Artificial Intelligence Legal Policy: Limits of Use of Some Kinds of AI

Dremluiga Roman
Far Eastern Federal University
Russia
dremluiga.ri@dvfu.ru

Prisekina Natalia
Far Eastern Federal University
Russia
nprisekina@gmail.com

ABSTRACT

The paper is devoted to analysis of legal issues concerned to development of AI technologies. The main question here: should governments develop rules regulating use of artificial intelligence and a system of licensing like with automobile transport or ban some types of AI? Comprehension of the current and future legal framework is very important. First of all, law is used to govern a society. It implies that examining AI from legal point of view allows to realize what challenges to social security are caused by expansive introduction of autonomous systems. Secondly, for developer of high technology products it is easier to decide what products should not be invested to since they may lead to negative legal consequences.

CCS Concepts

• Social and professional topics—Technology and censorship •
Social and professional topics—Governmental surveillance •
Social and professional topics—Governmental regulations •
Social and professional topics—Import / export controls

Keywords

Artificial intelligence, legal regulation, dangerous AI

1. INTRODUCTION

Day by day AI systems become more sophisticated and often used in critical areas as public transportation, medicine, military needs and even public security. It is already hard to ignore the profound disruptions AI is causing in so many societal spheres. These disruptive changes raise important ethical, legal, social and technical questions on how society may ensure that AI's deployment is beneficial and not harmful to people. There is no doubt that when thinking systems become widespread, our societies will inevitably face the issue of limiting permission for use and possession of some types of artificial intelligence systems.

There is analogy with weapon or explosive materials which not every person has a permission to use in the paper. In many countries an owner or a user must have a license to own or use a weapon or an explosive. Similarly, incapacitated persons are not permitted to use weapons according to law. For some types of AI system it would be reasonable

Some software companies faced the fact that legal and ethical discrepancy of AI systems leads to serious losses. The issue of

moral and legal compliance of new technology becomes a corner stone for making a decision. For instance, Amazon company shut down the project of AI recruiting technology because intellectual system developed a bias against women¹.

Is it possible that some types of Artificial intelligence or its application become so dangerous for society that it would be reasonable to prohibit owning or using them in general? There could be analogy drawn with guns or explosive materials which not every person has permission to use in accordance with law. In most countries you must have a license to possess a weapon or explosive and have special properties (age, mental capacity etc.). Therefore, children or incapacitated persons are not permitted to use a weapon by law. For some kind of AI system it would be reasonable. From this perspective, governments should develop rules regulating use of artificial intelligence and a system of licensing like with automobile transport. In case of serious negative consequences of not following the rules it will probably imply criminal liability (as in the sphere of transport, for example, when a drunk driver kills a pedestrian).

2. REVIEW OF EXISTING LAW

Nowadays we have a lot of things that are prohibited by law in general or criminal law in particular to use, distribute and possess in modern societies. In the majority of countries, among such things are counterfeited drugs, weapon, explosives, narcotics, biohazard materials etc. In practice limitations depend on jurisdiction and type of proscribed items or substances. For instance, in the United States law proclaims that “*whoever knowingly possesses or causes to be present a firearm or other dangerous weapon in a Federal facility (other than a Federal court facility), or attempts to do so, shall be fined under this title or imprisoned not more than 1 year, or both*” (U.S. Code, Title 18, Part I, Chapter 44, § 930 «Possession of firearms and dangerous weapons in Federal facilities»). A vendor of weapon has to have a license (U.S. Code, Title 18, Part I, Chapter 44, § 923 «Licensing») and forbear from selling, delivering, or otherwise transferring weapon to juvenile or minor (U.S. Code, Title 18, Part I, Chapter 44, § 922 «Unlawful acts»; US v Rene, 583 F.3d 8 (1st Cir. 2009)). Despite the fact that in the United States the right to bear and keep arms is protected by the Constitution², this right has serious limitations. For instance, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)³³ is

¹<https://www.theguardian.com/technology/2018/oct/11/tech-gender-problem-amazon-facebook-bias-women>

² U.S. Constitution, Second Amendment

³ Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), <https://www.atf.gov/>

⁴ See for instance: <https://www.cecc.gov/resources/legal-provisions/criminal-law-of-the-peoples-republic-of-china>

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

ICSCA '19, February 19–21, 2019, Penang, Malaysia

© 2019 Association for Computing Machinery.

ACM ISBN 978-1-4503-6573-4/19/02...\$15.00

<https://doi.org/10.1145/3316615.3316627>

created to do the regulatory enforcement and criminal investigation of gun trafficking cases.

Unlike the United States of America, most countries have stricter rules. For instance, Chinese Criminal Code states that “*whoever illegally manufactures, trades in, transports, mails or stores any guns, ammunition or explosives shall be sentenced to fixed-term imprisonment of not less than three years but not more than 10 years*”⁴. The similar approach is in Russian criminal law. Article 226 of the Criminal Code of the Russian Federation prescribes that “*stealing or possession of firearms, their components, ammunition, explosives, or explosive devices shall be punishable by deprivation of liberty for a term of three to seven years*” (Article 226, The Criminal Code of The Russian Federation No. 63-FZ Of June 13, 1996).

In case of other “dangerous things” the situation is similar to firearm regulation and control. Countries usually establish criminal liability of persons involved in the sale of unlawful drugs and a lot of them - for possession of unlawful drugs [2,3,4,13]. Standpoint of states to the illegal spread of explosives is quite negative. Such activity also implies criminal liability [14]⁵.

Among the grounds to introduce special legal rules for the so-called “dangerous things” is that governments mostly do not want criminals, infants, insane persons, non-qualified persons to possess, use, and distribute these “dangerous things” as they are able to create serious threat to public order, state and society. Although possession or distribution of the so-called “dangerous things” means only speculative not real negative consequences, it is widely accepted practice to assess such actions as a criminal act. Summarizing the practice of various states any kind of “dangerous things” has a special body to control its distribution, use, possession and production. Frequently a special legislation is enacted to establish rules of operations with proscribed items and substances.

3. APPLICATION OF TRADITIONAL LAW TO AI

With regard to Artificial intelligence there is an equivalent question: could it be enough dangerous that the state has to delineate special regulation to possess, use and distribute such type of AI. Partially, the answer is simple. When Artificial intelligence technology is combined with proscribed dangerous item or substances in a single device, primarily, existing legislation could be applied. We already have some rules on regulation of technology use, and spheres with dangerous things are well regulated.

Devices which AI technology and proscribed items or substances are parts have to satisfy both systems of rules. For example, if a person installs into its drone controlled by AI a machine gun, his/her actions with an autonomous vehicle would be covered both by the law of firearm control and by the drone flight regulation law.

If a device with AI is totally new, the use of technology is not covered by law with high probability. In this case the possible way is just to apply “dangerous things” legislation. For instance, if a new AI system is equipped with a gun, it has at least to comply with the legislation on firearms use and trafficking.

Equivalent way is used in testing a new military weapon on compliance with international law. As one researcher claims: “*if we have a previously used autonomous robot and a previously used weapon, it may be possible to combine them without further*

permission” [10]. It means that legal norms applied to new AI technology are just a sum of legal norms that applied to parts of a new autonomous device or software. Sometimes it is possible and would be reasonable, but the high risk exists in this case that properties of a new technology is not a combination of properties of its parts.

Imagine that some citizen of the United States has an autonomous aerial vehicle (AAV) that is designed with ability to follow all regulations related to automatic flights. It has software with programmed rules that stops drone when it is going to approach to forbidden areas: airports, strategic objects, government buildings or something else that is defined in regulations of any flights. Moreover, the operator of this AAV has totally legal gun which he keeps at home following all legal conditions for self-defense. From the point of the United States gun control law such activity is absolutely legal [12]. However, if the person sets up the gun on a drone, such new device will have ability to hit any target in the city in a short period of time, it implies that the new device becomes more dangerous than two separate devices: the gun and the drone. As a result, such devices would be regarded as an autonomous distant killer machine that is totally legal if we just combine two systems of rules designed for gun control and flights regulation. It means that issues may arise when we just apply existing traditional legislation.

Installation of AI could make more dangerous even common thing. For instance, a regular car with an AI driver could be regarded as a serious weapon. A car with a flesh and blood driver is already used for committing terrorist acts and murders. For instance, well-known example is a car-ramming attack⁶. In case of fully autonomous cars criminals get additional benefit in terms of time and price of preparation.

For any criminal the use of AI implies minimizing chances of discovery and disruption. Probably, for an individual criminal it would be too expensive and difficult to get and reprogram an unmanned car. Consequently, it would not be very common for individual criminals but for well-equipped and well-funded terrorist organizations as it is perfect opportunity to create threat everywhere in the world. Could be such car securely used just in accordance with current law on car possession?

4. NEW CHALLENGES

Threats described above are related to physical characteristics of intellectual systems and refer to just one type of AI when it is produced as a device^{7,8}. However, probably most dangerous properties of AI systems are intellectual. Distinguished capability of AI to work with a big data and inexplicable reasoning are fraught with threats that are beyond the law.

For example, one deep neural network system relying on analysis of just 5 pictures from a dating site deduced the sexuality of people with accuracy more than ninety percent. As authors of this

⁵ See also: Criminal Law of the People's Republic of China, Article 121, <http://www.fmprc.gov.cn/ce/cgvienna/eng/dbtyw/jdwt/crimelaw/t209043.htm>; Criminal Code of Russian Federation, Article 226. Stealing or Possession of Arms, Ammunition, Explosives, and Explosive Devices, <http://www.wipo.int/edocs/lexdocs/laws/en/ru/ru080en.pdf>

⁶ Mass murder in which a terrorist intentionally rams a motor vehicle into a crowd of people

⁷ In research papers this type of AI is mentioned as robot with AI

survey claim “Additionally, given that companies and governments are increasingly using computer vision algorithms to detect people’s intimate traits, our findings expose a threat to the privacy and safety ...” [8]. It implies that if somebody has enough data to train neural network, he/she is able to seriously breach people’s rights.

Any user of a university’s library may find a lot of academic researches on the issue of getting personal data or characteristics by deep neural networks from open personal internet pages. Mostly it is forecasted that such software will have a positive character of application [7] but also it could be used to totally discriminate, manipulate or control people [1, 5, 9]. It is possible to recognize emotions without visual contact just by using the voice of a person [6]. The described systems have no ability to kill or harm someone but to bring a greater potential danger to humanity.

In accordance with Article 17 of International Covenant on Civil and Political Rights⁸ *«no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence»*. AI threatens to accepted conception of privacy, because if it is so simple to detect your sexuality, internal mental states, hidden attraction, there is no place for privacy. The border between private and public life will become obliterated.

From a moral point of view it is problematic to understand whether such capabilities of AI comply with moral standards or not. For example, a detection of an internal psychological state of some person and use of this knowledge [15], is it merit from moral point of view? As we know, explosives, a firearm could be used in a legal and ethically acceptable way. Somebody can use great power of AI in an ethically right way to predict suicide or other negative consequences of person’s psychological state [16]. At the same time, such powerful AI is a serious weapon against society and its use has to be controlled by law.

In accordance with logic on legal restrictions of a traditional “dangerous thing” use, it seems that the legislator has to consider such an opportunity in case of most powerful AI systems. It is not a discussion on a total ban of software or hardware that has described abilities but an attempt to justify reasonable legal control.

In different jurisdictions it would not be the same. Restrictions must derive from a common legal policy. For instance, in human rights friendly states it would be logical that the legislator will seriously limit AI intervention in personal life of its citizens and establish criminal liability for the most dangerous violation of personal interests. In other states efforts could be focused on AI technologies that could harm people, society or government.

Some issues that are related to intellectual capabilities of AI are beyond the scope of modern ethics. For example, some governments want to use AI to prognosticate illegal behavior of its citizens. China is going to use sophisticated software “to predict crime and social unrest before it happens”⁹. China is not unique since similar systems are used by the policing agencies of such countries as the United States, Japan, Israel and Chile.

There are no doubts that it is to a social benefit, but at the same time it is interference into personal affairs. Conceptually, it is against the criminal law paradigm since it implies that a “guilty mind” without a criminal act is enough for criminal liability. But what would be in case when potential criminal decides to abandon the perpetration at the last moment or some time before.

It is a distinguishing characteristic of a human being to have a freedom of will. Freedom of will implies that a person who intends to commit a crime has an opportunity to stop at any moment, even at the moment when all the preparations for an act of crime have been finished. But what would be in case when AI system suggests wrong. It is not hypothetical question; there are some cases when it happened. For instance, in a famous case when AI systems in China have accused a woman pictured on the side of a bus of jaywalking¹⁰.

Reader could suppose that described breach of human rights is possible only in not human rights friendly country. But practice shows that even European experience where human rights are strongly defended sustains that in case of protection of the interests of national security and public order, the economic welfare of the country, in order to prevent unrest or crime, to protect the health or morals or to protect the rights and freedoms of others’ right for privacy could be seriously limited¹¹. It implies that conceptually systems of detecting crimes or other destructive behavior are not against ethical and legal rules.

The problem is that previously such systems were possessed by states only. Nowadays anybody due to open source code and open datasets could develop complicated system that would detect internal patterns of a person. Wide availability of such systems could lead to spreading of crimes committed with AI.

Regulation on limiting the use of intellectual capabilities of AI to dig personal information is not panacea. The practice of the European Court on Human Rights proves that even for simple cases of infringements of human rights with use of Information Technologies it is difficult to apply legal means to invoke a right to privacy. “It is virtually impossible for a citizen to check for all of these data flows whether his data is included, who collects the data, whether that is done according to all legal principles and if not, to take the matter to court” [11]. It means that regulation to control use of artificial intelligence would be inapplicable because people whose rights are encroached would not know about violation. Moreover, they would not have resources to invoke their infringed rights.

It seems that in case of a criminal offence committed with use of artificial intelligence it would be easier to separate violations from non-violations. In this case harm and negative consequences are more transparent. It should be noted that a problem with a firearm and other “dangerous things” is not to detect offences but to withdraw such means from uncontrollable circulation.

If a state wants to ban distribution of some type of intellectual software because it is very dangerous to society, public order or state, it means that a state has to control at least copying of forbidden computer code. Such acts could lead to even more serious consequences, some of them are anticipated in literature.

⁸ International Covenant on Civil and Political Rights, Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966 (entry into force 23 March 1976)

⁹ <https://www.independent.co.uk/news/world/asia/china-ai-crimes-before-happen-artificial-intelligence-security-plans-beijing-meng-jianzhu-a7962496.html>

¹⁰ <https://www.bbc.com/news/technology-46357004>

¹¹ Article 8 sub 2. The European Convention on Human Rights, Status as of 10/11/2018.

For example, it could be regarded as the first step to construction the world described in George Orwell novel “1984”.

Potential problem with prohibition of some kind of dangerous artificial intelligence software is enforcement. To successfully enforce a ban on use of some artificial intelligence system would consequently demand some sufficient surveillance and monitoring of private computers.

5. CONCLUSIONS

The arguments presented in this paper should not be read as the dismissal or the relevance of current ethical, technical solutions and regulatory AI governance frameworks. This paper demonstrates that an applicability of law against uncontrolled circulation of dangerous artificial intelligence systems is very disputable. It looks simpler when a legislator has to deal with artificial intelligence that is a digital brain of some device, but it is impossible in case of dangerous intellectually powerful software. In this paper the arguments are provided that certain types of artificial intelligence systems should be regarded as dangerous and their use should be limited to the broad masses. This should be done taking into account the rights and freedoms of citizens, so that the fight against crime does not turn into total surveillance.

The authors in this issue expertly engage with various hard questions. From the paper, it becomes clear that the authors are unsatisfied with the current state of AI governance. Nowadays, there is a clear trend related to the expansion of intervention in the private life of a person, caused by the spread of AI technologies, and, accordingly, there is a need to develop new guarantees for the observance of human rights in the current information society.

6. ACKNOWLEDGMENTS

The reported study was funded by RFBR according to the research project № 18-29-16129.

7. REFERENCES

- [1] Celli, F., Bruni, E., Lepri, B. 2014. Automatic personality and interaction style recognition from Facebook profile pictures. In *Proceedings of the 2014 ACM Conference on Multimedia*, 2014. 1101-1104
- [2] Corruption, drug trafficking and other serious crimes (confiscation of benefits) act, (Chapter 65a), Singapore, <https://sso.agc.gov.sg/Act/CDTOSCCBA1992>
- [3] Criminal Law of the People's Republic of China, Section 7: crimes of smuggling, trafficking in, transporting and manufacturing narcotic drugs, <http://www.fmprc.gov.cn/ce/cgvienna/eng/dbtyw/jdwt/crimelaw/t209043.htm>.
- [4] Criminal Code of the Russian Federation, Articles 228-234, <http://www.wipo.int/edocs/lexdocs/laws/en/ru/ru080en.pdf>.
- [5] Kaur, A. 2018. Automatic personality assessment in the wild. In *2017 7th International Conference on Affective Computing and Intelligent Interaction, ACII 2017*, Volume 2018-January, 29 January 2018, 586-590
- [6] Ke, X., Zhu, Y., Wen, L., Zhang, W. 2018. Speech emotion recognition based on SVM and ANN. *International Journal of Machine Learning and Computing*, 8(3), 198-202.
- [7] Khalil, A., Hajjdiab, H., Al-Qirim, N. 2017. Detecting fake followers in twitter: A machine learning approach. *International Journal of Machine Learning and Computing*, 7(6), 198-202.
- [8] Kosinski, M., Wang, Y. 2018. Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *Journal of Personality and Social Psychology*, 2018. 114(2), 246-257
- [9] Lay, A., Ferwerda, B. 2018. Predicting users' personality based on their 'liked' images on Instagram. In *CEUR Workshop Proceedings*, Volume 2068, 2018, 2018 Joint ACM IUI Workshops, ACM IUI-WS 2018.
- [10] Sharkey, N. Killing Made Easy: From Joysticks to Politics in P. Lin, K. Abney and G. A. Bekey (eds.) 2012. *Robot Ethics: The Ethical and Social Implications of Robotics*, MIT Press, London, 2012.
- [11] Van der Sloot, B. 2018 A new approach to the right to privacy, or how the European Court of Human Rights embraced the non-domination principle. *Computer Law and Security Review*, 2018. 34(3), 539-549
- [12] Vernick, J.S. 2013. Carrying Guns in Public: Legal and Public Health Implications. *Journal of Law, Medicine and Ethics*, 2013. 41(SUPPL. 1)
- [13] Violent Crime Control and Law Enforcement Act of 1994 of the United States, <http://legisworks.org/GPO/STATUTE-108-Pg1796.pdf>
- [14] U.S. Code, Title 18, Chapter 40 – «Importation, manufacture, distribution and storage of explosive materials», <https://www.law.cornell.edu/uscode/text/18/part-I/chapter-40>.
- [15] Zhao, L., Jia, J., Feng, L. 2015. Teenagers' stress detection based on time-sensitive micro-blog comment/response actions. In *Artificial Intelligence in Theory and Practice IV, 4th IFIP TC 12 International Conference on Artificial Intelligence*, IFIP AI 2015, Held as Part of WCC 2015, Daejeon, South Korea, October 4-7, 2015, Proceedings. 26-35.
- [16] Zhao, L., Li, Q., Xue, Y. 2017. Correlating stressor events for social network based adolescent stress prediction. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10177 LNCS, 642-658.