biometric identification. The development of one or several system-forming acts has been discussed by legislators but there are only some legislative initiatives that are at different stages of consideration. This is due to the general legal regulation of artificial intelligence systems and the circulation of personal data, which are carried out ad hoc. In 2020, the Decree of the President of the United States was adopted, and appropriate recommendations were developed for executive authorities.

Such tech companies as Amazon and Microsoft imposed a moratorium on this set of technologies until legislators form a sufficient regulatory framework or roadmap. In contrast, IBM announced that it would cease its participation in the related business projects (Feiner and Palmer, 2021).

State and local legislation go differently. In several states and cities, the use of the corresponding technologies is prohibited completely or significantly limited (Sakin, 2021). The use of these systems has attracted great public attention after the Black Lives Matter protests and arrests after the "2021 Capitol attack".

The EU has developed a draft Regulation of the European Parliament and the Council laying down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act). This draft is supposed to impose a ban on the use of artificial intelligence for the remote biometric identification of people in public spaces in real-time to protect law and order, except for three listed and defined situations when such use is necessary to achieve a significant public interest, whose importance outweighs the risks.

These situations include: firstly, the search for potential victims of crime, including missing children; secondly, a threat to human life or safety, in particular in case of terrorist attacks; thirdly, the detection, localization, identification and prosecution of persons who committed or are suspected of committing crimes according to constituent elements (32 elements of criminal offenses with imprisonment of at least three years) (Proposal for a regulation of the European Parliament and of the Council, 2016).

A similar position was expressed by the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) regarding the previously published European Commission Artificial Intelligence Regulation draft. The document states that given the extremely high risks associated with remote biometric identification in public places, the EDPB and EDPS call for a general ban on any use of artificial intelligence to

automatically recognize human features in public places such as the face, gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioral signals in any context (European Data Protection Board, 2021).

The EU is currently forming a stable and multidimensional system for the legal regulation of artificial intelligence and robotic systems for remote biometric identification in public places in real-time. However, the regulation of such public relations in the EU is "human-oriented", which protects and guarantees human rights and civil freedoms. This emphasizes the legal support of regulation in the field of technological development. At the same time, it slows down business processes and the application of specific products in public life. The EU is an important market for almost all big tech companies, so as with the GDPR. If adopted, this can become one of the key approaches since new technology products will be designed with these constraints in mind.

The most widespread use of artificial intelligence and robotic systems for remote biometric identification is typical of China. The regulation of these systems is reflected in civil law, as well as in regulatory legal acts on cyber security and data circulation. Currently, this sphere of public relations does not have special regulations. China has done quite a lot of work in the field of data protection. In 2016, the Cybersecurity Law of the People's Republic of China was adopted which established regulatory requirements like those of the EU and the US. Since China is a state with an authoritarian political system, data confidentiality is more connected with the decisions of public authorities rather than with the creation of a unified legal framework supported by independent judicial decisions.

This issue is common to other spheres of social and economic activity, where the freedom of private and public organizations is rather limited by the state's interests. By adopting legal acts, the state provides a lot of opportunities for unlimited participation in the activities of private companies and actively introduces innovations to create a unified system for controlling all the spheres of public life.

In July 2017, the State Council of the People's Republic of China announced a strategy for the development of artificial intelligence called the "Next Generation Artificial Intelligence Development Plan". According to this strategy, China aims at becoming a global leader in artificial intelligence by 2030, as well as to take a leading position in the development of regulatory acts, ethics, and standards for artificial intelligence. The concept represents only a general model and objectives of future legal regulation. Consequently, it should be considered in conjunction with other regulatory legal acts. Although this concept was developed by the state, the actual implementation of these innovations and transformations will be carried out by the private sector and local authorities (Roberts *et al.*, 2021).

The Chinese regulation is also characterized by rather quick adaptation to the use of new technologies in the market. Unlike the above-mentioned countries, China uses unmanned vehicles on public roads in marked areas (Ziyan and Shiguo, 2021) and created the first automated e-courts and a unified social credit system.

An important feature of China is a rather high level of citizens' approval of video surveillance systems if compared to the other countries. According to the study conducted by European scientists, the Chinese demonstrate much support for the use of face recognition technologies (67%), as well as the lowest dissatisfaction with their deployment (9%) (Kostka *et al.*, 2021).

On the one hand, China has adopted ambitious concepts in relation to the functioning of artificial intelligence and robotic systems and introduces innovations into public life much more actively than the EU and the USA due to centralized regulation. On the other hand, the development of these systems in China is controlled by the state, which, due to the high centralization of power, leads to the risk of human rights violations and the creation of total surveillance of citizens without any legislatively established framework and restrictions.

It can be argued that the use of artificial intelligence systems for remote biometric identification in public places can affect the privacy of a large part of the population, create a sense of constant surveillance and indirectly interfere with the freedom of assembly and other fundamental rights. In addition, the proper functioning of these systems and the impossibility of correcting errors when using these systems in real-time raises concerns.

It should also be noted that:

> Automatic face recognition not only tracks behavior but can also change it. When suspects know that they are being watched, for example, during a peaceful protest, their behavior might differ from what it would have been if they had not been watched (Gordon, 2021: 2).

Thus, the legislation of most democratic countries develops a system of legal regulation based on a balanced approach between the protection of human rights and the interests of national security. Legislators need to regulate the procedures and specific cases of using artificial intelligence for the remote identification of a person, as well as consider the possibility of limiting human rights.

4. The use of artificial intelligence and robotic systems to create social credit systems

Artificial intelligence for remote biometric identification together with systems for processing big data can be used to create social credit systems.

These trends cannot be called universal, but China is systematically moving towards the creation of a unified system for monitoring public life, i.e., it has begun testing these technological solutions in separate territories (Haciyakupoglu, 2021).

The assessment and classification of the individual's trustworthiness based on social behavior, known, or predicted personality traits can lead to the discrimination of certain social groups and their exclusion from public life.

Certain countries, including the EU, plan to introduce a complete ban on the creation of such systems. The draft Regulation of the European Parliament and the Council laying down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) established that such systems should be prohibited by law since the assessment and classification of the individual's trustworthiness based on social behavior, known or predicted personality traits can lead to the discrimination of certain social groups and their exclusion from public life (Proposal for a regulation of the European Parliament and of the Council, 2016).

A similar position was expressed by the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) regarding the previously published European Commission Artificial Intelligence Regulation draft. The document states that the EDPB and EDPS recommend a ban on the use of biometric data by artificial intelligence and robotic systems to divide people into social groups based on their ethnicity, gender, political or sexual orientation or other grounds on which discrimination is prohibited by Article 21 of the EU Charter on fundamental rights. In addition, the EDPB and EDPS believe that the use of artificial intelligence and robotic systems to detect human emotions is highly discouraged and should be prohibited, except for some cases (such as for some medical purposes where the recognition of patient's emotions is essential). The use of artificial intelligence and robotic systems for any type of social scoring should be prohibited (European Data Protection Board, 2021).

Conclusion

Thus, modern states have formed several approaches to the creation of social credit systems: some of them completely prohibit these systems, while others develop a technological and regulatory framework for the creation of national systems. It seems that the use of such systems will comply with the legislation of most democracies and fundamental international acts. From the legal viewpoint, it is necessary to prevent the creation and application of social ratings both at the national level and at the level of certain territories or spheres of public life.

The state should regulate public relations in the digital sphere, especially to protect human rights and civil freedoms, but there is a risk of excessive regulation. The latter can decrease the benefits of using technological solutions and slow down the development of the digital economy.

Acknowledgments

The study was funded by the Russian Foundation for Basic Research according to research project No. 18-29-16193.

Bibliographic References

BIOMETRICS AND FORENSICS ETHICS GROUP. 2021. Briefing note on the ethical issues arising from public–private collaboration in the use of live facial recognition technology (accessible). GOV.UK. Available online. In: https://www.gov.uk/government/publications/public-private-use-of-live-facial-recognition-technology-ethical-issues/briefing-note-on-the-ethical-issues-arising-from-public-private-collaboration-in-the-use-of-live-facial-recognition-technology-accessible. Consultation date: 05/05/2021.

CENTRE FOR DATA ETHICS AND INNOVATION. 2020. Independent report Snapshot Paper – Facial Recognition Technology. GOV.UK. Available online. In: https://www.gov.uk/government/publications/cdei-publishes-briefing-paper-on-facial-recognition-technology/snapshot-paper-facial-recognition-technology. Consultation date: 05/05/2021.

EUROPEAN DATA PROTECTION BOARD. 2021. EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination. edpb.europa.eu. Available online. In: https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en. Consultation date: 28/08/2021.

FEINER, Lauren; PALMER, Annie. 2021. Rules around facial recognition and policing remain blurry. CNBC. Available online. In: https://www.cnbc.com/2021/06/12/a-year-later-tech-companies-calls-to-regulate-facial-recognition-met-with-little-progress.html. Consultation date: 28/08/2021.

GORDON, Barrie. 2021. "Automated facial recognition in law enforcement: the Queen (on application of Edward Bridges) v the chief constable of South

Wales Police" In: Potchefstroom Electronic Law Journal. Vol. 24, pp. 1-29.

GURINOVICH, Aleksander; LAPINA, M.A; IVANOV, A.E. 2020. "Ways of restricting the rights of taxpayers under agreements for the avoidance of double taxation in national legislation" In: SAGE Open. Vol. 10, No. 4, pp. 1-8.

GURINOVICH, Aleksander; SMIRNIKOVA, J.L. 2021. "Debt policy of the Russian regions: economic and legal research" In: Indian Journal of Finance. Vol. 15, No. 1, pp. 23-35.

HACIYAKUPOGLU, Gulizar. 2021. China's social credit system: questions on the current status, role of data and surveillance, and influence outside of China. NATO Strategic Communications Centre of Excellence. Riga, Latvia. Available online. In: https://stratcomcoe.org/publications/chinas-social-credit-system-current-status-role-of-data-and-surveillance-and-influence-outside-of-china/209. Consultation date: 28/08/2021.

KOSTKA, Genia; STEINACKER, Lea; MECKEL, Miriam. 2021. "Between security and convenience: facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States" In: Public Understanding of Science. Vol. 30, No. 6, pp. 671-690.

LIVINGSTON, Steven; RISSE, Mathias. 2019. "The future impact of artificial intelligence on humans and human rights" In: Ethics & International Affairs. Vol. 2, pp. 141-158.

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS. 2016. EUR-Lex. Available online. In: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52021PC0206. Consultation date: 05/05/2021.

ROBERTS, Huw; COWLS, Josh; MORLEY, Jessica; TADDEO, Mariarosaria; WANG, Vincent; FLORIDI, Luciano 2021. "The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation" In: AI & Society. Vol. 36, pp. 59-77.

SAKIN, Nicole. 2021. Will there be federal facial recognition regulation in the US? iapp.org. Available online. In: https://iapp.org/news/a/u-s-facial-recognition-roundup/. Consultation date: 05/05/2021.

SURVEILLANCE CAMERA CODE OF PRACTICE. 2013. GOV.UK. Available online. In: https://assets.publishing.service.gov.uk/government/

uploads/system/uploads/attachment_data/file/1010815/Surveillance_Camera_Code_of_Practice__update_.pdf. Consultation date: 05/05/2021.

THE COURT OF APPEAL OF ENGLAND AND WALES. 2020. The Queen (on the application of Edward Bridges) (Appellant) v The Chief Constable of South Wales Police (Respondent) & others [2020] EWCA Civ 1058. Available online. In: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf. Consultation date: 05/05/2021.

WOOLLACOTT, Emma. 2021. UK Government accused of sneaking through new live facial recognition rules. Forbes.com. Available online. In: https://www.forbes.com/sites/emmawoollacott/2021/08/23/uk-government-accused-of-sneaking-through-new-live-facial-recognition-rules/?sh=e47cf88706f3. Consultation date: 28/08/2021.

ZIYAN, Chen; SHIGUO, Liu. 2021. "China's self-driving car legislation study" In: Computer Law and Security Review. Vol. 41, Article 105555.

UNIVERSIDAD
DEL ZULIA

CUESTIONES POLÍTICAS

Vol.39 Nº 71

Esta revista fue editada en formato digital y publicada en diciembre de 2021, por el ***Fondo Editorial Serbiluz, Universidad del Zulia. Maracaibo-Venezuela***

www.luz.edu.ve
www.serbi.luz.edu.ve
www.produccioncientificaluz.org