DOI 10.22394/1726-1139-2023-4-30-36

The Deepfake Technology: Threats or Opportunities for Customs

Anastasia G. Getman[1, *], *Ling Yilan*[2]

[1]Russian Presidential Academy of National Economy and Public Administration (North-West Institute of Management, Branch of RANEPA), Saint Petersburg, Russian Federation;*getman-ag@ranepa.ru
[2]Shanghai Shanghai Customs Colledge, (SCC), Shanghai, China

ABSTRACT

The development of science and technology contributes to the expansion of opportunities for using new ways in various fields of activity — such as remote work, cloud computing, and so on, which makes any activity more convenient and efficient. However, high technologies are not always associated with a positive effect, as new technologies lead to new risks. The article discusses Deepfake technology, a popular artificial intelligence technology, with which it is possible not only to change, but also to fake data, such as images, video, audio. On the one hand, this brings benefits and profits to the film industry, and on the other hand, it can threaten the protection of intellectual property rights. Customs authorities using various technologies need to be prepared to respond to deepfakes. The article is devoted to the issues of taking into account the risks for the customs authorities of countries in connection with the emergence and spread of deepfakes.

Keywords: Deepfake, Customs, technology, Customs risks, Intellectual property rights

For citing: Getman A.G., Ling Yilan. The Deepfake Technology: Threats or Opportunities for Customs // Administrative consulting. 2023. N 4. P. 30–36.

Технология Deepfake: угрозы или возможности для таможни

Гетман А.Г.[1, *], *Лин Илань*[2]

[1]Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Северо-Западный институт управления РАНХиГС), Санкт-Петербург, Российская Федерация; *getman-ag@ranepa.ru
[2]Шанхайский таможенный колледж, Шанхай, Китайская Народная Республика

РЕФЕРАТ

Развитие науки и технологий способствует расширению возможностей использования в различных сферах деятельности новых способов — таких как удаленная работа, облачные вычисления и т.д., что делает любую деятельность более удобной и эффективной. Однако высокие технологии не всегда связаны с позитивным эффектом, так как новые технологии приводят к возникновению новых рисков. В статье рассмотрена технология Deepfake — популярная технология искусственного интеллекта, с помощью которой возможно не только изменять, но и подделывать данные, такие как изображения, видео, аудио. С одной стороны, это приносит пользу и прибыль в области киноиндустрии, а с другой — может угрожать обеспечению защиты прав на объекты интеллектуальной собственности. Таможенные органы, использующие различные технологии, должны быть готовы реагировать на «дипфейки». Статья посвящена вопросам учета рисков для таможенных органов стран в связи с появлением и распространением дипфейков.

Ключевые слова: дипфейк, таможенные органы, технологии, таможенные риски, права на интеллектуальную собственность

Для цитирования: *Гетман А.Г., Лин Илань.* The Deepfake Technology: Threats or Opportunities for Customs // Управленческое консультирование. 2023. № 4. С. 30–36.

Introduction of Deepfake

A. Information of Deepfake Technology

Talking about high-tech, the artificial intelligence (further — AI) is worth mention. In recent years, the AI technology has developed rapidly, with products of not only higher quality, but also of richer forms, covering texts, images, sound, videos, etc. Among all AI technologies, the «Deepfake» is one of the most popular. As a certain kind of AI technology, it can tamper, forgery and automatic generate images, sounds and videos so as to realize face synthesis, voice simulation, and even video generation.

The term «deepfake» first appeared on Reddit (a US social news site) in 2017, where a user named Deepfakes uploaded some pornographic videos in which the faces of the protagonists were transformed into famous people by an AI algorithm. Since then, the term «deepfake» has been used in the media to describe deep forgery technologies or contents [4].

Deepfake, also known as AI-generated media technology, is a technology, combining deep learning with forgery that uses deep learning models to modify and forge data such as images, videos and audio. The most important algorithm of it is generative adversarial networks, short as GAN. GAN is equipped with two neural networks at the same time — the generator and the recognizer. A generator, based on a database, can automatically generate samples simulating the data in the database. A recognizer can evaluate the authenticity of the data generated by the generator. The two networks can produce large-scale and highly accurate outputs in game learning. With the development of the GAN, it can forge or automatically synthesize almost all kinds of image, sound and video to a degree that people can hardly distinguish the false from the real [3].

Nowadays, the most common form of Deepfake technology is AI face-transformation technology and there have been some applications mainly based on it, such as Deepfake, Face2Face, etc. [5; 7]. At the same time, FakeApp, Faceswap, Zao, FaceApp and other such softwares have been developed for the public with no technical cost[1].

B. General Impacts of Deepfake Technology

a. Positive Impacts

Like most emerging high-techs, the Deepfake technology creates many new possibilities in people's daily life. Here follows some examples.

First, it can help to repair movies and resurrect some dead actors playing their roles in the films. Second, it can create some special sound effects and dubbing in audiovisual works. Third, the technology can make the applications come true that allow us to try new clothes and hairstyles without actually do so. Fourth, it can be used to produce videos for such training of enterprises and hospitals[2].

b. Negative Impacts

Even though we can't deny that the Deepfake technology brings a lot of potentials to us for a more interesting life, the abuse of this technology has led to lots of negative impacts, even crimes, which has risen more and more attention nowadays, especially in the ethic field. Here I'd like to enumerate some risks of the abuse of the Deepfake technology in different aspects.

---

[1] Foley J. 14 deepfake examples that terrified and amused the internet. Creative Bloq. 3 Mar. 2022 [Electronic source]. URL: https://www.creativebloq.com/features/deepfake-examples. Accessed 5 April 2022 (accessed: 20.02.2023); Xuan Jing. Why is it worrying after the video "face-transformation" reached to the public and set off hundreds of millions of streams. Wenhui Bao. 27 Feb. 2019 [Electronic source]. URL: https://wenhui.whb.cn/third /baidu /201902/27/244520.html (accessed: 20.02.2023).

[2] Ibid.

In terms of reputation, producing fake pornographic videos by Deepfake as AI face-changing technology would smear or retaliate against others. In terms of face recognition, cracking the verification system, such as face recognition with the help of the Deepfake technology would enable criminals to engage in activities under other people's names. In terms of business, producing and disseminating deeply forged information by Deepfake about commercial competitors would damage the goodwill and so on. In terms of copyright, deeply forged pictures or videos would cause disputes over copyright infringement and the fair usage. In terms of justice, the possible Deepfake works would pose challenges for courts to authenticate evidence such as audios and videos.

Risk of Deepfake to Customs

Since the potentials brought by the Deepfake technology are mainly in the creative sector, no need to explain its potentials speaking of the field of Customs here. And we'd like to analysis the risks which may be produced by the Deepfake technology to the Customs management.

A. Object of «Deepfake-Risks»

At the beginning, let's take a wider view on the objects in the field of Customs which might be infringe because of the abuse of Deepfake technology.

The first object comes to the Intellectual Property Rights (further — IPR) under Customs protection. According to TRIPS Agreement[1], Customs authorities have the obligation to stop the goods which might infringe someone's IPRs to cross the border. However, the Deepfake technology may obstruct the Customs authorities to tell the infringing goods and as a result fail to protect IPRs at the border.

Second, it comes to the application of Smart Customs. With the development of the science and technology, more and more high-tech equipment has been used in Customs management to provide efficient inspect and convenient service as encouraged by the WCO in the Revised Kyoto Convention[2] to use information technologies and electronic commerce. However, there also emerge some new technologies, just including the Deepfake technology, that could infringe the high-tech Customs equipment to tamper the live data so that the high-tech equipment might fail to identify a criminal or analysis a risk.

For example, due to the development Strategy of the customs service until 2030 the main purpose is to create the Intelligent customs [2].

The third is the integrity. Since Customs plays a significant role in trade facilitation, revenue collection, and national security, the integrity is quite important in Customs, so it was initially placed on the WCO Agenda in the late 1980s. No matter in the Revised Arusha Declaration[3] early in 2003 or in the Compilation of Integrity Practices on Internal

[1] WTO-TRIPS — Part III — Article 58 Ex Officio Action: Where Members require competent authorities to act upon their own initiative and to suspend the release of goods in respect of which they have acquired prima facie evidence that an intellectual property right is being infringed: (a) the competent authorities may at any time seek from the right holder any information that may assist them to exercise these powers; (b) the importer and the right holder shall be promptly notified of the suspension. Where the importer has lodged an appeal against the suspension with the competent authorities, the suspension shall be subject to the conditions, mutatis mutandis, set out at Article 55; (c) Members shall only exempt both public authorities and officials from liability to appropriate remedial measures where actions are taken or intended in good faith.

[2] WCO-Revised Kyoto Convention-General Annex-Chapter6 Customs Control: 6.9. The Customs shall use information technology and electronic commerce to the greatest possible extent to enhance Customs control. (J14)

[3] WCO-Revised Arusha Declaration-Chapter 1 Leadership and Commitment: The prime responsibility for corruption prevention must rest with the head of Customs and the executive management team.

Control and Relationship with External Controls[1] recently, the integrity issue is always with great significance. However, the newly emerged Deepfake technology is just able to giver more possibilities to the Customs officers to infringe Integrity in Customs by taking bribes, falsifying evidence, and so on.

B. Possible Risks

Nowadays there is a TikTok account dedicated to Tom Cruise Deepfakes, whose mastery of the actor's voice and mannerisms has resulted in one of the most convincing Deepfake examples[2]. It comes out that the technology of Deepfake now has developed to create the extremely highly realistic counterfeits. When these extremely highly realistic forged-things enter the field of Customs, lots of tough problems may emerge. The first problem comes to Customs is that the deeply forged pictures or videos make it extremely hard for Customs to tell the fake ones so the detection rate of infringing goods is going to reduce and the IPR will be more difficult to protect. What's more, the Deepfake of required documents by the enterprises, especially Deepfake of the signatures and seals in the document, may disrupt the Customs management.

Second, more security risks. According to the US Fortune magazine, in December 2019, the US company Kneron succeeded in deceiving the face recognition system of Alipay and WeChat payment, and passed the self-service terminal inspections in such places as the airport, railway stations with synthetic portrait videos made by the deepfake technologies [3]. In addition, an experiment of Swiss scientists came out with a terrible news that the latest facial recognition system has identified the «face-transformation videos» with a result of a 95% error rate [6]. As a result, it can be imaged that the deeply forged pictures or videos are able to forge personal identity to pass the Customs face recognition system. The deeply-forged pictures may tamper with people's passport information. What's worse, some deepfake works may successfully fool the facial recognition systems in Customs supervision zones, such as the condition in an airport as in the example. It may help someone, especially an internationally wanted criminal or smuggler, cross the border successfully under false identities. Under this circumstance, the high-tech equipment of e-Customs these days to work with graph and video information, including the face recognition system, as well as the intelligent examination system and 350° intelligent monitoring system, may be affected inevitably.

Third, more integrity problems. a streaming service platform has put forward a video made with Deepfake technology to gather the super recognizable faces of Tom Cruise, Robert Downey, Jr, George Lucas, Ewan McGregor and Jeff Goldblum discussing streaming and the future of cinema at a roundtable[3]. It means people may create video in which anyone will do anything as the creator want, so it is possible that the forged video includes a Customs officer one day.

Then what will happen?

On one hand, deeply forged voices or videos may impersonate a Customs officer to fabricate decisions so as to deceive or blackmail the declarants. On the other hand, lots of risks may appear concerning the integrity. One possibility is that Customs officers may use the Deepfake technology to change the related audio and video data from the

[1] WCO-Compilation of Integrity Practices on Internal Control and Relationship with External Controls-FORWARD: In order to be fully effective in preventing corruption and executing their broad mandate, Customs administrations should design and implement appropriate control mechanisms for detecting unethical behavior, including provisions for in-depth investigations into potential breaches of internal policies and the application of proportionate sanctions, where appropriate.

[2] *Foley J.* 14 deepfake examples that terrified and amused the internet...; *Xuan Jin*g. Why is it worrying after the video "face-transformation" reached to the public and set off hundreds of millions of streams...

[3] Ibid.

internal network. For example, they may change the videos of the law enforcement recorder to cover up the Customs officers' wrong behaviors in law enforcement, such as inspection not complying with the requirement, the violence of law enforcement, taking bribes, etc. Another possibility is that enterprises may use deeply-forged videos to tamper with the surveillance videos of the customs warehouses and such places, affecting customs law enforcement, to cover up their Customs-found problems and avoid Customs control.

Suggested Solution to Customs

The risks produce by the Deepfake technology are just emerge as the development of this high-tech. The field of Customs has been affected too. It's quite important for the Customs around the world to pay attention to the Deepfake condition these days and then to prevent and solve the risks brought by the technology and take measures to fight against these risks to maintain the efficacy and authority of the Customs management.

A. Solution to Customs Authorities

First, the Customs authorities may specifically train the Customs officers for the Deepfake problem, which enables the officers to identify the Deepfake works and protect IPRs on the border better. It is expected be a feasible action since that a joint team of scientists has tested 1000 face-transformation videos and found that ordinary people have to go through special training to tell the real from the fake [1].

Second, the Customs authorities may cooperate with scientific research institutes to develop new identification technology suitable for Customs inspection to improve the detection rate of Deepfake works. As known, there are many scientists dedicated to develop such technologies to identify the Deepfake works and they have actually got some achievement. For example, it is found that the blinks, the eye condition[1], and the subtle changes when blood entering the skin of the person in the face-transformation videos [6] can be used to identify the Deepfake video. What's more, there has already developed some Deepfake identification technologies, such as Reversed Cracking, a technology to identify face-transformation videos[2].

Third, with the development of science and technology as well as the changing environment nowadays, the Customs authorities around the world all start e-Customs, which is a new type of high-tech management with great efficiency and importance. So, facing such risks brought by the Deepfake technology in e-Customs as mentioned before, the Customs authorities should focus on the risks and put forward measures to solve them and support the development of e-Customs. As a result, the Customs authorities may depend on the risk management system and combine the technical inspection of e-Customs and the traditional physical inspection to strengthen the cross-border supervision.

Fourth, another solution for the e-Customs is that the Customs authorities may optimize their internal network system, improving the security protection and strengthening the management authority of the supervision network to avoid data tampering caused by both the Customs side and the enterprises side.

Fifth, although the Deepfake works cause almost technical problems, the solution of propaganda and education is of equal importance. As for the public, the Customs au-

[1] Schwartz O. You Thought Fake News Was Bad? Deep Fakes Are Where Truth Goes to Die // THE GUARDIAN. Nov. 12, 2018 [Electronic source]. URL: https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth (accessed: 20.02.2023).

[2] Ibid.

thorities may propagandize more Customs policies of IPR protection to the public to increase authority so as to help the public not to be deceived. As for the Customs themselves, the Customs authorities may highlight the integrity education of Customs officers and add the data security and protection to the existing Customs quality education. As for the related enterprises, the Customs authorities may strengthen the propaganda and education among enterprises to avoid the occurrence of counterfeiting events at the source.

B. Solution to WCO

WCO, as an international organization united with the world's Customs, should also pay attention to the risks appearing with the Deepfake technology and take some special measures to lead the Customs around the world better overcome the problems.

First, it is significant for WCO to provide assistance on the Deepfake prevention. Not all Customs authorities around the world have the ability to identify the Deepfake or deal with the problems brought by the Deepfake, especially the undeveloped areas. As a result, WCO may provide international assistance on the Deepfake issue, including the technical assistance, human resource construction and best practice introduction.

Second, WCO may gather the scientists and institutes to further research the unique characteristics of Deepfake products so as to help develop the anti-Deepfake technologies special for Customs inspection at the global level with its unique international influence and appeal as well as its significant fund.

Third, WCO may cooperate with other international organizations, such as WIPO and WTO, to take cooperated measures to work with the Deepfake issues in the aspect of international construction of legislation or agreement, propaganda and so on.

Conclusion

Deepfake technology, a complicated and advanced technology, is a product of a certain stage of AI development. Nowadays, it can generate highly realistic audiovisual works that human abilities and technologies can hardly identify, which has brought both positive potential and negative risks in our life. For example, Rospatent has issued two patents to Sberbank for technologies that help detect deepfakes. It means, that big organizations began to seriously engage in developments in this area[1].

So is in the Customs field. Summing up, the Customs should face the problems emerged with the Deepfake technology directly and work out some targeted solution to maintain the high-quality of Customs management.

References

1. Getman A.G. The digitalization of mechanisms of interaction of right holders with the federal Customs service of Russia when receiving a public service for maintenance of the customs register of intellectual property objects // Theory and practice of management of state functions and services. Tariff regulation: a collection of scientific papers based on the results of the National scientific and Practical Conference, St. Petersburg, November 10–17, 2021. SPb. : St. Petersburg State University of Economics, 2021. P. 64–69 (in Rus).
2. Getman A.G. Digitalization of customs technologies as a factor in improving the reliability of supply chains // Advances in chemistry and chemical technology [Uspekhi v khimii i khimicheskoy tekhnologii]. 2022. Vol. 36. N 1 (250). P. 23–25 (in Rus).
3. Cao Jian-feng. Deepfake technology: the legal challenge and response // Information Security and Communications Privacy. 2019. N 10. P. 35–40.

[1] [Electronic source]. URL: https://incrussia.ru/news/sber-deepfake/ (accessed: 28.11.2022).

4. Li Minglu. The Criminal Law Approach to Deep Fake. Science Technology and Law Chinese-English. 2021. N 5. P. 40–47+73. DOI:10.19585/j.cnki.cn11-2922/n.2021.05.005.
5. Meng Xue, Liu Zongyuan, and Li Qlan. Challenges and countermeasures brought by deepfake to network trusted identity management // Cyberspace Security. 2020. 11.05. P. 75–79.
6. Yan Xin, Hua Ling. Al face transformation also has a bug, see if the character blinks // Science and Technology Journal. 2019. 18 Mar. [Electronic source]. URL: https://baijiahao.baidu.com/s?id=15282982 94084425847&wfr=spider&for=pc (accessed: 09.03.2022).
7. Wang R., Chu B., Yang Z., Zhou L. An overview of visual Deep Fake detection techniques // Journal of Image and Graphics. 2022. Vol. 27. N 1. P. 43–62. DOI: 10.11834/jig.210410.

About the authors:

Anastasia G. Getman, Associate Professor of Department of Customs Administration of North-West Institute of Management, Branch of RANEPA (St. Petersburg, Russian Federation), Candidate of Economic Sciences, Associate Professor; getman-ag@ranepa.ru

Ling Yilan, Student of 4 course of the Faculty of Customs Administration, Shanghai Customs Colledge, China; 744640189@qq.com

Литература

1. *Гетман А.Г.* Цифровизация механизмов взаимодействия правообладателей с ФТС России при получении государственной услуги по ведению таможенного реестра объектов интеллектуальной собственности // Теория и практика управления государственными функциями и услугами. Тарифное регулирование : сборник научных трудов по итогам IV национальной научно-практической конференции, Санкт-Петербург, 10–17 ноября 2021 года. СПб. : Санкт-Петербургский государственный экономический университет, 2021. С. 64–69.
2. *Гетман А.Г.* Цифровизация таможенных технологий как фактор повышения надежности цепей поставок // Успехи в химии и химической технологии. 2022. Т. 36. № 1 (250). С. 23–25. EDN PWVADS.
3. *Cao Jian-feng.* Deepfake technology: the legal challenge and response // Information Security and Communications Privacy. 2019. N 10. P. 35–40.
4. *Li Minglu.* The Criminal Law Approach to Deep Fake. Science Technology and Law Chinese-English. 2021. N 5. P. 40–47+73. DOI:10.19585/j.cnki.cn11-2922/n.2021.05.005.
5. *Meng Xue, Liu Zongyuan, and Li Qlan.* Challenges and countermeasures brought by deepfake to network trusted identity management // Cyberspace Security. 2020. 11.05. P. 75–79.
6. *Yan Xin, Hua Ling.* Al face transformation also has a bug, see if the character blinks // Science and Technology Journal. 2019. 18 Mar. [Electronic source]. URL: https://baijiahao.baidu.com/s?id=15282982 94084425847&wfr=spider&for=pc (accessed: 09.03.2022).
7. *Wang R., Chu B., Yang Z., Zhou L.* An overview of visual Deep Fake detection techniques // Journal of Image and Graphics. 2022. Vol. 27. N 1. P. 43–62. DOI: 10.11834/jig.210410.

Об авторах:

Гетман Анастасия Геннадьевна, ведущий научный сотрудник НИЛ Стратегического планирования и евразийской интеграции, доцент кафедры таможенного администрирования Северо-Западного института управления РАНХиГС (Санкт-Петербург, Российская Федерация), кандидат экономических наук, доцент; getman-ag@ranepa.ru

Лин Илань, студент 4 курса факультета таможенного дела Шанхайского таможенного колледжа (Шанхай, КНР); 744640189@qq.com