Advances in Social Science, Education and Humanities Research, volume 441
6th International Conference on Social, economic, and academic leadership (ICSEAL-6-2019)

Legal Protection of Personal Image in Digital Relations: Leading Trends

Galina Komkova*
Saratov State University
Astrakhanskaya str. 83, 410012 Saratov
Russian Federation
e-mail: komkova_galina@mail.ru

Roman Amelin
Saratov State University
Astrakhanskaya str. 83, 410012 Saratov
Russian Federation
e-mail: ame-roman@yandex.ru

Svetlana Kulikova
Saratov State University
Astrakhanskaya str. 83, 410012 Saratov
Russian Federation
e-mail: kulikovasveta@inbox.ru

Abstract. Development of digital technologies creates new opportunities for obtaining and using the image of a citizen without her or his knowledge. This creates serious problems in both public law and civil law relations. A study of domestic and foreign scientific legal literature shows that the content of the human right to own image remains insufficiently developed by modern legal science. Most often, the right to an image is narrowed down to protection from illegal distribution of photographs and video materials, as evidenced by both Russian judicial practice and the practice of the European Court of Human Rights. An important legal problem is the use by state bodies of facial recognition technologies (FRT). These leading technologies are useful for finding people during disasters, identifying a person in the "smart city" system, identifying offenders and tracing criminals. However, there are doubts about the constitutionality of the use of FRT both for video surveillance in the real physical world, and for identifying individuals on online services and websites, since there is no sufficient legal regulation of the use of these information technologies. This can provoke violations of the rights of citizens by state bodies and officials. A comprehensive legal regulation of the implementation of the human right to own image, as one of the components of the right to privacy, personal and family secrets, is necessary. We conclude that modern states are obliged to develop and adopt legislative measures that do not allow the use of an electronic profile of a person without his consent.

Keywords: *legal protection, personal image, digital relations, leadership*

1 Introduction

With the development of digital technology, users can post their photos and video fragments, as well as images of other people on the Internet. They can easily copy, modify and distribute them. Posting on social networks and on YouTube channels of photo and video materials creates certain problems of legal regulation of their further use. The use of technologies for identifying persons in commercial or public interests may lead to a violation of their rights. The ability to recognize faces from photographs posted on social networks or online galleries poses threats to privacy.

Every person from birth has an individual appearance. The right to appearance belongs to the category of personal rights of citizens, such as the right to a name, personal inviolability, privacy, honour, dignity and business reputation. An important component of these rights is the possibility of self-identification of a person, awareness of his uniqueness, especially in relation to other people.

The ability to fix the appearance of a citizen using video and photography or using artistic methods gives rise to the right to a personal image, i.e. the right of the subject whose appearance is represented in the image to independently determine the fate of portraits, photo and video materials with his appearance.

In the legal doctrine, the right to a personal image is considered in several aspects:

- in constitutional law, as a component of the right to privacy, the right to personal dignity;
- in civil law, as protection of the object of civil rights;
- in informational law, as the use of biometric personal data in modern Big Data processing technologies.

In connection with the above, it is important to study the regulatory legal acts of Russia and other states that govern the implementation of the subjective right to a personal image; conduct an analysis of judicial practice on the protection of the right to an image and formulate proposals for improving legislation in this area.

2. Personal image as a component of the right to privacy and the right to dignity

The ban on the use of the image of a citizen without his consent is one of the elements of privacy guaranteed by the constitutions of most democratic states and international legal acts. In Russian constitutional law, private life is considered as a complex category, which includes freedom to dispose of oneself, confidentiality of personal and family information, confidentiality of correspondence, inviolability of the home, secrecy of voting (Lopatin 1999), the right to dignity of the person, freedom of conscience and confession, reproductive rights (Romanovskij 2001; Veliyeva 2014), the right to restrict access to information about a person's private life (Kulikova 2012). In the works of foreign scholars, privacy is understood as the degree of independence of the individual from the attention of society and the state. The definition of the right to privacy as "the right to be left alone" (Margulis 1977) has become most famous. The right to privacy is interpreted as the right to independently determine the boundaries of personal information space (Alderman and Kennedy 1997; Solove 2008), the degree of anonymity of the person, that is, "invisibility" for government agencies, trading and marketing campaigns (Kobsa and Schreck 2003; Culnan 1993; Kim 2004; Smith et al. 2011), including IT anonymity. Free access to the Internet, the ability to post various kinds of information about yourself and other people often contribute to the violation of the right to privacy. This has created a new scientific problem: the definition of legal and ethical mechanisms for protecting the private space of an individual in the digital age (Mazaev 2016; Barinov 2016; Acquisti and Gross 2006; Bowie and Jamal 2006; Boyd 2008; Culnan 2000).

Privacy is guaranteed by the norms of generally recognized international acts: Art. 12 of the Universal Declaration of Human Rights, art. 17 of the International Covenant on Civil and Political Rights (1966). These documents prohibit arbitrary and unlawful infringement of privacy information, and also guarantee the right to protect the law from such interference (OHCHR 1948).

Although these acts were adopted in the middle of the last century, the rights enshrined in them did not lose their relevance. International organizations are discussing the need for their support in modern conditions. Secrets of privacy are currently being addressed through the prism of digital telecommunication technology. So, in the UNGA Resolution of December 18, 2013 (A/RES/68/167) "The Right to Privacy in the Digital Age", the concept of extending guarantees of human rights to the virtual environment was formulated: "same rights that people have offline must also be protected online".

These ideas were further developed in the Report of the Office of the United Nations High Commissioner for Human Rights of June 30, 2014 and the UNGA Resolution "The Right to Privacy in the Digital Age" (A/RES/69/166) (UN 2014). In particular, the Resolution states that the effective solution of problems related to the right to privacy in the context of modern communication technologies requires constant dialogue and coordinated participation of all interested parties: governments, civil society, the scientific and technical community, business, scientists. There is an urgent need to ensure that any surveillance policy or practice complies with human rights requirements, including the right to privacy, through the development of effective mechanisms to guarantee protection against abuse.

The right to privacy, respect for personal and family secrets is fundamental, but international acts provide for the possibility of restricting it to achieve publicly significant goals. Thence, Art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms of November 4, 1950 provides for three interrelated conditions under which interference with privacy is permissible (ECHR 1950):

1. such interference is prescribed by law;
2. it is necessary in a democratic society;
3. it is carried out for the purposes specified in the Convention: in the interests of national security and public order, the economic well-being of the country, in order to prevent unrest or crime, to protect the health or morality, or to protect the rights and freedoms of others.

In Russian law, the restriction of the right to privacy in the aspect of the realization of the right to an image is possible when the use of the image is carried out in the state, public or other public interests (Article 152.1 of

the Civil Code of the Russian Federation) (Civil Code of the Russian Federation 1994). Defining these interests is key. The Decree of the Plenum of the Supreme Court of the Russian Federation "On the application by the courts of certain provisions of Section 1 of the first part of the Civil Code of the Russian Federation" (June 23, 2015, No. 25) states that there is public interest in cases where "a citizen is a public figure (occupies a state or municipal office, plays a significant role in public life in the field of politics, economics, art, sports or any other field) and the publication and use of the image is carried out in connection with political or social discussion or interest in the person is socially significant". The same resolution clarifies that the image of a citizen can be used without his consent in order to protect law and order and state security (for example, in connection with the search for citizens, including missing persons or participating in or witnessing offenses (paragraph 44) (Civil Code of the Russian Federation 1994).

The concept of "public interest" was also explained in the Decree of the Plenum of the Supreme Court of the Russian Federation of June 15, 2010 No. 16 "On the Practice of the Application by the Courts of the Law of the Russian Federation "On Mass Media", which specifically indicated that not every interest shown by the audience should be attributed to the public interest. For example, the need of society for the detection and disclosure of threats to a democratic rule of law and civil society, public safety, and the environment is a public interest. In this connection, the Plenum of the Supreme Court of the Russian Federation recommended that the courts delimit reports of facts concerning the performance of their functions by officials and public figures, and, for example, messages about the details of the private life of a person who is not involved in any public activities (Supreme Court of the Russian Federation 2010).

The possibility of restricting the right to a personal image as a component of the right to privacy for the purpose of disseminating information of public interest has repeatedly become the subject of appeals to the Constitutional Court of the Russian Federation. In 2019, this court several times considered the constitutional provision, which states that it is allowed to collect and disseminate information about a person's private life (including his image) if, due to his profession, occupation and other circumstances, he is in the centre of public attention and public interest is manifested in any information about him.

The activities of the Constitutional Court are one of the most effective mechanisms for protecting the Constitution, protecting human rights and freedoms and restoring them (Komkova 2015). In its determination on the complaint of Bezrukov dated February 12, 2019 No. 274-O, the Constitutional Court indicated that information about private life, especially of an intimate nature, cannot be recognized as socially significant information only because it concerns a public (widely known in society) person including representatives of creative professions.

In the determination of March 26, 2019 No. 698-O on the complaint of Leonova, the Constitutional Court noted that the conditions for the publication and use of the image of a citizen must be observed in the aggregate - in other words, the mere inclusion of a person as a public figure is not enough for the publication and use of his personal image.

The problem of realizing human rights on the Internet is increasingly attracting the attention of the European Court of Human Rights. According to the estimates of Antopolsky at the end of May 2019, the European Court examined about 2.5 thousand cases, on complaints of violation of rights on the Internet, including cases in which the Russian Federation acted as a defendant (Antopolsky 2019).

Complaints of persons who file a violation of their right to their own image in the media or on the Internet are dealt with under Article 8 of the Right to Respect for Private and Family Life and Article 10 of the Freedom of Expression of the European Convention. In considering complaints of a violation of the right to a personal image, the Court takes into account the objectives of the publication and further use of images. For example, in the case of Toma v. Romania, the ECHR indicated that photographing and further publicizing the photograph of the applicant at the police station did not meet the objectives set by the European Convention (for example, searching for a criminal, ensuring his appearance in court, satisfying the interests of justice) (ECHR 1950). In the case of the Ageevs v. Russia, the European Court considered that although the discussion about the ill-treatment of the adopted child was indeed of great public importance, the publication of his photograph during his stay in the burn centre did not add any necessary information and was redundant, therefore, the ECHR found a violation the right to privacy of the child and his right to image. The criterion of conformity or non-compliance with the purpose of restricting the right to a personal image was used in other similar cases (Verlagsgruppe News GmbH v. Austria, Murray v. The United Kingdom, Nimitz v. Germany, Ashby Donald v. France).

3. The right to a personal image as an object of civil rights

In civil law, the image of a citizen is "a material object (thing), which nevertheless embodies the intangible appearance of a citizen" (Gavrilov 2015; Mikryukov 2013). The dual nature of the right to a personal image, which combines ideal and material good, is paid attention to Russian and foreign Researchers (Fridman 2019; Synodinou 2014; Logeais and Schroeder 1998). Researchers note that in modern conditions there is an "unprecedented commercialization of the individual" (Belyaeva 2019), images of personalities, and not only well-known ones, are used when promoting a product or service on social networks; photos are used for

window dressing, printing advertising products, on customer feedback pages, on the sites of medical clinics and beauty salons to illustrate the effect of the provision of services, etc. (Jung 2011). In such situations, the problem of the legality of using the image is articulated, first of all, as the presence or absence of the need to coordinate with the subject the possibilities and conditions for placing its image.

The already mentioned Decree of the Plenum of the Supreme Court of the Russian Federation dated June 23, 2015 No. 25 indicates that a citizen's posting of his image on the Internet makes his image public, but does not give other people the right to freely use such an image without obtaining the consent of the person represented.

An analysis of court decisions on civil claims allows us to conclude that the courts almost always side with the plaintiffs, whose right to image was violated. However, the amount of compensation for non-pecuniary damage varies and largely depends on the purpose of using the image, the degree of distribution of the contentious informational materials and the nature of the plaintiffs suffering. For example, in one case, a photograph of the plaintiff without her consent was posted on a site whose owner specialized in providing "consulting services to men to improve communication skills in dealing with women", and the photograph was used to attract the attention of potential customers. The Cheryomushkinsky District Court of Moscow held that approximately $ 40 was enough to compensate for the moral damage of the plaintiff (decision No. 2-4448 / 19 of September 5, 2019). In another case, the plaintiff's photo was used as an illustration on a site that advertised retro shows of Soviet pop stars without his consent. The Leninsky District Court of Perm decided to recover 10 times more compensation for non-pecuniary damage in favor of the plaintiff - approximately $ 400 (decision No. 2-3296 / 2019 of November 7, 2019). A rather big resonance was caused by a case when a resident of Yekaterinburg discovered that her photo was used to advertise samples of tombstones for monuments. The Kirov District Court of Yekaterinburg decided to recover non-pecuniary damage in the amount of approximately $ 600 (decision No. 2-5882 / 2019 of December 18, 2019).

The use of information technology allows you to create distorted versions of images (in Russia, for example, the so-called "Internet memes" and demotivators are popular). As a result, persons whose images are distorted in this way consider that their right to dignity is violated.

Researchers have noted that claims for protecting the right to a personal image are often accompanied by libel suits and suits for intentionally causing emotional distress (Barbas 2015; Dogan and Lemley 2006; Tan 2008).

In Russia, the case related to the placement in the Internet encyclopedia "Lurkmore" of the image of the singer Syutkin with an obscene signature-meme gained the greatest fame. The Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) filed a lawsuit in defence of the singer with reference to the Federal Law "On Personal Data" (On Personal Data 2006). Roskomnadzor pointed out that the image together with the person's name and surname constitute personal data and therefore cannot be processed and published without his consent, and the case of the creation of a meme was interpreted as processing personal data. The lawsuit was upheld by the court. Later, the agency posted an explanation that using a public person's photo as the personification of an Internet meme that is not related to his personality is a violation of personal data law.

Judicial practice to protect one's appearance from distortion is not widespread. An example is the case considered by the Judicial Collegium for Civil Cases of the Arkhangelsk Regional Court. The plaintiff demanded the removal of the Internet page on the social network Vkontakte. An abusive text about a man named Dmitry and a photo of a male plaintiff with a "female appearance" edited using Photoshop were posted on this page. The court acknowledged that the text was indeed offensive, but considered that Dmitry's name was not enough to identify the applicant, and the photograph depicted a woman who did not look like the plaintiff, therefore the lawsuit was denied (33-5048/2017 September 11, 2017).

4. Personal image in the conditions of modern Big Data processing technologies

The next aspect of considering the implementation of the right to a personal image is associated with successes in the processing of "big data" and pattern recognition algorithms, which is due, firstly, to the widespread use of video surveillance, and secondly, to the use of digital face recognition (FRT) technologies.

Face recognition technologies today are part of regularly used biometric methods that automatically recognize a person based on his physical, biological or behavioural characteristics ((Rassolov et al. 2019). Since 2002, biometrics has been recognized as the main method of identification in documents standardized by the International Civil Aviation Organization (ICAO) at the UN. ICAO member countries accept FRT as the main and mandatory method of identification (which can be supplemented at the discretion of identification using fingerprints, scanning the iris, etc. (Mamaev 2018)).

Throughout the world, government agencies use CCTV cameras in transport hubs, in crowded places, using FRT to search and mark individuals — in order to control migration at borders and within countries (Romashov 2019), and to detect offenders. Considering the problem of implementing an administrative ban on

visiting certain places, Shavaleev (2017) enthusiastically writes about the prospects of an intelligent face recognition system: “the system should be structured in such a way that when fixing a person with a ban, it will immediately be delayed”, which “will lead to the effective execution of this type of punishment, thereby preventing the commission of new offenses by these persons” (Shavaleev 2017; Stepanov 2012).

Face recognition technologies are one of the important building elements of the infrastructure of the modern information society – both in its everyday manifestations (for example, speaking about the functioning of “smart cities”, accounting systems of “electronic government”), and in critical situations (for example, searching for people during disasters). At the same time, the threat of violation of the rights of citizens associated with the dissemination of these technologies is becoming increasingly relevant and alarming.

We are concerned about large-scale government projects to create biometric databases (primarily personal images) without sufficient legal and procedural guarantees for their use. We are witnessing such threatening trends as the growth of the analytical potential of technologies based on the use of data in a geometric progression; mass tracking; access to user data available to commercial enterprises; the introduction of mandatory requirements in various states for telecommunications companies and Internet service providers that require them to store communications data for a long period of time, attempts to weaken encryption and anonymity at the state level, the exchange of intelligence data, and, finally, the threat of hacking biometric databases by both public services and ordinary offenders (Romashov 2019).

In the fall of 2019, the Savelovsky District Court of Moscow refused to satisfy the requirements of Popova. She demanded to remove her images from the database and recognize the actions of the Department of Information Technology of the Main Directorate of the Ministry of Internal Affairs of Russia on the use of FRT in the "City CCTV System" as illegal. The judge pointed out that “the Department does not carry out activities aimed at establishing the identity of a particular citizen. The database does not contain personal data of citizens (name, etc.), as well as biometric personal data (iris, height, weight, etc.) that are necessary to establish the identity of a citizen. The face recognition algorithm compares the image coming from the cameras with the photo provided by the law enforcement agency. The Department does not receive personal data of persons, since the Department does not have the technical and legal ability to compare them. Thus, in the absence of a personal identification procedure, video images of citizens cannot be considered biometric personal data. Accordingly, there is no need to obtain the citizen’s written consent for the processing of biometric personal data”.

This reasoning, in our opinion, is unreasonable, since the legislation refers to personal data any information relating directly or indirectly to a specific individual. This person was determined and brought to administrative responsibility precisely on the basis of the analysis of archived videos, which was the reason for going to court. Arguments that a particular operator cannot independently carry out such identification, and the pattern recognition algorithms themselves can reveal a coincidence with only 65% probability, are obviously inconsistent and would deprive the whole legal construction of the protection of personal data meaningless, leading to a vicious circle: before identification of a citizen there is nothing to protect, and after identification it is too late.

This logic is even less true with respect to generally accessible archives, databases, and individual photo and video recordings containing images of citizens. Modern technologies for processing "big data", the availability of millions of digital "profiles" of citizens in social networks, numerous leaks of personal data bases lead to the fact that the identification of a particular person in a photo or video is only a matter of desire and means.

The trend of restricting the use of face recognition technologies arises in a number of democratic countries. So, in 2019, San Francisco imposed a complete ban on the use of FRT by the police and other municipal services to counter potential abuse (Conger et al. 2019). In October 2019, the forty largest world music festivals promised to abandon the use of this technology (Gurley 2019). A lawsuit was filed against the developer of the Clearview AI application, widely used by US law enforcement to identify suspects. The complaint notes that the defendant “without obtaining any consent and without notice” used the Internet to covertly collect information about millions of American citizens. He downloaded about three billion photographs, and then used artificial intelligence algorithms to scan the geometry of the faces of each person depicted in the photographs (Khodakovsky 2020). According to human rights defenders, the method itself violates many privacy laws.

At the same time, in other countries the opposite trend is observed, aimed at building a system of total control. So, in China, personal space is steadily narrowing. In secondary schools, an experiment is being conducted on equipping classes with smart cameras, which can determine not only what the student is doing, but also his psycho-emotional state by facial expression (Antonova et al. 2019). A full-fledged system of “social rating” and continuous monitoring has been established for Uyghurs in the Xinjiang Uygur Autonomous Region of China. According to press reports, China has become the first country to use this technology for video surveillance of people based on ethnicity: “just like the recognition system tags “rec_female” or “rec_sunglasses”, it also tags “rec_uygur”. If one Uigur lives near the place of installation of the CCTV camera

and, say, six Uighurs come to him within 20 days, the system will send an alarm notification to the police" (The Security News 2019).

It seems extremely controversial to introduce a moratorium on a certain group of data processing methods and declare them to be obviously illegal. We think so, not only because these methods are widely and effectively used "for peaceful purposes", but also because, according to the extremely accurate statement of Bruce Schneier, "attention to one specific identification method distracts from the nature of that observation society, ... where the widespread mass surveillance is becoming the norm" (Schneier 2020). Face recognition technologies are only a small part of the total surveillance system, in which identification is only the first step in the further processes of correlation and discrimination. It is important for companies and governments to distinguish between people in order to treat them differently (this includes displaying various advertisements, offering different tariffs for services, and the special attitude of the state, for example, to persons identified as demonstrators).

Face recognition is not the only technology associated with the processing of personal images of people, the use of which leads to a violation of their rights. In recent years, manufacturing techniques for fake photos and videos have reached a certain technical excellence. They transfer facial features from the image of a person to the target video (photo) with a high degree of credibility. This technology is called "deepfake". The first deepfake video appeared in 2017, in which the celebrity's face changed places with a porn actor (Nguyen et al. 2019). Globally, the use of such technologies poses a threat to global security, since deepfake methods can be used to create videos of world leaders with fake speeches and other similar content aimed at discrediting, hate propaganda, etc. (Chesney and Citron 2019; Howcroft 2018). But if in national legislation, as a rule, legal means are provided for counteracting such acts (for example, in the Russian Federation in 2019 a law was passed establishing liability for disseminating inaccurate socially significant information under the guise of reliable messages), then the problem of violation of personal rights using deepfake technologies, it is not fully understood and developed. Meanwhile, the personal rights of a citizen can be violated without the spread of fakes with the aim of falsification or discrimination. So, in 2019, the paid service DeepNude received significant popularity. Its developers trained the neural network to "undress" the women depicted in the photographs, selecting and substituting nude samples that are most suitable for the figure in the photo in automatic mode. The service turned out to be so popular that the authors themselves were forced to close it, fearing numerous lawsuits.

Currently, the law enforcement practice of several states qualifies the use of appropriate technologies as slander if it is proved that fake images were distributed with malicious intent. In some countries, such as the UK, there are such crimes as pornography or cyberbullying. In the United States, the Senate is considering a bill "Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019", which provides for criminal liability for the distribution of defamatory citizens with fake photos and videos made using neural networks (H.R.3230 2019). However, a violation of a woman's personal rights, of course, also occurs in cases where such images are created without the goal of further distribution, although at the moment a certain legal position on this issue has not been developed.

5. Conclusions

Overall, the announcement of any technologies, algorithms, computer programs obviously outlawed is seen as a hopeless measure at this stage. History has not yet known significant success in this direction, from the pursuit of creating the first torrent trackers to modern crypto messengers. Legal thought should develop in the direction of increasing the effectiveness of legal regulation of the use of such technologies.

First, the prospects for such regulation are seen in relation to technologies massively used by government bodies and large companies, including face recognition technology. The accumulation of videos with images of citizens, the creation of digital profiles that can be compared, the use of intelligent algorithms to identify a person, the subsequent decisions and actions regarding such a person - each of these steps should be regulated as much as possible. Limitations should be worked out aimed at maintaining a balance between ensuring freedom of citizens and their safety. In particular, it is possible to allow the creation of digital profiles only for a limited circle of persons (wanted offenders, missing persons, etc.), although in this case it will be difficult to identify persons who have committed an offense for the first time and who have come to the cameras. Severe restrictions should be imposed on the exchange of identification data, as well as the use of identification technologies by private companies, unless the user voluntarily agrees to identify his face (for example, to unlock a smartphone, etc.) with strict control of storage and the transmission of information arising from such goals.

In general, in our opinion, the possibilities of modern information technologies related to the processing of personal images of people require a new careful reading of such constitutional rights as the right to privacy, freedom and personal inviolability. So, the concept of personal integrity must be extended to the "digital forms of existence" of an individual - reflected, inter alia, in personal images, videos, virtual

accounts. The right to privacy is not so much connected with the protection of communications (ensuring the confidentiality of mail and other items), but with the accumulation and processing of personal data of a person, including the same personal images and videos. The rule of law, which Russia respects, is obliged to develop and adopt legislative measures that do not allow anyone (government agencies, officials, private campaigns, any people) to use the electronic profile of a person without his consent. This area of development of legal doctrine seems very promising for the coming periods of the development of the information society.

Acknowledgments

This work was supported by grant 20-011-00355 from the Russian Foundation for Basic Research.

References

Acquisti A, Gross R (2006) Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. Proceedings of 6th Privacy Enhancing Technologies Symposium, Cambridge, UK, June 28-30, pp. 36-58

Alderman E, Kennedy C, The Right to Privacy, 1st edn. (NY: Vintage Books, 1997), 432 p.

Antonova NIn, Beljaeva SB, Paunova JA, The legal concept of robotics. Monograph, 1st edn. (Moscow: Prospect, 2019), 240 p.

Antopolsky AA (2019) Human rights and Internet: Case-Law of the European Court of Human Rights. The Proceedings of the Institute of State and Law of the RAS 14(2): 159-185. doi: 10.35427/2073-4522-2019-14-2-antopolsky.

Barbas S, Laws of Image: Privacy and Publicity in America, 1st edn. (Stanford: Stanford Law Books, 2015), 328 p.

Barinov SV (2016) Forensic Characteristic of Criminal Violations of Privacy Perpetrated on the Internet. The Actual Problems of Russian Law 9:137-141. doi: 10.17803/1994-1471.2016.70.9.137-141

Belyaeva KK (2019) Transferability of Image Rights in The Russian Federation and Abroad. The Bulletin of Civil Law 2:27-60

Bowie NE, Jamal K. (2006) Privacy Rights on the Internet: Self-Regulation or Government Regulation? The Business Ethics Quarterly 3:323-342. doi:10.5840/beq200616340

Boyd D (2008) Facebook's Privacy Trainwreck: Exposure, Invasion and Social Convergence. The Convergence. The International Journal of Research into New Media Technologies 1:13-20. doi:10.1177/1354856507084416

Chesney R, Citron D (2019) Deepfakes and the new disinformation war: The coming age ofpost-truth geopolitics. The Foreign Affairs 98:147. https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war. Accessed 12 Apr 2020

Civil Code of the Russian Federation (1994) (Part 1) of November 30, 1994 No. 51-FZ. Code of laws of the Russian Federation. 1994. No. 32. Art. 3301.

Conger K, Fausset R, Kovaleski SF (2019) San Francisco Bans Facial Recognition Technology. The New York Times. https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html. Accessed 2 Apr 2020

Culnan MJ (1993) «How Did They Get My Name»? An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. The MIS Quarterly 3:341-364. doi:10.2307/249775

Culnan MJ (2000) Protecting Privacy Online: Is Self-Regulation Working? The Journal of Public Policy and Marketing 19(1):20-26. doi:10.1509/jppm.19.1.20.16944

Dogan SL, Lemley MA (2006) What the Right of Publicity Can Learn from Trademark Law. The Stanford Law Review 58:1161 – 1220. doi:10.31235/osf.io/r8pvh

ECHR (1950) European Convention for the Protection of Human Rights and Fundamental Freedoms of November 4, 1950. https://www.echr.coe.int/Documents/Convention_ENG.pdf

Fridman VE (2019) Right for Image: Specifics of Legal Regulation, Ways of Protection. The IP. Copyright and Related Rights 8:45-56

Gavrilov EP (2015) Protection of the External Appearance and Protection of the Image of a Citizen. The Economy and Law 10:13-25

Gurley LK (2019) 40 Major Music Festivals Have Pledged Not to Use Facial Recognition Technology. VICE. https://www.vice.com/en_us/article/ywakpj/40-major-music-festivals-have-pledged-not-to-use-facial-recognition-technology. Accessed 2 Apr 2020

H.R.3230 (2019) Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019. https://www.congress.gov/bill/116th-congress/house-bill/3230. Accessed 5 Apr 2020

Howcroft E (2018) How faking videos became easy and why that's so scary. The Bloomberg, September 11. https://fortune.com/2018/09/11/deep-fakes-obama-video/. Accessed 3 Apr 2020

International Covenant on Civil and Political Rights (1966) Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966. https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx Accessed 3 Apr 2020

Jung AM (2011) Twittering Away the Right of Publicity: Personality Rights and Celebrity Impersonation on Social Networking Websites. The Chicago-Kent Law Review 86:381-417

Khodakovsky K (2020) The Clearview AI app for facial recognition is being tried for infringing on freedoms. The 3DNews. https://3dnews.ru/1002294. Accessed 7 Apr 2020

Kim MC (2004) Surveillance Technology, Privacy and Social Control: With Reference to the Case of the Electronic National Identification Card in South Korea. The International Sociology 2:193-213. doi: 10.1177/0268580904042900

Kobsa A, Schreck J (2003) Privacy through Pseudonymity in User-Adaptive Systems. The ACM Transactions on Internet Technology 3:149–183. doi:10.1145/767193.767196

Komkova GN (2015) Modification of Modern Constitution of Russia. The Izv. Saratov Univ. (N. S.), Ser. Economics. Management. Law 15:90-95

Kulikova SA (2012) Constitutional and Legal Aspects of the Content of the Concept of "Secret". The Leningrad Journal of Law 30:221-229.

Logeais E, Schroeder J-B (1998) The French Right of Image: An Ambiguous Concept Protecting the Human Persona. The Loyola of Los Angeles Entertainment Law Review 18:511-542

Lopatin VN (1999) Protection of the Right to Privacy. The Journal of Russian Law 1:85-97

Mamaev V (2018) Biometrics: From Premonition to Materialization. The Bank review 3:70 – 73.

Margulis ST (1977) Conceptions of Privacy: Current Status and Next Steps. The Journal of Social Issues 3: 5-21. doi:10.1111/j.1540-4560.1977.tb01879.x

Mazaev DV (2016) Citizen image protection on the Internet. The Bulletin of the Saratov State Law Academy 6: 103-112.

Mikryukov VA (2013) Subject-time Limits of Protection of the Image of the Citizen. The Lawyer 4:3-8

Nguyen Th, Nguyen C, Nguyen T, Duc T, Nahavandi S (2019) Deep Learning for Deepfakes Creation and Detection. Research Gate. https://www.researchgate.net/publication/336058980_Deep_Learning_for_Deepfakes_Creation_and_Detection. Accessed 2 Apr 2020

OHCHR (1948) The Universal Declaration of Human Rights. Adopted by the UN General Assembly on 10.12.1948. http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf

On Personal Data (2006). Federal Law of July 27, 2006 N 152-ФЗ. Code of Laws of the Russian Federation, July 31, 2006, N 31 (1 part), Art. 3451.

Rassolov IM, Chubukova SG, Mikurova IV (2019) Biometrics in the Context of Personal Data and Genetic Information: Legal Issues. Lex russica 1: 108-118. doi: 10.17803/1729-5920.2019.146.1.108-118. doi:10.17803/1729-5920.2019.146.1.108-118

Romanovskij GB, Right to Respect for Private Life, 1st edn. (Moscow: MZ-Press, 2001), 312 p.

Romashov PA (2019) Privacy Issues in the Digital Age. The Perm legal almanac. Annual scientific journal 1:103 - 118

Schneier B (2020) We're Banning Facial Recognition. We're Missing the Point. The New York Times. https://www.nytimes.com/2020/01/20/opinion/facial-recognition-ban-privacy.html. Accessed 2 Apr 2020

Shavaleev BE (2017) Enforcement of Administrative Prohibition against Visiting Official Sports Competition Sites on Days of Carrying out thereof. The Administrative law and process 7:80 - 82

Smith HJ, Dinev T, Xu H (2011) Information Privacy Research: An Interdisciplinary Review. The MIS Quarterly 35: 989-1015. doi: 10.2307/41409970

Solove DJ, Understanding Privacy 1stedn. (Harvard University Press Cambridge: MA, 2008), 272 p.

Stepanov AA (2012) Introduction of Intelligent Face Recognition Systems at the Objects of the Ministry of internal Affairs of Russia in the Omsk region. Prospects and problems of implementation. The Information Technologies, Communication and Protection of Information of the Ministry of internal Affairs of Russia 2:151 - 152

Supreme Court of the Russian Federation (2010) The Decree of the Plenum of the Supreme Court of the Russian Federation of June 15, 2010 No. 16 "On the Practice of the Application by the Courts of the Law of the Russian Federation "On Mass Media". Bulletin of the Supreme Court of the Russian Federation. 2010. No. 11

Synodinou T (2014) Image Right and Copyright Law in Europe: Divergences and Convergences. The Laws 3 (2):188 – 189. doi:10.3390/laws3020181

Tan D (2008) Beyond Trademark Law: What the Right of Publicity Can Learn from Cultural Studies. The Cardozo Arts & Entertainment Law Journal 25:913-994

UN (2014) Report of the Office of the United Nations High Commissioner for Human Rights "The right to privacy in the digital age" June 30, 2014 https://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc. Accessed 2 Apr 2020

Veliyeva DS (2014) Right for Respect of Private Life: International Realization and Protection Standards. Izv. Saratov Univ. (N. S.). Management. Law 14:443-448