ISSN 2713-2749

Legal Issues in the DIGITAL AGE

Вопросы права в цифровую эпоху

2/2020

Legal Issues in the **DIGITAL AGE**

Вопросы права в цифровую эпоху

2/2020

ISSUED QUARTERLY

Articles

Comment

News

Publisher
National Research
University Higher School
of Economics

Address:
3 Bolshoy Triohsviatitelsky Per., Moscow 109028, Russia
Tel.: +7 (495) 220-99-87
https://digitalawjournal.hse.ru/
e-mail: lawjournal@hse.ru

When the Invented Becomes the Inventor: Can, and Should AI Systems be Granted Inventorship Status for Patent Applications?

Lindsey Whitlow

Buswell Fellow, Assistant Director for Research, Center for Legal & Court Technology, William & Mary Law School, B.A., M.S., J.D. Address: William & Mary Law School, P.O. Box 8795, Williamsburg, VA 23187-8795, USA. E-mail: lawhitlow@wm.edu

Abstract

Artificial Intelligence ("AI") systems have become vastly more sophisticated since the term was first used in the 1950s. Through the advent of machine learning and artificial neural networks, computers utilizing AI technology have become so advanced that a team of attorneys in the United Kingdom claim that their AI machine, DABUS, actually created patentable inventions. The team went so far as to file patent applications with the European Patent Office, the UK Intellectual Property Office, and the US Patent and Trademark Office. All applications named DABUS as the inventor. This sparked a heated debate within academic and legal communities that centered around whether AI can be an inventor, and, if so, what this might mean for the current state of patent law. This paper discusses the purposes of patent law through a brief look at its history, in an effort to highlight why patent law as it stands may no longer be one- size-fits-all. It considers the evolution of AI systems to explain how one might determine that a machine could be "creative" and therefore justifiably named as inventor. It surveys popular opinions and organizes them on a spectrum ranging from those who believe that patent law should stay as it is and that AI cannot be an inventor, to those who, more dramatically, advocate for the abolition of patent protection for AI inventions. This paper suggests that legislators be proactive in traversing this technological minefield rather than reactive, as technology will continue to outpace, and trample, law if left to its own machinations.

Keywords

Artificial Intelligence; Patent Law; Creativity Machine; Emerging Technologies; Inventor; Artificial Inventor; Patent; USPTO; Copyright; Trademark.

Acknowledgements: The work was supported by a grant from Silicon valley Community Foundation, funded by Cisco Systems, Inc. The author is grateful to Professor Iria Guiffrida for her outgoing support and guidance. All errors are authors own.

For citation: Whitlow L. (2020) When the Invented Becomes the Inventor: Can, and Should AI Systems be Granted Inventorship Status for Patent Applications? // *Legal Issues in the Digital Age,* no 2, pp. 3–23.

DOI: 10.17323/2713-2749.2020.2.3.23

Introduction

In early August 2019, the Artificial Inventor Project, led by an international team of attorneys, filed patent applications for two inventions in both the US and the EU: one for a "fractal container" — the purpose of which is to "improve grip heat transfer in and out of the container" and enable one container to be connected to another — and the other a "neural flame" — a lighted device to be used for search-and-rescue missions[1]. These inventions seem innocuous enough, and likely to meet the novelty, utility, and non-obviousness requirements for patentability[2]. So what in these applications could possibly spark controversy among legal academics and practitioners, and have the business and tech worlds holding their breath? One small, seemingly insignificant detail: in the area where an applicant must list the inventor of the product or process for which the patent is sought, these attorneys listed DABUS[3], a "Creativity Machine," rather than a human inventor[4].

The patent system[5] is built to deal with "inventors" as human beings. Introducing the possibility that a non-human can "create" or author something has either not been contemplated, or sometimes completely refuted, by US law [Kop M., 2019][6]. Now, however, the United States Patent and Trademark Office (USPTO) recognizes the need to address this question. On August 27, 2019, the USPTO promulgated a request for comment in the Federal Register for several questions relating to Artificial Intelligence (AI) and the patent system[7]. Shortly thereafter, what began as a quest to determine how patent law must react to new uses of technology was then expanded to include all of intellectual property law, and the comment period was extended.

---

[1] Artificial Inventor Project, *Patent Application*. Available at: http://artificialinventor.com/patent-applications [hereinafter AIP *Patent Applications*] (accessed: 05.02.2020)

[2] See: 35 U.S.C. §§ 101–103 (2019).

[3] DABUS, or Device for the Autonomous Bootstrapping of Unified Sentience.

[4] AIP *Patent Applications*...

[5] For the purposes of this commentary, unless otherwise noted, "patent system" refers to the United States' patent application and granting process pursuant to 35 U.S.C. §§ 101–390 (2019).

[6] *See:, e.g.*, Naruto v. Slater, 888 F.3d 418, 420 (affirming the district court opinion that Naruto, a crested macaque, did not have standing to sue under the Copyright Act for infringement of a "selfie" taken by the primate with defendant's camera because he is an animal).

[7] Notice, US PTO, Request for Comments on Patenting Artificial Intelligence Inventions, 84 FR 44889. Aug. 2019.

There are arguments for and against awarding AI systems the title of "inventor". Within these arguments and opinions lie core policy questions that the USPTO must address, namely whether inventors can only be human. This commentary endeavors to provide a broad overview of some of the more common positions held by industry leaders and academics on the state of patent law in response to these filed applications. Many such policy opinions and positions rely heavily on the history and purpose of the patent system; the same facts and history construed differently depending on said position.

Part I of this paper charts brief histories of both the patent system and AI, and how we arrived at the current policy discussion. What follows in Part II is a rudimentary, and barbarously simplified, description of how AI systems, and in particular DABUS, work, and how they might share characteristics with a human "inventor". Part III then introduces industry opinions about the idea of inventorship. Part IV touches on how similar questions have been asked and answered before by describing how different countries have reacted to the use of AI in copyrighted, or copyrightable, works. This paper then concludes by suggesting that, rather than following the legal precedent of being reactionary, legislators should take strides now to push these important legal developments forward.

1. Histories Repeat

1.1. Patent Pending — a History

Patents, or the precursor of patents as we know them today, were first introduced in the 1400s [Chirambo C., 2019] and were initially distributed on an *ad hoc* basis[8]. The advent of the printing press in the mid-fifteenth century naturally spurred the need for protection of *literary* works, as dissemination became simpler — however, this event simultaneously created an open market for the imitation of inventions as published news became prominent and new inventions were shared on a wider, and more rapid, scale [Bugbee B., 1967: 17]. In response, inventors became savvier: Filippo Brunelleschi, Florentine architect and engineer,

[8] *See: History of Patent Law*. Available at: https://onlinellm.usc.edu/blog/history-of-patent-law/ (accessed: 13.12.2019)

> refuse[d] to make [his] machine available to the public, in order that the fruit of his genius and skill may not be reaped by another without his will and consent; …if he enjoyed some prerogative concerning this, he would open up what he [wa]s hiding, and disclose it to all [Bugbee B., 1967: 17–18].

This was the first "patent" that recognized an inventor's inherent right to his invention, "and the contractual nature, or *quid pro quo*, of patent protection". The preamble to this grant alone was an acknowledgment by the Florentine government of the benefit to the city of Florence, and society, of incentivizing — and thereby stimulating — creativity by its population, and in providing legal protection for the same.

Subsequent to the heavy decline in the granting of monopolies in Florence [Bugbee B., 19–20], Venice was the next to take up the patent mantle. Importantly, the Venetian Senate then passed what is the first-known general patent law, which embodied the basic tenets of Brunelleschi's patent [Bugbee B., 22]. It read:

> We have among us men of great genius, apt to invent and discover ingenious devices … Now, if provision were made for the works and devices discovered by such persons, so that others, who may see them could not build them and take the inventor's honor away, more men would then apply their genius, would discover, and would build devices of great utility and benefit to our commonwealth.

This law mirrors the underlying policy introduced by the Florentine government: we are inventors and discoverers, but if we are to put in effort to invent and discover, this work should be protected from theft, and inventors should be rewarded for innovation.

The Venetian system spilled over to other parts of the world throughout the following centuries [Bugbee B., 25–27, 35–43][9]. It even extended to colonial America, by way of England and its the Statute of Monopolies [Bugbee B., 36–38]; [Hovenkamp H., 2016: 263, 270][10]. An ad hoc monopoly-granting process continued in the United States until finally, upon the writing of the U.S. Constitution, there was a federal mandate of intellectual

[9] Discussing French, German, and Dutch patent practices based on Venetian patent principles and the English Statute of Monopolies).

[10] *Brief History of Patent Law of the United States*. Available at https://ladas.com/education-center/a-brief-history-of-the-patent-law-of-the-united-states-2/ (accessed: 07.05.2014). The Statute of Monopolies was a reaction to the commercial middle class opposing the grants of patent as royal showings of favor, which limited their ability to engage in mechanical and chemical inventiveness with exclusive rights to their innovations.

property protection directed to Congress: "Congress shall have Power … [t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries…"[11].

What we see throughout the history of inventive development is a consistent belief that human invention requires incentive, and that the way to incentivize is to offer exclusive rights in the manufacture and production of an entity's innovation. However, while the Patent Act frames inventorship and patentability in reference to human creation, there is no threshold of human control or input for the inventive process written into the law[12]. It seems fair to say that these same incentives to create, invent, or discover cannot exist for AI systems. But perhaps it goes further than that: with the need to incentivize human inventors of AI to push their ideas forward. To see how this detached layer of incentivizing human inventors affects the progress of AI development, we will need to similarly follow the advent and history of artificial intelligence.

1.2. They Walk Among Us — From Science Fiction to Science

AI is a complex field, and defining it proves difficult for most scholars and practitioners [Lea G., 2015]. Since AI can comprise innumerable technologies, and combinations of technologies, it is difficult to condense the concept into one singular definition [Marr B., 2018; Pring-Mill D., 2018]. For purposes of this discussion, it will helpful to start with the first recognized uses of the phrase "artificial intelligence".

Though the idea was bandied about for some time, the concept of "thinking machines" was formally introduced by Alan Turing in his paper *Computing Machinery and Intelligence*, which asked: "Can machines think?" [Turing A., 1950: 433]. The now-famous "Turing Test" was created as a way to address this quandary — if a machine can answer questions, fooling a human judge into thinking that it is human, then the program is said to be exhibiting intelligence [Hern A., 2014][13]. The first known use of the phrase "artificial in-

[11] US Constitution, Art. I, § 8, cl. 8.

[12] World Economic Forum. 4th Industrial Revolution. White Paper: Artificial Intelligence Collides with Patent Law. World Economic Forum Writing Organization: Center for the 4th Industrial Revolution. P. 9. Available at: http://www3.weforum.org/docs/WEF_48540_WP_End_of_Innovation_Protecting_Patent_Law.pdf. (accessed: 09.04.2018)

[13] See also: Exec. Office of the President National Science and Technology Council Comm. on Tech. Preparing for the Future of Artificial Intelligence 5 n.4 (2016).

telligence" came in 1956, when John McCarthy called to order the Dartmouth Summer Research Project on Artificial Intelligence, where researchers from disciplines as varied as language simulation and complexity theory were to gather and begin a discourse about what we now call the field of AI.

Following early successes with computer-based, complex problem solving, like IBM's Deep Thought chess-playing machine in the 1980s [Higgins C., 2017]. AI researchers began with an assumption: if an AI could solve a more advanced problem, then it should also be able to solve much simpler ones. This turned out not to be the case [Higgins C., 21][14]. The realization that the human skills that are the most difficult to reverse engineer are the unconscious ones [Rotenberg H., 2013: 108-109] contributed to a marked cooling off period in AI research. Researchers shifted focus from attempting to solve grand, societal problems to resolving narrow challenges for which there are clear measures of success [Dormehl L., 22].

One area to which this focus was applied was the advent of "expert systems". These involved AI systems operating as problem-solving tools alongside human counterparts. Reasoning was not enough to solve real-world problems; it had to be combined with knowledge in order for it be useful. If, for instance, programmers wanted a computer that would be useful in the field of neuroscience, the system would need to be deeply familiar with every facet of the field in the same way that a studied neuroscientist would be. Programmers and developers "suddenly had to become 'knowledge engineers,' capable of taking human experts in a variety of fields and distilling their knowledge into rules a computer could follow. The resulting programs were called 'expert systems'" [Dormehl L., 23–24].

Creating these systems seemed like a stroke of genius — until the process began hitting roadblocks. Counterintuitively, these expert systems would become *less* accurate as more rules were introduced: the more "knowledge rules" that were incorporated into the system, the more undesirable interactions between those rules would crop up. Essentially the rules, when interdependent, would cause the system to break if a contradictory rule was programmed. The process was complex, and cost prohibitive [Dormel L., 27].

But things changed again in 1996, when two students at Stanford University built a "smart web catalogue" [Dormehl L., 28] — a promising algo-

[14] Enter the Moravec Paradox — suddenly it seemed like it was "comparatively easy to make computers exhibit adult-level performance on intelligence tests or playing checkers, and difficult or impossible to give them the skills of a one-year-old when it comes to perception and mobility".

rithm that became the boost AI needed in the court of public opinion, and which contributed to the rapid growth of the field. Within a decade, Geoff Hinton introduced the concept of "deep learning [Dormehl L., 49]". Scientists moved away from programmable knowledge as seen in expert systems, and attempted to model the neural pathways of the human brain inside a computer by creating artificial neural networks [Dormehl L.,31]. In other words, these artificial neural networks are the computational approximation of the human brain [Hawkins J., 2004: 18–21][15]. Though neural networks had been the rejected sibling to traditional AI research, suddenly, this became the only way forward [Dormehl L., 29, 49].

1.3. Crossing the Streams

Here is where we arrive at the crux of our discussion: the point at which patent principles and AI overlap and/or intersect. As quoted above, the provision in the Constitution that gives Congress the power to promote science and the useful arts allows for securing to *authors* and *inventors* the exclusive right to their works[16]. It has long been understood that "authors" and "inventors" refer to humans. In early August 2019, a team from the UK University of Surrey decided to test the boundaries of the patent system: the team filed two patent applications in both the USPTO and the European Patent Office (EPO) claiming an AI system called DABUS as the inventor[17]. The filing tabled the question of how would patent offices react to the claim that the invented has become the inventor.

In response, on August 27, 2019, the USPTO sent out a call requesting comments for patenting AI inventions[18]. The request states that the USPTO "is interested in gathering information on patent-related issues regarding artificial intelligence inventions for purposes of evaluating whether further examination guidance is needed to promote the reliability and predictability of patenting artificial intelligence inventions[19]". The request asked questions like: "What are the different ways that a natural person can contribute

[15] How well neural networks can be mapped to mimic the structure of the brain is not necessarily agreed upon by all AI researchers.

[16] US Const. Art. I, § 8, cl. 8.

[17] AIP Patent Applications…

[18] Notice, USPTO, Request for Comments on Patenting Artificial Intelligence Inventions, 84 FR 44889 (Aug. 2019).

[19] Ibid.

to conception of an AI invention and be eligible to be a named inventor?" and "Do current patent laws and regulations regarding inventorship need to be revised to take into account inventions where an entity or entities other than a natural person contributed to the conception of an invention?"[20] Within two months, a second call was made that expanded the request to also include copyright and trademark[21].

2. How Might AI be Considered an Inventor?

While the USPTO asked several questions surrounding AI inventions in its request for comment, the application filing that sparked debate among legal practitioners and business entities centers around one particular question: whether an AI system can be considered an inventor for patent-filing purposes. The team that filed the application supports AI inventorship[22]. A cursory scan of some of the comments the USPTO received evidences that industry leaders oppose it[23]. The trouble with a blanket statement that AI can or cannot be granted inventorship is that there are several different types of AI, all with varying capabilities, all trained in different ways.

2.1. Machine Learning

Before AI can perform any great inventive or creative steps, it must be built, programmed, and trained. The first two steps of this process are wildly

[20] Ibid.

[21] Notice, USPTO, Request for Comments on Intellectual Property Protection for Artificial Intelligence Innovation, Federal Register no 58141 (Oct. 2019). The conversation about patentability for AI-created inventions started almost three decades prior to these requests for comment. As discussed above, AI has been slower to develop into the all-powerful, self-sufficient thinking machine early AI researchers predicted. Asking questions about patentability for AI inventions in the early 2000s may have been simply twenty years ahead of its time. *See, e.g.*, WIPO Worldwide Symposium on the Intellectual Property Aspects of Artificial Intelligence, (Mar. 1991); Vertinsky L., Todd R. *Thinking About Thinking Machines: Implications of Machine Inventors for Patent Law*, 8 Boston University Journal of Science & Technology Law, 2002, pp. 574, 586–87. ("To take a futuristic view, it may one day become necessary to obtain an assignment of invention rights from computer agents, and in the meantime, due diligence over what computer resources are being used, how, and who owns, controls, and has access to the results is warranted").

[22] See: generally: AIP Patent Applications...

[23] See, e.g., Letter from Thomas M. Coughlin, President, IEEE-USA, to Under Secretary of Commerce for Intellectual Property and Director of the US Patent and Trademark Office. Available at: https://ieeeusa.org/wp-content/uploads/2019/10/101619.pdf [hereinafter IEEE Letter] (accessed: 16.10.2019)

outside the scope of this commentary. However, it is relevant to discuss the training process for AI algorithms to better understand why one might make a policy argument in favor of an AI system being awarded inventor or author status. This training can be done through machine learning — "the ability for computers to learn without being programmed" [Wallace L., 2019]. Based on the documentation surrounding DABUS and the type of learning typically used in Creativity Machines, here we focus on two machine learning methods: supervised learning and unsupervised learning.

In supervised machine learning, the goal of training the algorithm is to uncover insights — *i.e.*, recognize patterns or categorize information — from data, by telling the system the desired output[24]. This process typically has three phases: training, validation, and testing. In the training phase, the algorithm is given "inputs" — data from which it can draw its conclusion — and is told the desired output from this set of data [Ashley K., 2017]. Because the algorithm has the input, and correct output, it can "learn" how variables assigned by the trainer relate to the target output; this helps the system to recognize patterns and make predictions based on the given input[25]. The goal is for the machine to be able to make these categorizations correctly with every piece of data, based on its prior "learning". Once a machine or algorithm has "learned" what it must do, in theory the AI can then take over on its own [Nielsen M., 2019].

Unlike supervised machine learning, when conducting unsupervised machine learning, the algorithm is not given a predetermined set of outcomes[26]. Because there is no desired output, the algorithm cannot classify the data inputs; rather, the goal of this type of training is instead to learn more about the data itself [Brownlee J., 2016]. The important difference between this type of machine learning and supervised learning is that, within the zetabytes of information available on the internet, there are an impossible number of unlabeled or incorrectly labeled data sets. In unsupervised learning, no labels are provided to the machine; it simply has input with no explanation [Dormehl L., 50]. This allows the machine to sift through the data for patterns that a human, given the same magnitude of data, could not possibly see.

[24] Supervised Machine Learning, Data Robot. Available at: https://www.datarobot.com/wiki/supervised-machine-learning/ (accessed: 18.12.2019)

[25] Supervised Machine Learning, Data Robot…

[26] See: Unsupervised Machine Learning, Data Robot...

Both of these types of machine learning lead to machines being able to make predictions based on vast amounts of input. As machine learning continually evolves and increases its prediction accuracy, machines become better able to perform tasks that would previously require human input [Agraval A.et al, 2018].

2.2. DABUS, or the "Device for the Autonomous Bootstrapping of Unified Sentience"

Law is reactive, and often slow to be so. As discussed, the idea of an AI invention then inventing things itself is not new, and neither is the discussion about how patent law will have to deal with it when it happens. While inventions have been deemed "creative" before August 2019, intellectual property law — at least in the United States[27] — has not changed with the growth of AI technology. The team that initiated the Artificial Inventor Project[28] seems to have done so to force the hands of patent offices to confront the question of whether AI can be considered an inventor.

According to the attorneys who filed the applications, DABUS is a "Creativity Machine" — "a particular type of connectionist artificial intelligence"[29]. Connectionist AI systems operate through the use of *artificial neural networks*, which are modeled after the way that neurons and synapses are thought to fire in the human brain, and are used to mimic the way humans learn [Dormehl L., 2019]. There are two neural network layers at play in Creativity Machines: the first network, and what this paper will call the "novelty network," is trained using general information from a variety of fields of knowledge, and is made up of a series of smaller neural networks[30]. It is tasked with generating novel ideas in response to disruptions, or "self-perturbations," in the way the smaller neural networks weigh and interpret statistical data from new inputs[31]. A second, overarching network monitors the novelty network for any ideas that are "sufficiently novel compared to the machine's pre-existing knowledge base"[32]. It responds by increasing or

[27] See: Part IV.

[28] Frequently Asked Questions, Artificial Inventor Project/ Available at: http://artificialinventor.com/frequently-asked-questions/ (accessed: 13.12.2019)

[29] AIP Patent Applications...

[30] AIP Patent Applications...

[31] Ibid.

[32] Ibid.

decreasing the perturbations to which the smaller neural networks react when interpreting data, in order to "form and ripen ideas having the most novelty, utility, or value"[33]. Through this "learning" process, one may start to see how by analogy, an AI system may be considered inventive.

The Artificial Inventor Project maintains that DABUS was trained only on general knowledge "in the field"; as its training was likely unsupervised, there would be no expected outcome from its machinations[34]. Its goal was simply to create something novel. From this training, DABUS came up with these inventions independently, and was able — on its own — to designate them as novel[35].

In some cases of invention by an AI system, a human may still be considered the inventor, perhaps because she exhibited inventiveness in creating a program to solve a specific problem, or carefully curated the information provided to the machine, or even identified the machine's output as novel and inventive[36]. The Artificial Inventor Project team argues, however, that no human may be considered the inventor of *these* inventions[37]. DABUS was not created to solve any particular problem, it was not given training data specifically relevant to its creations, and the machine itself identified that the inventions were novel within the scope of prior art of which it was "aware"[38].

These are all arguments made to support the idea that DABUS itself can and should be the only available option to list as the inventor of these innovations: it exhibited the inventiveness required of a human creator, and no human can claim to have had a hand in its processes. But convincing a patent office of these things is no small task. When so much needs to be proved just to show that an AI system is even capable of creative invention without human intervention, it seems like a monumental, and fruitless, effort for the Artificial Inventor Project team to push the need to list DABUS as the inventor of these products. However, the Manual of Patent Examining Procedure ("the Manual")[39], used by all patent examiners when determining

[33] Ibid.

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] Ibid.

[38] Ibid.

[39] See: generally MPEP (9th ed. Rev. 08.2017, Jan. 2018).

whether or not to approve a patent application, gives some insight as to why the team is driving these test cases forward.

First, patent law requires the naming of an actual inventor, or joint inventors, and the applied-for subject matter[40]. The Artificial Inventor Project asserts that DABUS is the inventor. DABUS's creator, Stephen Thaler, would not be allowed to list himself as inventor because he had no part in the conception of the products for which the group is seeking patent protection[41]. Patent seekers may not simply leave this area of the application blank, because, secondly, if an inventor is not listed, or is listed incorrectly and is not subsequently corrected, the Manual requires that "Office personnel should reject the claims under 35 U.S.C. 101 and 35 U.S.C. 115"[42]. If Thaler were to claim to be the inventor, but a patent office deems that not to be the case, any applications or claims may be rejected on that fact alone, leaving aside the discussion of whether AI can be a "creator". Because the patent system requires the disclosure of how an object is made or a process is completed in order to be patent-eligible[43], once the information is on record, it becomes public knowledge. The risk, particularly for businesses, is that naming the wrong inventor would result in no one receiving a patent [Crouch D., 2018], but with a chance that now the process is public information and the invention can no longer be monetized on the same scale.

Through this official interpretation of the patent-granting system, it makes sense that there are diverging opinions on how the USPTO should deal with AI as inventors.

3. The AI-Space Continuum

How industry leaders and legal practitioners have reacted to these claims seems to fall on a varied spectrum, though many of the ideas and opinions have areas of overlap. While not all responses to the USPTO's request for comment have been published as of this writing, several industry leaders and associations have weighed in, sharing their views of how the patent system should react to patents filed with an AI inventor moving forward.

[40] See: 35 U.S.C. § 115(a) (2019).

[41] AIP Patent Applications, supra note 1

[42] MPEP §§ 706.03(a), 2157 (9th ed. Rev. 08.2017, Jan. 2018).

[43] See: 35 U.S.C. § 112(a) (2019).

3.1. Legal Gymnastics and the "Law of the Horse"[44]

On one end of the spectrum are proponents for leaving the law in its current state. The Institute of Electrical and Electronics Engineers (IEEE)[45] and the American Intellectual Property Law Association (AIPLA) submitted comments to the USPTO for each of its inquiries[46]. When answering the question "Do current patent laws and regulations regarding inventorship need to be revised to take into account inventions where an entity or entities other than a natural person contributed to the conception of an invention?" AIPLA's position is a clear "no."[47] The letter states that the law requires an inventor to be a natural person, and though DABUS is currently a case testing this principle, it is unclear whether this AI system "is truly 'inventive AI.'"[48] Even if inventive AI does exist in the future, AIPLA says, that still does not dictate that AI should be granted automatically the title of inventor; rather, "it will be necessary to consider what types of activities by AI entities would be considered as inventive contributions to the claimed invention"[49].

Similarly, the Intellectual Property Owners Association (IPOA) emphasizes that "inventors" must be natural persons, and notes that "if non-natural entities were afforded inventor status, additional downstream issues would also need to

[44] *Easterbrok F.* (1996). "The best way to learn the law applicable to specialized endeavors is to study general rules. Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any effort to collect these strands into a course on 'The Law of the Horse' is doomed to be shallow and to miss unifying principles"). By way of analogy, proponents of prohibiting a machine from being named as an inventor may posit that we do not need a law specific to AI and inventorship; rather, the general rule requires a human to be inventor, and we shall find a human to name on the application, even if she does not meet the traditional "inventorship" standard.

[45] See: IEEE Letter… ("AI designers who created an AI's system's specifications, objectives, and input/output architectures, and who "trains" the AI system (or specifies that training) should be named the inventors of any inventive output of the AI system").

[46] See: Letter from Barbara A. Fiacco, President, American Intellectual Property Law Association, to Under Secretary of Commerce for Intellectual Property and Director of the US Patent and Trademark Office. Available at: https://www.aipla.org/docs/default-source/advocacy/documents/aiplacomments_uspto_rfc_patentingai2019nov08.pdf?sfvrsn=b1945306_0 [hereinafter AIPLA Letter] (accessed: 08.11.2019)

[47] Ibid. at 3–4.

[48] Ibid. at 4.

[49] Ibid. at 4. Later responses to USPTO questions seem to clarify AIPLA's position: the consequences of allowing AI to be named inventor would necessarily affect the measure against which one would determine a person having ordinary skill in the art ("PHOSITA") for the purposes of a patent validity analysis. Ibid. at 8.

be addressed"[50]. For instance, a common concern is that a machine cannot fulfill the requirement for an inventor to sign an affidavit affirming that she is the original inventor, and that she understands that a false statement to that effect has legal consequences[51]. In addition, IPOA cites the fact that it would impossible to depose a machine to determine its inventorship status[52].

Interestingly, however, when answering the question "Are there any other issues pertinent to patenting AI inventions that we should examine?" AIPLA recognizes that depending on the type of AI and the way it analyzes data and "learns" from it, the connection between human inventor and AI system may become more tenuous as AI systems become more "intelligent"[53]. We begin to see areas in which relying on the patent system in its current state may cause problems for future AI innovations.

3.2. Change is Inevitable, and the Sooner the Better

While industry associations seem to agree that changing the law to include AI in the definition of inventor is unnecessary and problematic, legal practitioners differ even amongst themselves as to the impact AI will have on the current patent regime in the United States. In an interview with legal practitioners, Law. com asked Kathi Vidal of Winston & Strawn and John Dragseth of Fish & Richardson, whether current laws and regulations regarding inventorship should be revised in light of the DABUS patents [Graham S., 2019]. Where Dragseth is unconcerned because society is not at a place where "an entity or entities other than a natural person [can] contribute to the conception of an AI invention", Vidal looks ahead: in short, "adding AI to the [already divided incentives for the current patent system in other industries] may stretch our 'one-size-fits-all' patent system to its breaking point". She continued by saying that "very rule needs to be rethought when it comes to AI and all the data the AI analyzed to come up with the invention…if we are going to reward AI inventions, we need to make sure the public receives the appropriate *quid pro quo*".

[50] Letter from Henry Hadad, President, Intellectual Property Owners Association, to Under Secretary of Commerce for Intellectual Property and Director of the US Patent and Trademark Office. Available at: https://ipo.org/wp-content/uploads/2019/11/IPO-Comments_Patenting-AI.pdf [hereinafter IPOA letter]. Accessed: 11.11.2019

[51] See: 35 U.S.C. § 115(b)(2) (2019); 37 C.F.R. § 1.63 (2020); MPEP 602.01(a) (9th ed. Rev. 08.2017, Jan. 2018).

[52] IPOA letter, 6.

[53] Ibid. 9.

One way in which scholars propose to reform the patent system is to increase the patentability threshold as it pertains to AI-created inventions. They suggest a recalibration of the definitions for an inventive step, prior art, and non-obviousness, and standardizing, or at least balancing, guidelines regarding who or what may be considered a "person having ordinary skill in the art". [Kop M., 16; Ramalho A., 2018]. For example, a person operating with an AI would likely embody a different definition of "ordinary skill" from someone doing the same research or production without the use of a machine. This would keep the current patent system in place generally, while changing the quintessential questions asked by examiners with regards to AI inventions.

Change to the patent system, it seems in this view, is necessary, whether or not that means a complete overhaul of the legal regime. There are questions and answers that cannot be addressed or even contemplated by the current state of the law. Technology evolves too quickly for whatever adaptations are made in how the current legal system approaches the awarding of patents. Proponents of these changes, however, do not necessarily advocate for excommunicating AI to another legal realm entirely. They merely push for stretching the metaphorical rubber band to capture that which is not currently suited for traditional notions of patent law protection.

3.3. And Now for Something Completely Different

A subset of the academic population believes that if these issues are not resolved satisfactorily *prior to* AI technology becoming fully capable of creative invention, this would then stifle the incentive for the investment in AI research and innovation. The proposed resolution for this group of scholars often involves a complete change to the patent system, or another regime for regulation entirely.

While it is widely agreed that an AI system would not need to be incentivized to invent in the same way the patent system rewards human inventors, the computer scientists, trainers, and machine learning experts behind these technological marvels may still require the incentive to even create the AI that can accomplish those tasks. Ryan Abbott, theoretical front man of the Artificial Inventor Project, asserts that lack of protection will lead to lack of innovation[54]. He states that if "outdated IP laws around the world don't respond

[54] AIP Patent Applications…

quickly to the rise of the inventive machine, the lack of incentive for AI developers could stand in the way of a new era of spectacular human endeavor"[55].

Other scholars take this view a step further, asserting that traditional patent law is outdated — but even if it were to take into account recent technological development, it cannot be applied to AI-inventions [Yanitsky-Ravid S., Xiaoqiong L., 2018: 2215–2231]. These academics go so far as to advocate for abolishing patent protection for AI inventions. They assert that traditional view that a human person must be identified as inventor for AI-generated inventions is an unrealistic threshold: "AI systems can produce a surprisingly large number of inventions, write and submit numerous patent applications, and even evaluate (or monitor) the risk of patent claims". AI systems can be programmed to fulfill necessary patent-eligibility requirements with regard to its inventions; if the law was not intended to cover human inventors alone, it is theoretically possible that AI systems could be entitled to patent rights in their creations.

The state of the technology may call for a completely new regime for protection, one outside of intellectual property law. Diametrically opposed to Judge Easterbrook's discussion of the law of the horse, perhaps the introduction of legislation and regulation specific to AI should come under the purview of an entirely new agency, rather than existing within current frameworks that need be stretched and manipulated to account for the unique effect AI has on just about every aspect of modern life. The logistics of creating such a new regime have not been contemplated in modern literature, likely because each agency touched by AI reacts to developments seemingly within their purview as they appear. A new system would require the development of an agency that would hardly be able to build from models that already exist, and it is possible that agencies would not let go of this type of regulation to another agency quietly.

3.4. International Approaches and Recent Decisions

Other jurisdictions are facing these same questions. Most jurisdictions represented in the IP5[56] specifically restrict inventorship rights to natural

[55] Ibid.

[56] About IP5 co-operation, five IPoffices. Available at: https://www.fiveipoffices.org/about (accessed: 17.01.2020). Members of the IP5 are EPO, Japan Patent Office (JPO), Korean Intellectual Property Office (KIPO), National Intellectual Property Administration of the People's Republic of China (CNIPA), and the USPTO. Ibid.

persons[57]. Europe, however, does not follow this pattern. Article 60(1) of the European Patent Convention (EPC) simply states that "the inventor or his successor in title is entitled to the right to a European Patent"[58]. "The EPC does not define the term 'inventor' or construe inventorship rights as being limited to only natural persons. Thus, Inventive AI may be recognized by the EPO as an inventor"[59].

Despite the wording, or lack thereof, surrounding inventorship in the European Union, the applications naming DABUS as inventor have been denied in both the EPO and the UK Intellectual Property Office (UKIPO; [Nurton, 2020]). The EPO has not fully explained its reasoning, but relying on Article 81 and Rule 19 of the EPC, stated that the applications "do not meet the requirement of the European Patent Convention (EPC) that an inventor designated in the application has to be a human being, not a machine"[60]. As stated above, this requirement is not clear in the wording of the EPC rules and articles applicable to inventorship; this interpretation of those rules may be the first of its kind.

The UKIPO, on the other hand, published a decision that called other facets of the patent application into question: it accepted that DABUS was the creator, but as a machine, it could not legally be considered the inventor [Nurton J., 2020: 112]. Further, the machine cannot have rights in the invention, and therefore could not possibly assign those rights to the designated "owner" of the invention listed in the application. The Hearing Officer also raised a question that will likely spark further debate in the future: "given that an AI machine cannot hold property rights, in what way can it be encouraged to disseminate information about an invention?"

4. Déjà Vu All Over Again

As with many other questions raised by the USPTO, there is a substantial likelihood that, though these applications have been rejected, they have succeeded in their purpose: to begin a conversation that will likely be hap-

[57] AIPLA Letter, at 10.

[58] Convention on the Grant of European Patents (European Patent Convention) Art. 60(1), Oct. 5, 1973, 1065 U.N.T.S. 199.

[59] AIPLA Letter, at 10.

[60] EPO refuses DABUS patent applications designating a machine inventor. Available at: https://www.epo.org/news-issues/news/2019/20191220.html. (accessed: 20.12.2019). The EPO press release also states that a reasoned decision is expected.

pening for years to come. Of course, this is not the first discussion regarding AI-created intellectual property, specifically within copyright law. The EU and the United States both hold that "there can be no copyright [in the case of purely AI Created works] because of *inter alia* the absence of a human author's own intellectual creation as an extension of his personality". This has been the assumption across all intellectual property forms in these jurisdictions.

Contrary to this, however, the United Kingdom implemented a computer-generated works (CGW) regime, which "stretches human authorship towards algorithmic authorship". The rights given to CGW are slightly different than typical copyright protection; for instance, no moral rights are awarded, and the protection term is shortened to 50 years[61]. This seems odd, considering the UK's decision to reject the Artificial Inventor Project's application. In theory, the same type of concerns would be brought forth in both IP regimes: if a machine can be considered an author, there is still a question of whether the machine can assign its ownership rights over to the copyright registration applicant.

It is curious that this concern was considered more of an issue in the patent context. Speculating, one could say there are two reasons for this divergence. First, it is possible that the decision with regards to the DABUS patent applications is an effort by the UKIPO to roll back some of its policies on computer-generated works. Second, the office may have found something so uniquely present in the patent system and inventiveness requirements that the analogy to copyright rulings cannot apply.

If either reason, this shift toward allowing certain of CGW or AI-Generated Works to be attributed to the AI itself in copyright law still has the potential to carry over to the patent side of intellectual property. Because the requirements for invention are more strenuous than the requirements for works of authorship, the speed of AI development can only tell how these offices will approach these questions moving forward.

Conclusion

The law is reactive. As it stands, there is heated debate as to whether AI is in a place to purely be creative or inventive — but regardless, the time seems

[61] Japan follows a similar strategy, with a commercial component: "only AI Generated Works that have a significant economic impact, will be granted protection".

to be coming. The Artificial Inventor Project's goal in submitting applications naming an AI as inventor appears to be an attempt to begin the conversation surrounding these systems, and how the law can and should react to these innovations *before* they exist, knowing this technology is coming.

The dominant view is that, for now, the law should remain as it is. However, regarding the speed with which AI develops, legislators and regulators heeding this advice may be faced sooner than they think with AI that can do what DABUS is purported to have done, with more alacrity and even less human intervention. It may be time for legislation and regulation to attempt to work ahead of technological innovations to continue to provide incentives for the development of these AI systems.

References

Agrawal A., Gans J., Goldfarb A. (2018) *Prediction Machines: The Simple Economics of Artificial Intelligence.* Cambridge (Mass.): Harvard Business Review Press, 272 p.

Ashley K. (2017) *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age.* Cambridge (UK): University Press, 446 p.

Brief History of Patent Law of the United States (2014) Available at: https://ladas.com/education-center/a-brief-history-of-the-patent-law-of-the-united-states-2/ (accessed: 15.08.2020)

Brownlee J. (2016) Supervised and Unsupervised Machine Learning Algorithms. Available at: https://machinelearningmastery.com/supervised-and-unsupervised-machine-learning-algorithms/ (accessed: 15.08.2020)

Bugbee B. (1967) *Genesis of American Patent and Copyright Law.* Washington: Public Affairs Press, 208 p.

Chirambo C. (2019) Introduction to the Patent System: Challenges Facing Small Offices. Available at: https://www.wipo.int/edocs/mdocs/pct/en/wipo_pct_gbe_19/wipo_pct_gbe_19_topic_1b.pd (accessed: 15.08.2020)

Crouch D. (2018) When Co-Inventors Fail to Cooperate — Nobody Gets a Patent. Patently-O. Available at: https://patentlyo.com/patent/2018/05/inventors-cooperate-nobody.html (accessed: 15.08.2020)

Dormehl L. (2017) *Thinking Machines.* New York: Tarcher Perigee, 288 p.

Dormehl L. (2019) What is an artificial neural network? Here's everything you need to know. Available at: https://www.digitaltrends.com/cool-tech/what-is-an-artificial-neural-network/ (accessed: 15.08.2020)

Easterbrook F. (1996) Cyberspace and the Law of the Horse. *University of Chicago Legal Forum*, no 4, p. 207.

Graham S. (2019) Can AIs Hold Patents? Experts Answer USPTO's Questions about Artificial Intelligence. Available at: https://www.law.com/therecorder/2019/08/29/can-ais-hold-patents-experts-answer-usptos-questions-about-artificial-intelligence/ (accessed: 15.08.2020)

Hawkins J., Blakeslee S. (2004) *On Intelligence: How a New Understanding of the Brain Will Lead to the Creation of Truly Intelligent Machines.* New York: Holt, 272 p.

Hern A. (2014) What is the Turing test? And are we all doomed now? Available at: https://www.theguardian.com/technology/2014/jun/09/what-is-the-alan-turing-test (accessed: 15.08.2020)

Higgins C. (2017) A Brief History of Deep Blue, IBM's Chess Computer. Available at: https://www.mentalfloss.com/article/503178/brief-history-deep-blue-ibms-chess-computer (accessed: 15.08.2020)

Hovenkamp H. (2016) The Emergence of Classical American Patent Law. *Arizona Law Review*, vol. 58, p. 270.

Kop M. (2019) AI & Intellectual Property: Towards an Articulated Public Domain. Unpublished manuscript. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3409715# (accessed: 15.08.2020)

Lea G. (2015) The Struggle To Define What Artificial Intelligence Actually Means. Available at: https://www.popsci.com/why-we-need-legal-definition-artificial-intelligence (accessed: 12.08.2020)

Marr B. (2018) The Key Definitions of Artificial Intelligence (AI) That Explain Its Importance. Available at: https://www.forbes.com/sites/bernardmarr/2018/02/14/the-key-definitions-of-artificial-intelligence-ai-that-explain-its-importance/#1a0646664f5d (accessed: 15.08.2020)

Nielsen M. (2019) Neural Networks and Deep Learning. Determination Press. Available at: http://neuralnetworksanddeeplearning.com (accessed: 15.08.2020)

Nurton J. (2020) EPO and UKIPO Refuse AI-Invented Patent Applications. Available at: https://www.ipwatchdog.com/2020/01/07/epo-ukipo-refuse-ai-invented-patent-applications/id=117648/ (accessed: 15.08.2020)

Pring-Mill D. (2018) Everyone Is Talking About AI — But Do They Mean the Same Thing? Available at: https://singularityhub.com/2018/03/15/everyone-is-talking-about-ai-but-do-they-mean-the-same-thing/ (accessed: 15.08.2020).

Ramalho A. (2018) Patentability of AI-generated Inventions: Is a Reform of the Patent System Needed? *Institute of Intellectual Property Journal*, no 2, pp. 25–26.

Rotenberg V. (2013) Moravec's Paradox: Consideration in the Context of Two Brain Hemisphere Functions. *Activitas Nervosa Superior*, vol. 55, pp. 108–109.

Turing A. (1950) Computing Machinery and Intelligence. *Mind*, vol. 59, pp. 433–460.

Vertinsky L., Rice T. (2002) Thinking About Thinking Machines: Implications of Machine Inventors for Patent Law. *Boston University Journal of Science and Technology Law*, no 8, pp. 586–587.

Wallace L. (2018) What You Need To Know About AI. Available at: https://www.forbes.com/sites/forbestechcouncil/2018/01/08/what-you-need-to-know-about-ai/#6a73019253c7 (accessed: 15.08.2020)

Yanisky-Ravid S., Liu X. (2018) When Artificial Intelligence Systems Produce Inventions: The 3A Era and an Alternative Model for Patent Law. *Cardozo Law Review*, vol. 39, pp. 2215–2231.

The Inadequacy of Current Remedies for Violation of Data Subjects' Rights and How to Fix it

Alexander Savelyev

Associate Professor, International Laboratory on Intellectual Property and Information Technology Law, National Research University Higher School of Economics, Candidate of Juridical Sciences; senior attorney, IBM East Europe/Asia Ltd. Address: 20 Myasnitsky Str., Moscow 101000, Russia. E-mail: alexandersavelyev83@gmail.com

Abstract

The paper focuses on civil law remedies for violations of data subjects' rights: claims for damages and claims for compensation of moral harm. Based on an analysis of academic literature, as well as of Russian and international case law, it is argued that, although these remedies are endorsed by the GDPR and other laws, they are inadequate and do not conform to the requirements for an "effective remedy" stipulated by major international legal documents on human rights. The main reasons are: 1) difficulties in proving the fact and the amount of a legally recognized category of damage because the typical consequences of data privacy violations (e.g. the chilling effect caused by dataveillance, negative emotional reactions, etc.) are not considered legally significant by the courts; 2) inability to prove with a substantial degree of certainty a causal link between the violation and the damage incurred because such damage occurs remotely and within complex flows of data. This produces an imbalance in the enforcement of data protection laws so that public law remedies such as administrative fines predominate. This approach is not compatible with the goals of empowering the individual and ensuring control over usage of one's data because there cannot be effective control without an effective remedy to enforce it. In practice this leads to under enforcement of data protection laws because under-resourced data protection authorities cannot address most of the violations that pertain to data protection. A new type of remedy that would resemble the statutory damages applicable to copyright infringement in some jurisdictions should be introduced. Its punitive and decentralized nature would become an additional incentive for data controllers to invest in compliance with data protection laws. From a long-term perspective, it may facilitate including individuals in management of their personal data, without which it would be impossible to effectively address the risks brought about by massive and ubiquitous data processing and algorithmic decision-making.

Keywords

privacy, data protection, compensation, moral harm, effective remedy, statutory damages.

Acknowledgements: This paper was prepared as part of the Basic Research Program at the National Research University Higher School of Economics (HSE) and supported by a subsidy from the "5–100" Russian Academic Excellence Project.

For citation: Savelyev A.I. (2020) The Inadequacy of Current Remedies for Violation of Data Subjects Rights and How to Fix it // *Legal Issues in the Digital Age,* no 2, pp. 24–62.

DOI: 10.17323/2713-2749.2020.2.24.62

Introduction

It is a well-known axiom that a right without remedy is not a right at all. Therefore, any right should be accompanied by a remedy for its breach, and that remedy should be effective — especially so if a fundamental right of a person is at stake[1]. The right to protection of personal data is treated as a fundamental right in the EU[2]. In the Russian Federation, the right to protection of personal data is considered a part of the constitutionally guaranteed right to respect for private and family life[3]. A right of this kind should definitely have adequate remedies for its breach.

Existing international documents impose certain obligations on governments to provide such remedies for breaches of fundamental rights. According to the United Nations, "as part of their duty to protect against business-related human rights abuse, States must take appropriate steps to ensure, through judicial, administrative, legislative or other appropriate means, that when such abuses occur within their territory and/or jurisdiction those affected have access to effective remedy." The obligation of states to ensure that any legislative provisions incorporating or implementing fundamental rights are in fact effective is stipulated in other international documents, e.g. in Article 2 of the International Covenant on Civil and Political Rights[4] and Article 13 of the European Convention on Human Rights[5]. EU documents also contain

[1] See Art. 25 of the UN Guiding Principles on Business and Human Rights. New York, 2011, p. 27. Available at: https://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_eN.pdf (accessed: 01.08.2020)

[2] Art. 8 of the EU Charter of Fundamental Rights.

[3] Art. 23 and 24 of the Constitution of the Russian Federation; Art. 2 of Federal Law on 27 July 2006 No. 152-FZ "On personal data".

[4] "Each State Party to the present Covenant undertakes: (a) To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity; (b) To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy; (c) To ensure that the competent authorities shall enforce such remedies when granted."

[5] "Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

similar provisions in Article 47 of the Charter of Fundamental Rights of the European Union[6] and Article 19 of the Treaty on European Union[7]. The European Court of Human Rights (ECHR) has interpreted effectiveness to mean that the remedy must be capable of providing redress in respect of the applicant's complaints and that it offers reasonable prospects of success within a reasonable timeframe[8].

Calling for effective remedies for violation of data subjects' rights is not only supported by academic studies but also has definite foundations in the prevailing framework of international law.

Violation of a data subject's rights may incur different types of liability for a data controller. Some of these liabilities fall within public law and have a purely punitive purpose, e.g. administrative and criminal liability. Others like reimbursement of damages or compensation for moral harm are "horizontal" in nature and have a compensatory purpose.

Public law remedies and a punitive tendency in the enforcement of data protection laws are prominent in both Russian and foreign case law. Administrative fines are the main kind of sanctions imposed on data controllers that are liable for breach of personal data regulations and in particular of data subjects' rights[9]. Data subjects may sometimes benefit from administrative fines or the threat to apply them, e.g. through access to their personal data or its deletion; but they do not receive monetary compensation themselves under a system of administrative fines. Administrative fines imposed on a data controller by a court or a data protection authority (DPA) in response to a violation of data subjects' rights are paid to the government rather than to the individual concerned.

However, a breach of data subjects' rights may result in material or non-material damage to natural persons, such as loss of control over their personal

[6] "Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article."

[7] "Member States shall provide remedies sufficient to ensure effective legal protection in the fields covered by Union law."

[8] *Vuckovic and Others* v *Serbia*, ECHR 25 Mar 2014. References: 17153/11 – Legal Summary, 2014, ECHR 387.

[9] This is evident from the preponderance of news reports on enforcement of data protection that describe cases in which an administrative fine was imposed on a data controller by a data protection authority; also, all the discussions about the effectiveness of sanctions on violation of data protection regulations are reduced mostly to debating what the amount of fines should be and whether they are high enough to induce data controllers to comply with the law. There appear to be no reports of high-profile cases in which data subjects received compensation for damages in amounts as large as the administrative fines imposed on data controllers

data or limitation of their rights, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality for personal data protected by professional secrecy, or other significant economic or social disadvantages to the natural person concerned, as is explicitly recognized in §85 of the Recitals to the GDPR.

Discrimination is one of the most common negative consequences of unlawful processing and one of the main risks in applying algorithmic governance throughout a society. For example, if an employer refuses to shortlist a candidate for interview on the basis of an internet search of posted images that reveal a candidate's ethnicity, it may constitute discrimination based on ethnic origin. However, if an employer refuses to interview based on the candidate's posts in a certain group in Facebook, this would also constitute a form of discrimination that may not be clearly prohibited from a legal perspective but is more frequent in circumstances that now prevail. The loss of a job opportunity in either situation can have a great impact on an individual.

Incorrect profiles based on false, irrelevant or sensitive data may also lead to serious negative consequences for individuals, such as inability to qualify for loans from financial institutions. For example, one data broker (ChoicePoint) incorrectly reported a criminal charge of "intent to sell and manufacture methamphetamines" in the file of a specific person. It resulted in immediate rejection of her job applications. She could not even obtain credit to buy a dishwasher. Once notified of the error, ChoicePoint corrected it, and some other companies to whom ChoicePoint had sold her file corrected their reports promptly; but the individual had to request a correction repeatedly from many others and ended up suing one [Q. Mui Y., 2011][10]. Given the access of multiple data controllers to certain kinds of personal data, this may become a typical scenario rather than an exceptional one.

Identity theft also poses a substantial risk. The few statistics available on identity theft in the EU suggest that almost 2% of the EU population (8,2 million individuals) have been affected by identity theft resulting in an average individual loss of €2,500 s or €20 billion at the EU level. The loss to businesses is estimated to be as high as 0,4% of EU GDP[11]. However, the true magnitude of identity theft remains difficult to quantify inasmuch as there is

[10] Available at: http://www.washingtonpost.com/business/economy/little-known-firms-tracking-data-used-in-credit-scores/2011/05/24/gIQAXHcWII_print.html. (accessed: 01.08.2020)

[11] CSES. Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft: Final Report, 11 December 2012.

no commonly accepted definition for identity theft, it is not often reported to police, and victims are in many cases unaware that they have been targets of identity fraud.

If we acknowledge that personal data breach is a violation of a fundamental right of individuals, then we should agree that the losses which individuals sustain from these data incidents should be properly compensated to them. This idea is reflected in much current legislation. According to Article 79(1) of the GDPR, "each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation". Paragraph 146 of the Recitals to the GDPR reinforces the point:

> The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation…. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Data subjects should receive full and effective compensation for the damage they have suffered.

Article 78 in Chapter VIII of the GDPR emphasizes the point that an effective legal remedy is not automatically present whenever remedies are available under national law. For example, the option to lodge a complaint with a supervisory authority according to Article 77 of the GDPR is explicitly mentioned as not constituting an effective judicial remedy inasmuch as supervisory authorities are not considered courts but administrative bodies (albeit vested with special independence) [Kuner C., Bygrave L., 2020: 1135]. In *Schrems* v *Data Protection Commissioner*, the European Court of Justice found that the complete absence of "any possibility for an individual to pursue legal remedies…does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter"[12]. The GDPR explicitly states that exclusively administrative remedies are insufficient to meet the threshold for an effective remedy.

At the time of writing there are no reports of high-profile cases resulting in compensation to an individual for damages caused by processing of their

[12] *Schrems* v *Data Protection Commissioner*, ECJ, C-*362*/14, 06 October 2015, § 95.

data in violation of GDPR provisions[13]. By contrast, there are a great many instances in which data protection officers levied administrative fines on data controllers[14].

Unlike the GDPR, Article 1(2) of the Russian law on personal data[15] explicitly recognizes two types of private law remedies available to data subjects: the right to claim damages and the right to claim compensation for moral harm. In theory, these types of remedies are intended to address different types of losses. A loss suffered by the data subject may be either economic or non-economic in nature. The type of loss incurred determines the type of remedy to be applied: damages claimed on grounds of an economic loss; and compensation for moral harm claimed on grounds of a non-economic loss. An economic loss is incurred if the interests harmed have a market value which can be assessed according to the economic rules prevailing in that market. Damage which is not economic in nature (such as mental suffering) can only be given a monetary equivalent through the judicial decision to compensate for moral harm. In practice, however, the first remedy (a claim for damages) is not used, while the second one (compensation for moral harm) is not effective enough and does not have much impact in protecting data subjects' rights.

---

[13] There were some cases of the kind when Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data was in force. But they were few in number and attracted very little attention compared to the enforcement of data processing agreements and associated fines for their violation.

[14] Among the most recent reports are an ICO Statement "Intention to fine Marriott International, Inc. more than £99 million under GDPR for data breach", 9 July 2019. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/?fbclid=IwAR1TkwUg_CLdroHQTDVLOmmezfcfTRFiPo-jvPJBgRATT2ANwSkCRVrRP9A) (accessed: 01.08.2020); and "British Airways faces record £183m fine for data breach" reported by BBC News, 8 July 2019 (available at: https://www.bbc.com/news/business-48905907?fbclid=IwAR3ILh0ntXc6usYUgaqWJN4pv3L1BFr5VfSN6eps_SE8tLIyKwn9rzQluyQ (accessed: 01.08.2020); "The Romanian National Supervisory Authority for Personal Data Processing imposes the first fine under GDPR on Unicredit Bank in the amount of 130 000 Euro", 27 June 2019 (available at: https://www.dataprotection.ro/index.jsp?page=Comunicat_Amenda_Unicredit&lang=en&fbclid=IwAR2yvwm5eqWp1Ek2MlrM8XIZPia0AGWhvh9TN7Qoh9DK3H5RTWe3mnru-NE (accessed: 01.08.2020); and also "French DPO (CNIL) imposes fine in the amount of 20 000 Euro on UNIONTRAD", 18 June 2019 (available at: https://www.cnil.fr/fr/uniontrad-company-20-000-euros-damende-pour-videosurveillance-excessive-des-salaries?fbclid=IwAR0I_4gtBwwJ9ZZ_Avm8NLfB3r_cWpXwPST4oB6jXu2bTrEqfx39LJj-WKLQ (accessed: 01.08.2020).

[15] Federal Law "On personal data" No. 152–FZ of 27 June 2006 (with subsequent revisions and amendments). This law is based on international and EU data protection law and was adopted as a part of the implementation measures of Council of Europe Convention No. 108, which has been ratified by Russia.

This paper argues that the problem with ensuring effective remedy arises not only from certain distinctive features in the Russian legal system and its case law, but also from the incompatibility of these remedies with particular aspects of data protection. That incompatibility renders them inadequate for effective protection of data subjects' rights. The best way to flesh out this argument is to proceed with a description of general rules applicable to these remedies followed by an account of public law liabilities for violating a data subject's rights. In the following sections Russian law on these matters is described in detail and also compared to EU and international law.

1. Overview of private law remedies available to data subjects

1.1. Damage claims for breaches of data subjects' rights

A claim for damages is one of the most common "horizontal" remedies available for breach of one's civil rights. A damage claim addressed by a data subject against a data controller is contestable. By default, such a claim will refer to a tort because the obligations of a data controller are established directly by law and do not require any agreement concluded with the data subject.

However, it may be argued that a claim for damages may in certain limited circumstances be contractual in nature because specific obligations of the data controller concerning processing personal data have been explicitly stated as a part of the contractual terms that were accepted by the data subject. For example, it may be the case that a data subject has expressed consent by means of a clickwrap agreement (e.g. to the terms of use or privacy policy presented in an online interface) that covers processing of personal data in the course of providing services. The fact that these terms constitute a part of the online contract, which the data subject accepts in a way similar to accepting the other terms of the contract, supports the argument that breach of these contractual provisions concerning personal data processing should be treated the same as a breach of the other provisions of the contract.

In the event that there are no contractual relations between the data controller and the data subject such that the conditions applicable to processing personal data are stated as a distinct set of terms consented to by the data subject, any claim for damages will definitely be based upon a tort.

Regardless of the nature of the damage claim raised by the data subject (a topic which deserves more extensive study), there are no substantial differences in the burden of proof placed on the data subject. In either case that burden is very difficult to manage.

None of these claims (whether contractual and non-contractual) are mutually exclusive. Data subjects may choose the basis of their claims at their own discretion.

Regardless of the nature of the relations forming the basis for the claim, the burden of proof imposed on data subject will consist of the following items:

fact of violation of the data subject's right which has been granted by the law;

amount of loss incurred;

causal link between the violation and the amount of loss claimed.

The data controller's fault is not a part of the burden of proof because contract law presumes that the data controller acting as a commercial entity is at fault whenever a data subject makes a claim a data controller. However, a determination of fault may have an impact on success of the claim, and that will also be covered in the discussion that follows. Let us take a closer look at those elements in the burden of proof and outline the main difficulties facing data subjects in pursuing their claims.

1.1.1. The fact of violation of the data subject's right which has been granted by the law

Violation of a data subject's right should be proved by presenting evidence that the data controller failed to comply with specific provisions of the data protection regulations as they pertain to the data subject. The most typical types of violations of a data subject's rights are:

unlawful transfer of personal data from data controllers (employers, public authorities, mobile operators, credit institutions, etc.) to third parties;

improper and excessive collection and storage of personal data by public authorities, or by commercial entities (telecom operators, supermarket chains, banks, etc.) without legitimate purpose, proportionality and sufficient guarantees of security;

storage of inaccurate information;

manipulation of inaccurate personal data stored and processed legally, including by means of algorithmic decision-making;

publication of personal data in the media or on the internet;

denial of access to personal data held by the data controller or insufficient responses to requests for access to personal data;

refusals to correct, delete and block information in personal data files or insufficient responses to requests for corrections, deletion and blocking of information in personal data files[16].

In some cases when these violations are encountered in the course of interacting with a data controller, it is not very difficult to prove the fact, e.g. when there is denial of access to information about personal data processed or failure to delete personal data upon request. A copy of the communications between the data subject and data controller may suffice for the purpose. Certain other violations, such as data leakage, may sometimes be established by referring to information which appears in mass media. Other violations, such as unlawful disclosure of personal data to a third party, may become apparent during contact with other persons when they refer to information that was disclosed only to the data controller (direct marketing, etc.), although inferences of this kind can also be very difficult to validate.

Of course, not all of the many violations of data protection laws committed daily by data controllers will be visible to data subjects. Those violations may be come to light only after a detailed audit of a particular data controller by a data processing authority (DPA) or as a result of whistleblowing. But the mere fact that there are some violations which cannot be discovered by the data subject does not mean that there is no need to have legal instruments empowering them in other situations. As has aptly been said, "Nobody made a greater mistake than he who did nothing because he could do only little"[17].

1.1.2. Amount of loss incurred

The second element that the plaintiff has to prove in order to succeed with a damage claim is the fact of losses and their amount. Financial loss is rarely encountered in data privacy violations[18]. It typically comes up in identity theft cases that involve unauthorized money transfers or lost opportunities to qualify for a loan. In these exceptional cases proving the

[16] For a more extensive listing of kinds of violations, see, e.g.: Access to data protection remedies in EU Member States published by the EU Agency for Fundamental Rights (FRA), p. 26.

[17] This is usually attributed to Edmund Burke.

[18] According to the EU FRA, few complainants in most of the sixteen EU member states have suffered financial losses as a result of data protection violations. EU FRA, Access to data protection remedies, p. 28.

amount of damages should not be much of a problem. But it will be difficult in most other cases for an individual to calculate the amount of damages caused by violation of their rights as a data subject because of the intangible and non-pecuniary nature of the harm. In most cases those calculations will be speculative and fall short of being persuasive in court.

Recent amendments to the Civil Code of the Russian Federation have established a more liberal approach since 2014 to proving the amount of damages claimed. Those amendments have made proof to a reasonable degree of trustworthiness allowable (Article 393 (5). In contrast to earlier case law, the courts cannot now dismiss a damage claim in its entirety on the sole grounds that its amount was not proven with sufficient precision by the plaintiff. This view is now a feature of Russian case law. According to the Supreme Court of the Russian Federation, failure to prove the exact amount of damages incurred does not relieve the party that committed a breach from liability. In such cases the court should determine the amount of damages for which compensation is due[19]. These clarifications and legislative developments have made things easier for plaintiffs, but they do not release them from the requirement to provide objective evidence for financial loss in general.

For damage claims based on contractual relations between a data controller and a data subject, specific contractual provisions relating to exemptions and limitation of the data controller's liability may apply. While those provisions may be enforceable generally based on the principle of freedom of contract, some of them may be invalidated as unfair contract terms in accordance with applicable legislation[20], or they may be rendered void on grounds of violating mandatory provisions of the data protection regulations. Resorting to those avenues for claiming damages imposes an additional burden on data subjects because of the effort and expense involved in suits of that kind.

1.1.3. Causal link

Finally, the data subject has to prove that there is sufficient causal linkage between the data controller's act and the loss suffered. In most cases

[19] Section 9 of the Review of Case Law of the Supreme Court of the Russian Federation, No. 2, 2016.

[20] See, e.g.: Unfair Contract Terms Directive 1993; Art. 428 of the Civil Code of the Russian Federation.

this is almost impossible to prove due to the extremely complex nature of information flows. As noted authority on privacy issues Daniel Solove puts it: "There are too many entities collecting and using personal data to make it feasible for people to manage their privacy separately with each entity. Moreover, many privacy harms are the result of an aggregation of pieces of data over a period of time by different entities." [Solove D. 2013: 1881]. The remote nature of the link between data protection violations and harms incurred is recognized by other legal scholars as well [Lynskey O., 2015: 209]. A speaker at an OECD roundtable used the metaphor of a blank cheque to describe the situation and argued that, when someone reveals private data to others, they are signing a blank cheque that "may never come back to her, or may come back to him, or may come back for an indeterminably small or large price to pay. That price could be mild embarrassment, an annoying spam, or a devastating case of identity theft." [Acquisti A., 2010: 26]. The Electronic Privacy Information Center (EPIC) argues that "opaque industry practices result in consumers remaining largely unaware of the monitoring of their online behavior"[21].

Hence, it is not possible for a data subject with limited knowledge and limited understanding of personal data flows to single out a clearly defined cause and effect relation from an entire chain of information flows and determine the potential seriousness of the harm. There are too many factors affecting the overall harmful result, and therefore it is not possible to isolate a particular unlawful act of the data controller from the overall picture and then show a causal link as a "mechanistic" pattern.

Disputes arising from information processing are substantially different from conventional commercial disputes where it is far easier to show a causal link (e.g. a vendor fails to deliver goods and that results in penalties imposed on the buyer by his counterparty for failure to deliver a product in which the missing goods were an important element). For information flows the damage is too remote and consequently may not be legally relevant in terms of liability. For example, a data controller may find it useful to create a centralized database containing various types of personal data, but the database may have a single point of vulnerability to large-scale identity theft. Individual data subjects could object to keeping certain kinds of information in the database on the grounds of that the data minimization prin-

[21] EPIC, Search Engine Privacy. Available at: https://epic.org/privacy/search-engine/ (accessed: 14.07.2020)

ciple requires that only relevant and necessary personal data be retained (although the data controller could counter that objection by claiming that keeping the data results in greater efficiency and is of legitimate interest). Consider the following scenario: certain pieces of personal data, which were not strictly necessary for the data controller's operations but were included in the database, might subsequently fall into the hands of a third party who in turn processes it further and forwards the results to another person; that person might have their data hacked and then used for fraudulent transactions. It would be impossible to the individual to link the fraud to the initial breach of the data minimization principle by the initial data controller.

The difficulty data subjects face in proving causation is acknowledged by legal specialists. For example, in her analysis of the GDPR, Emmanuela Truli argues that "the person who has suffered damage may not easily have had access to information proving that e.g. he did not get a job offer or credit due to the incorrect information collected, stored or disseminated by the controller, or the damage may not have been immediate." [Truli E. et al, 2017: 312]. Other academic specialists in law and technology observer observe that "because of information asymmetries, data subjects are often unaware (or at least less conscious than data controllers and other entities) about the nature, extent and use of collected data." [Lazaro C., Le Métayer D., 2015: 10]. To sum up, it is arguable that the causal link is the most difficult part of the burden of proof imposed on data subjects in pursing their claims for damages.

1.1.4. Fault of the data controller

There is a presumption in Russian law that the data controller is at fault in damage claims on both contractual and tort grounds. The GDPR adopts a similar approach, when describes the conditions under which controller or processor won't be held liable: "A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage"[22]. Strictly speaking, the fault of the data controller is not a part of the overall burden of proof imposed on a data subject by Russian law. However, it deserves some attention because the data controller's fault may affect the success of a data subject's claim for damages.

[22] Art. 82(3).

A data controller's fault may be based upon intent or negligence[23]. Many types of personal data breach may be attributable to intent, which is often influenced by the substantial economic benefits that the data controller may gain from the unlawful use of personal data. A hospital might provide patients' information to other companies in its group or to third party companies for use in direct marketing; or a provider of cloud services may secretly comb through documents stored by data subjects for the same reasons [Truli E., 2017: 317]. Other types of violations of data protection laws, such as failure to implement adequate technical measures to protect personal data, may be attributable to negligence. But in practice this distinction between intent and negligence does not play a substantial role in assessing the merits of the claim: any fault will suffice.

Strict liability may apply under some conditions. This is the case when the liability is connected with the commercial activity of the defendant and has a contractual nature. If a data controller breaches terms concerning data processing expressed in a contract with data subjects and the contract was concluded as part of the commercial activities of the data controller, then the controller will be liable regardless of the absence of fault (Article 401(3) of the Civil Code of the Russian Federation). The data controller may be exempt from liability only if they prove that the violation was due to force majeure. Actions of third parties, especially when they are potentially foreseeable, such as hacker intrusions, cannot be treated as force majeure[24]. Thus specifying relations between the data subject and data controller in an agreement covering personal data processing in a contractual format can be advantageous for the data subject because it can support a stricter treatment of fault; however this advantage may be diminished if the contract contains clauses that limit liability and exclude warranties.

[23] According to Art. 401(1) of the Civil Code of the Russian Federation, "a person is recognized as not at fault, if with the degree of care and caution that was required of him by the nature of the obligation and the conditions of commerce, he has taken all measures for the proper performance of the obligation". The form of fault (intent or negligence) is irrelevant to the amount of damages claimed; any form of fault for a data controller is a sufficient basis for claiming damages.

[24] However, not all courts would share this view. For example, in one of the disputes considered by a Korean court an overseas hacker took personal details relating to 18 million customers of Auction, of whom 145,000 (organized in ten groups) brought "collective" individual suits. In 2010 the Seoul Central District Court held in favor of Auction (upheld on appeal by the Seoul High Court in 2013), finding that its security was not at fault (Auction argued that it was not mandatory to install firewalls at that time because they were not very effective) and apparently also because of the swift response by Auction's management. This is described in: [Greenleaf G., 2014: 132].

1.1.5. Difficulties in legal representation of claims

The complexity of the facts which must be considered in disputes concerning damage claims for violation of a data subject's rights may make legal representation quite expensive, and the time required for litigation and its other general costs may be also be prohibitive for data subjects. By contrast, data controllers, especially the larger companies, have almost unlimited budgets for litigation and are further motivated to litigate in order to prevent the establishment of unfavorable precedents in case law. When the data subject's claim is unlikely to prevail or the amount of damages awarded would probably be small, lawyers have little incentive to take on lawsuits for data subjects. Data subjects for their part are mostly unwilling to pay high legal fees for disputes of this kind, especially when there is little chance of success. The end result is that data subjects in private law disputes with data controllers usually cannot secure legal representation.

Singapore provides the best practical illustration of these points. According to Graham Greenleaf's survey of Asian privacy law, "given the costs of initiating litigation in Singapore, and the risks of costs being awarded against the plaintiff, there is therefore no low-cost or low-risk means by which Singaporean data subjects can seek modest amounts of compensation for data protection breaches."[Greenleaf G., 2014: 313].

1.1.6. Overview of the current situation

In many jurisdictions the prospects for civil law remedies available to data subjects are not very encouraging. As Greenleaf finds, although Hong Kong has a relatively litigious culture in which there are frequent defamation suits, compensation claims there show that the "system did not work". It is believed that only one claim of this kind during the first fifteen years since new regulations on data protection (Personal Data Ordinance of 1995) were adopted has been successful, and there was other one misconceived attempt [Greenleaf G., 2014: 115]. There have been no cases of compensation or damage claims by data subjects in India, nor are any reported in Macao, although its data protection law has been in force since 2005 and is considered one of the strongest (at least on paper) [Greenleaf G., 2014: 268, 283, 519][25]. In

[25] The only evident exception among Asian data privacy laws is in South Korea where some suits brought by data subjects have been successful.

Germany as well non-contractual claims by data subjects based on breaches of data protection rules are viewed as exceptional [Truli E., 2017: 318]. According to the EU Agency for Fundamental Rights (FRA), civil claims are rare because complainants in the sixteen EU member states surveyed were reluctant to initiate court proceedings because of high costs, lengthy procedures and a perceived need to be represented or assisted by a lawyer[26].

In sum, damage claims by data subjects against data controllers are rarely made because they fail to take into account the actual nature of the factors involved in data protection; therefore resorting to such claims cannot be considered effective as a protection for data subjects' rights. According to the report prepared by the European Union Agency for Fundamental Rights, which is one of the most comprehensive studies of the enforcement of data protection remedies, "the available remedies in this sphere are not effective enough"[27]. Let's now turn to the second type of remedy available to the data subject — compensation for moral harm.

1.2. Compensation for moral harm from breaches of data subjects' rights

1.2.1. General criteria for compensation

The underlying requisites for recovery of non-material damage in various countries vary greatly, although there are generally two basic models. Some European legal systems regard every kind of damage as in principle recoverable. The remainder adopts a contrasting approach in which non-material damage is generally compensable only when the law explicitly deems it so.

The Russian law "On personal data" follows the second approach and explicitly provides for compensation of moral harm for violation of data subjects' rights. Data subjects will have to prove the same things required for damage claims: the fact of violation of the data subject's rights granted by the law; the fact of harm; and the causal link between the violation and the moral harm. The main difference from the requirements for claims of dam-

[26] EU FRA, Access to data protection remedies, p. 35.

[27] Comment on the EU FRA report, Access to data protection remedies in the EU Member States, posted 7 February 2014 on the website of the Human Rights House Foundation. Available at: https://humanrightshouse.org/articles/fra-report-access-to-data-protection-remedies-in-eu-member-states/ (accessed: 01.08.2020)

ages is in the second requirement: the nature of a moral harm claim precludes requiring the plaintiff to produce detailed calculations of its amount.

Because this kind of remedy is intended to compensate for non-pecuniary losses, it seems at first glance as if it may be a more suitable remedy for violations of data subjects' rights. According to the clarifications of the Supreme Court of the Russian Federation, moral harm may occur in the form of mental suffering caused by estrangement from relatives, the impossibility of continuing active social life, loss of employment, disclosure of family or medical secrets, physical pain, etc.[28]

In contrast to Russian law, European law considers potential types of non-pecuniary loss more broadly and includes "impairment of the quality of life" in addition to pain and suffering (VI.–2:101 (4) (b) of the EU Draft Common Frame of Reference). Commentary on the Draft Common Frame of Reference (DCFR) explains: "typical examples are provided by infringements of incorporeal rights of personality (among others, incursions into spheres of privacy; derogatory statements which have as a consequence a negative impact on the social profile of the person concerned)." [Von Bar Ch., Clive E. et al., 2009: 3040]. While the concept of non-pecuniary loss as "impairment of the quality of life" may adequately reflect the consequences of some violations of data subjects' rights, a narrowly literal interpretation may not address many types of harm related to privacy.

1.2.2. Russian approach

From a technical standpoint, the list of grounds provided by the Supreme Court of the Russian Federation for claiming moral harm from mental suffering is not exhaustive and may extend to most of the possible grounds for claiming privacy-related mental suffering: damage to reputation, discrimination, interference of third parties in private matters, etc. However, actual case law diverges sharply from this broad approach.

The mere statement by the data subject that a certain violation of their rights caused distress and emotional suffering is routinely rejected by Russian courts. As one of the courts put it, "the mere fact of violation of data subjects' rights does not provide a basis for claims for damages or compensation of moral harm"[29]. According to the established case law, the pres-

[28] Art. 2 of Decree of Plenum of the Supreme Court of the Russian Federation "Some issues in the application of legislation on compensation for moral harm". 20 December 1994. No. 10.

[29] Appellate judgment of the Novosibirsk Region Court. 31 July 2017. No. 33-10465/2017.

ence of moral harm is to be confirmed by verifiable evidence, e.g. a record obtained from a medical institution of a pertinent diagnosis (depression or a nervous disorder)[30]. It is evident that in most cases a data subject will not be able to present such "bullet-proof" evidence.

It may come as a surprise that this position of the Russian courts is on the same page with the DCFR when it states that "negative emotional responses such as annoyance, anger, disgust and repulsion which lie within the spectrum of normal, everyday feelings *are not enough to meet the threshold of physical or mental suffering necessary to succeed with the claim*" (italics added.- A. S.) [Von Bar Ch., Clive E. et al., 2009: 3040]. However, these emotions are the most typical ones when particular rights of data subjects' are violated. Failure to recognize the legal significance of such violations deprives data subjects of an effective remedy for protecting their rights and *de facto* relieves the data controller from liability and responsibility toward the data subject for such violations. This is especially concerning if we examine the position of the European Court of Justice (ECJ), which held that even certain types of fear may have legal significance. In its landmark decision invalidating the EU's Data Retention Directive[31], the ECJ maintained that the mere fact of performing certain kinds of processing, such as profiling or data retention, is '"likely to generate in minds of persons concerned the feeling that their private lives are the subject of constant surveillance"[32].

In addition to the way current legal remedies fail to recognize the distinctive features of privacy-related harm, there is also a problem with arriving at the amount of compensation for moral harm. According to Russian law, the courts have a substantial degree of discretion in determining the amount of monetary compensation awarded when hearing a claim for compensation of moral harm. The court is to set it:

> depending on the nature of the physical and moral suffering caused to the victim and also the degree of fault of those who caused the harm in in the event that the fault is a basis for compensation for harm. In de-

[30] See e.g. Appellate judgment of the Court of Moscow City. 22 December 2015. No 33-48112/2015.

[31] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105)

[32] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v. Ministry of Communications, Marine and Natural Resources and Others and Kärntner Landesregierung und Others, 2014, OJ C175/6, § 34.

termining the measure of compensation for harm, the requirements of reasonableness and justice must be considered. The nature of physical and moral suffering shall be evaluated by a court taking into account the factual circumstances under which moral harm was caused and the individual peculiarities of the victim[33].

The GDPR has established a more detailed list of factors which the courts should take into consideration when setting the amount of compensation:

the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor[34].

Although in theory judicial discretion in setting of the amount of compensation should simplify things for data subjects by removing the need to prove the precise amount of loss suffered, in practice the courts do not exercise this discretion much to the advantage of data subjects.

Russian case law shows how this judicial discretion plays out in fact. The average amount of compensation for moral harm that is awarded to data subjects in Russia varies from 500 to 10,000 rubles (that is approximately from €7 to €130). For example, compensation in the amount of 500 rubles was awarded to a data subject for having information about their failure to make timely public utilities payments posted by a data controller in the public hall of the subject's apartment house[35]. The same amount of compensation was awarded for sending unsolicited SMS marketing messages[36]. The sum of 10,000 rubles was awarded for using an individual's personal identification in an example of how to fill in an application form with the Pension Fund because the personal data had been made publicly available without consent of the data subject[37]. In another case 10,000 rubles were awarded for processing the personal data of an individual to draft a loan

[33] Art. 1101(2) of the Civil Code of the Russian Federation.

[34] §146 of the Recitals to the GDPR.

[35] Cassation judgment of the Saratov Regional Court. 14 February 2012. No. 33-489.

[36] Appellate judgment of the Novosibirsk Regional Court. 31 July 2018. No. 33-7489/2018.

[37] Judgement of Primorsky District Court. 14 July 2014. No. 33-5960.

agreement, which was then used to make legal claims against the individual even though the agreement was not valid because the signature was forged[38].

Many judgments of Russian courts on compensation of moral harm for violation of data subjects rights' are issued without an indication of the amount awarded, which is in keeping with the regulation on maintaining anonymity in the decisions of the courts. But there is no reason to believe that such "anonymized" judgments contain awards substantially different from the ones described above. Cases with much higher awards would be noteworthy enough to be disclosed in other ways, e.g. in mass media and through social networks. Even in those rare cases where the court of first instance has awarded compensation in amounts exceeding the averages indicated above, an appellate court has frequently reduced them[39].

There are two reasons for the negligible amounts of compensation for moral harm in Russia. First, there are no established methods for calculating compensation for moral harm, nor are there any guidelines for their calculation that are more detailed than the provisions of the Civil Code described above [Erdelevskiy A., 1999: 192]; [Marchenko S.V. et al., 2004]. In these circumstances, courts do not provide any explanation of how they arrived at the specific amount of money awarded, and they are reluctant to make themselves conspicuous by departing from the usual small amounts in earlier case law. The courts seem to have become captives of the previous case law and cannot change their approach without legislative intervention. The second reason is that Russian courts tend to acknowledge the occurrence of moral harm more readily when it also affects the material well-being of a person. For example, when harm to the health of a person seriously affects their ability to work and causes an obvious decline in their standard of living, the courts are much more likely to allow compensation for moral harm in addition. Here again we see a misunderstanding of the nature of the privacy harm and of the way data privacy violations produce distress.

The nominal amount of compensations for moral harm awarded by Russian courts has come under heavy criticism in Russian legal discourse [Bogdanova O.V., 2017]; [Tabunschikov A.T., 2017] and even by Russian government authorities. Specifically, in its annual report for 2017 the Russian Service for the Protection of Consumers (Rospotrebnadzor) indicated that the compensation for moral harm when consumer rights are violated

[38] Appellate judgment of the Saint Petersburg Court. 16 August 2018. No. 2-293/2018.

[39] Appellate judgment of the Saint Petersburg Court. 16 August 2018. No. 2-652/2018 (in this case the appellate court decreased the amount of compensation from 30,000 rubles to 10,000 rubles).

should not be 5,000 or 10,000 or even 25,000 rubles, but much higher[40]. Rospotrebnadzor also argues for a uniform way to calculate moral harm[41]. While these recommendations may improve the case law in consumer protection, they are unlikely to be applied to compensation for moral harm resulting from violation of data subjects' rights. Piecemeal solution here will not be enough; more fundamental changes are needed.

1.2.3. European approach

European case law is becoming more generous with the amounts of compensations awarded, but still leaves much to be desired. According to a European Union Agency for Fundamental Rights Report:

> the amounts awarded vary greatly between Member States. Austria for instance, sets an upper limit of €20,000 for non-pecuniary damages, but the range of cases in other Member States suggests that awards of compensation are often much lower, ranging from €300 to €800 in Finland, up to €600 in Sweden, and from €1,200 to €12,000 in Poland[42].

Case law in the UK deserves a closer look, as some of the arguments put forth there and the way they were countered have substantial weight outside of the UK's jurisdiction and may help to illustrate better the main ideas of this paper.

Until recently UK case law could not boast of compensation for moral damage from privacy-related misdeeds. One of the landmark cases is *Google Inc.* v *Vidal-Hall and others*[43]. This is the first case, where the Court of Appeal of England and Wales recognized moral damages under the UK Data Protection Act of 1998. Prior to that case, compensation for distress which was not accompanied by pecuniary loss had not been awarded by UK courts[44].

[40] Protection of Consumers in the Russian Federation in 2017 A Government Report. Moscow, 2017, p. 150 (in Russian)

[41] Idem.

[42] EU FRA, Access to data protection remedies, p. 21.

[43] Google Inc v Vidal-Hall [2015] EWCA Civ 311.

[44] Section 13 (2) of the UK Data Protection Act 1998 provided that "an individual who suffers distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that distress if (a) the individual also suffers damage by reason of the contravention, or (b) the contravention relates to the processing of personal data for the special purposes." A literal interpretation of this provision leads to conclusion that, absent certain pecuniary loss or processing for special purposes (journalistic, literary or artistic), no compensation for distress is possible. This approach was supported by Buxton LJ in Johnson v Medical Defence Union, 2007, EWCA Civ 262.

Moreover, one of the grounds on which it was argued that the UK had not implemented the Data Protection Directive correctly was that the "UK Act does not provide for 'moral damages'"[45].

The Court of Appeal was asked to examine the claim in this case that the defendant had misused private information, acted in breach of confidence, and in breach of its statutory duties under the UK Data Protection Act by tracking and collating information relating to the claimants' internet usage on the Apple Safari browser without their knowledge and consent. That information was subsequently used for Google's targeted advertisements. It was alleged that their personal information was not respected despite the fact that the claimants had set their privacy settings in the browser to block third party cookies[46]. The Court of Appeal, satisfying the claim for misuse of private information, highlighted the status of data protection as a fundamental right in the EU Charter of Fundamental Rights, suggesting that it would be odd if this right could be violated with "relative impunity by a data controller, save in those rare cases where the data subject had suffered pecuniary loss as a result of a breach"[47]. The conclusion was that compensation can be awarded even though no actual financial loss occurred and that any other approach is not compatible with the concept of "effective remedy" under Article 47 of the EU Charter of Fundamental Rights[48].

While no specific reference is made to moral damage or moral harm in the GDPR, it does state in Article 82(1) that "Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered." The provisions of Article 82 provide a comprehensive framework for such claims, which can be used to minimize the discrepancies between the rules for liability that were put in place by various national laws under the EU's Data Protection Directive of 1995.

Apart from that clear indication that both pecuniary and moral types of damages may be compensated, the GDPR also states that they may be claimed against data processors that have not complied with the GDPR ob-

[45] Google Inc v Vidal-Hall, §70.

[46] Similar cases have been brought against Google in the United States, leading to a US$22.5 million Federal Trade Commission fine and a US$17 million settlement with state attorneys general. Available at: https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented; https://www.insideprivacy.com/united-states/google-settles-safari-tracking-charges-brought-by-state-ags-for-17-million/ (accessed: 01.08.2020)

[47] Google Inc v Vidal-Hall, §78.

[48] Google Inc v Vidal-Hall, §91.

ligations specifically directed to processors or where they have acted outside or contrary to lawful instructions of a data controller. Therefore, the distinction between data controllers and data processors is somewhat irrelevant in adjudicating compensation claims.

In general, the wording of Article 82 of the GDPR supports the conclusion that compliance with the GDPR requires a two-tier enforcement system consisting of "a mutually reinforcing combination of public and private enforcement that blends public fines with private damages." [O'Dell E., 2017: 3][49]. The reality is that almost all enforcement is carried out through the public enforcement tier due to the ineffectiveness of the private one.

1.2.4. US approach

US law contrasts with the EU and Russian approaches by retaining a narrow definition of privacy harm. It focuses on pecuniary losses and does not allow compensation for moral damage from privacy-related malfeasance. For example, in *Smith* v *Chase Manhattan Bank* the defendant sold its customer information to third parties in violation of its privacy policy and earned a commission on targeted sales by those third parties to the plaintiff and others. The plaintiffs' contractual legal claim was rejected by the court on the grounds that they could not prove any actual harm inasmuch as they were "merely offered products and services, which they were free to decline"[50].

It was also argued that potential claims based on the fear that surveillance deters individuals from exercising their right to freedom of expression guaranteed by the First Amendment to the US Constitution or that the information may be misused in the future are likely to fail due to Supreme Court's rejection of such a "chilling effect" in its *Laird* v *Tatum* decision. In that case the Supreme Court found the claim without merit, as it did not show any objective harm or threat of future specific harm[51]. Claims against government agencies for damages from invasion of privacy based on the Privacy Act 1974 must also demonstrate "actual damages", and the Supreme Court has held that distress is insufficient to amount to "actual damages" for these purposes[52].

[49] Available at: https://ssrn.com/abstract=2992351 (accessed: 01.08.2020)

[50] Smith v Chase Manhattan Bank 741 NYS2d 100.

[51] Laird v Tatum 408 US 1 (1972).

[52] Doe v Chao 540 US 614 (2004); Federal Aviation Administration v Cooper 566 US 284 (2012).

These examples show that many courts prefer a conservative approach in cases where no specific moral harm has been proven and either dismiss the case entirely or award compensation in amounts so minimal that data subjects are discouraged from vigorously defending their privacy rights. There are exceptions of course, but they do not change the restrictive *status quo*.

2. Some Consequences of Current Approaches

The weak enforcement of individuals' claims for damages and compensation for moral harm justifies a number of concerns.

2.1. Data protection legislation may become a tool primarily for facilitating the state's own agenda

The preponderance of administrative fines among the liabilities attached to privacy-related harms skews the balance away from private law remedies, in which the data subject is the "master" of their claim and the beneficiary of its successful outcome, and toward public law remedies, in which a state authority advances the claim and derives all the financial benefit from its success. That imbalance conflicts with the ideas that individuals should be empowered by giving them free choices and that "natural persons should have control of their own personal data"[53].

Those ideas are derived from a conception of privacy that includes control over information[54]. According to Alan Westin, author of Privacy and Freedom privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." [Westin A., 1967: 7]. According to philosopher Charles Fried, "privacy is not simply an absence of information about us in the minds of others, rather it is the control we have over information about ourselves." [Fried C., 1984: 209]. In other words, the rights of data subjects are not negative rights understood in a passive or nega-

[53] Recital 7 to the EU GDPR. One of the aims of the new regulation outlined in EU policy documents was to "put individuals in control of their own data". See: European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 Final, p. 2.

[54] As a rule, violation of the right to data protection leads to a violation of the right to privacy, at least in its informational aspect, but a privacy violation does not necessarily result in a violation of the right to data protection.

tive sense as the right to be left alone, but instead they are *proactive* rights which facilitate active involvement of individuals in managing their data. Individuals should therefore be instrumental in making data protection law more effective.

However, there cannot be control without the opportunity to mount an effective defense of a right, including the possibility of defending it at the discretion of its owner. Where there is no effective access to justice in order to obtain redress, there is no additional accountability for those processing data; hence, there is no true control. Outsourcing enforcement solely to data processing authorities creates merely an illusion of control by data subjects because the DPA is a state authority performing its functions primarily in the interests of the state rather than in the interests of the data subject. One's privacy will be valued less than matters of national sovereignty over information or efficiency in the operations of the state authority.

Personal data regulations have already become "dual use" in nature and pursue two different purposes. One officially declared purpose is to respond to the need for protecting the interests of data subjects. A second more covert purpose is to implement a political agenda of increasing control over the internet. A vivid example of this approach is data localization regulations, which have the officially proclaimed purpose of protecting individuals from misuse of their information, but in fact are intended to facilitate law enforcement, increase growth in the local data center market, and provide conditions suitable for keeping the nation's internet autonomous and under national control.

Russia is no newcomer to using personal data legislation for such political purposes. In his comprehensive examination of cross-border data flows and the attempts to control them, Christopher Kuner finds that national regulation of data protection (and of transborder personal data flow in particular) is frequently a way to protect national interests and national sovereignty. Although the examples provided by Kuner date from the 1970s and '80s, they still seem quite relevant to current concerns [Kuner C., 2013: 30].

There are other items in a state agenda for which "assistance" from a DPA may come in handy, such as protecting local companies or advancing economic and geopolitical ambitions. If you ask any major internet company why it made a certain decision that has an impact on processing personal data, you will hear some variation of "to improve the user experience". But as Frank Pasquale, a persistent critic of the way privacy is succumbing to business interests has pointed out, "we all know that it's only a certain kind

of user experience that is really valued and promoted…. the more a person clicks on ads and buys products, the better …. the more a person draws other potential ad clickers in — the more valuable they become." [Pasquale F., 2015: 166]. Such an approach certainly results in processing more and more information from individuals and sharing it with more parties. Because it may facilitate the growth of data-dependent companies and of certain associated segments of the national economy, a DPA may give a sympathetic hearing to a data controller's arguments that these intrusive kinds of data processing are a "legitimate interest" of the data controller, or that proper consent with lengthy privacy policies has been obtained, or that they are necessary for "fulfilling the terms of an agreement". Any resulting privacy harm would be regarded as "collateral damage", necessary to achieve the primary, more important goal.

Finally, the desire of national governments to gather intelligence has lured them into a pragmatic, extensive and largely secret partnership with interests whose concern is not the public good but private profit or personal advancement [Pasquale F., 2015: 47]. Considerations of "national security" usually override those of human rights, and a DPA may have no say in balancing those concerns or else advocate the policy that the government told it to promote, even if the DPA is formally independent from the government.

The logical extension of that way of designing data protection legislation would be turn it into a mere set of administrative rules that channel the flow of personal data. The law's core purpose of protecting the fundamental human right to privacy through protecting data would vanish.

2.2. Underenforcement of personal data protection legislation by underresourced DPAs resulting in underprotection of individuals

The lack of effective remedies available to data subjects themselves makes them indifferent to protecting their privacy and rights, and as a result the rights of data subjects become degraded. Data subjects must lodge a complaint with a DPA in order to protect their interests, and the DPA's resources are not unlimited. It is not possible to review and investigate each complaint and to punish every violation of data protection regulations. The headlines in the media about fines levied on data controllers are a drop in the sea of overall non-compliance by data controllers that consider themselves out of the reach of DPAs or under their radars. This means that a huge number of violations remains unaddressed, which in turn substantial-

ly diminishes the motivation of data controllers to implement the necessary data protection measures. The hope that violations will go unnoticed is too alluring. If data subjects had an effective remedy to directly deploy against data controllers, it would greatly augment the efforts of DPAs and increase the cost of non-compliance for data controllers so that they would make an attempt in good faith to comply with data protection regulations.

Something is needed to reach a better balance between individuals and data controllers. The argument usually made against improving the balance starts from the claim that private organizations have an insatiable appetite for data and hinges on faith in the usefulness of ever-increasing data to inform decision-making and make it more effective. Individuals are losing this tug of war. Data protection law has been labelled a "dead letter" because legislation and judicial decisions are allegedly having only a marginal effect on data protection practices [Rule J., 2007: 192]. While introducing more effective remedies available to data subjects will not by itself change this trend, it may place some extra weight on the scale in favor of individuals. It may add a qualification to the current jape, "If the product is free, you are the product," and turn it into, "If the product is free, you are the product unless you have a weapon impossible to ignore at your disposal."

Administrative fines and DPA crackdowns cannot replace the initiative of individuals in protecting their own privacy interests. Apart from any of the other previously mentioned factors, DPAs do not have the resources to uncover, investigate and address all the possible violations of data protection. An increase in the number of complaints submitted to DPAs will only aggravate this problem. For example, in Russia there has been a 44% increase in complaints from data subjects during the first half of 2019 compared to the same period in 2018[55].

Only individuals themselves, or a group of them backed by organizations specializing in privacy protection, may challenge this status quo. Perhaps the result would be disappointing, but again: "nobody made a greater mistake than he who did nothing because he could do only little."

In short, the current approach of saddling the data subject with the burden of proof for establishing specific damages and a causal link with a specific violation discourages claims, reduces private enforcement of data protection rights, and undermines the effectiveness of the data protection system.

[55] Available at: https://rkn.gov.ru/news/rsoc/news68534.htm?fbclid=IwAR30E519qNDsnR68XrgcwoCcrQpZ3_1KCX1zRD2hqsjBN5Z1gn_XDHQxQLY (accessed: 01.08.2020)

3. How to Fix it?

3.1. Statutory compensation as an alternative remedy

The foregoing analysis of Russian case law and some examples drawn from the case law of other countries shows that the main problem with the claims for compensation of data subjects is in proving that there was definite certain harm recognized by law and establishing a causal link between a violation and the harm. Other kinds of remedies, such as compensation for moral harm, also fail to adequately address the problem. Therefore, the most obvious improvement is to exclude definite harm and causation from the burden of proof.

Although this solution may at first seem simplistic and radical, considering some analogous situations should help us see how reasonable it is. And we do not need to go far to find them: the clearest analogy can be found in intellectual property law. To avoid having copyright owners go through the difficult exercise of determining the exact number of infringements and the possible causal links to harm, a special remedy was applied in many jurisdictions: statutory damages[56] or in the terminology of Russian law "compensation for violation of an exclusive right"[57]. According a study from 2013, twenty-four countries have adopted a remedy of this kind for copyright infringement[58].

Although some "prototypes" of statutory damages may be found in the legislation of the Russian Empire[59], statutory damages are an innovation that the United States has applied to copyright laws in the international arena, and it succeeded in exporting it to other countries through bilateral and multilateral treaties as well as by other means [Samuelson P., et al., 2013: 530][60]. The original rationale for statutory damages was typically that estab-

[56] 17 United States Code §504 Remedies for infringement: Damages and profits.

[57] Art. 1252(3) of the Civil Code of the Russian Federation.

[58] Azerbaijan, Bahamas, Bahrain, Belarus, Bulgaria, Canada, China, Costa Rica, Dominican Republican, Israel, Kazakhstan, Kyrgyzstan, Liberia, Lithuania, Malaysia, Morocco, the Republic of Korea, the Republic of Moldova, the Russian Federation, Singapore, Sri Lanka, Ukraine, the United States, and Vietnam. The authors of the study points out that the United States is in strange company here.

[59] According to Art. 23 of the 1911 Law on Copyright of the Russian Empire, a copyright owner is entitled to claim damages for infringement, the amount of which is defined by the court in accordance with the requirements of fairness.

[60] Available at: https://cyber.harvard.edu/people/tfisher/IP/Samuelson_SDs_2013.pdf (accessed: 01.08.2020)

lishing the number of copies that had been made by an underground pirate publisher would be difficult and that awards of statutory damages would save rights holders from having to do so. Statutory damages are an atypical ("extraordinary") remedy mainly because they allow owners of rights to recover substantial monetary damages within a fixed range of amounts without any proof that the plaintiff suffered any actual harm from the infringement or that the defendant profited from the infringement. According to US copyright law, these damages can be awarded in whatever amount the judge or jury deems "just" within a range between US $750 and US $30,000 per infringed work, and up to US$150,000 per work if the infringement is willful. Under Russian law the range is between 10,000 and 5,000,000 rubles (approximately, US$150 to US$80,000 per infringed work). If the statutory minimum seems out of proportion with the offense, awards less than the statutory minimum are possible, although this to a certain extent undermines the punitive purpose of this remedy[61].

Personal data and objects of copyright have many similarities. Both consist of *information*. Both copyright infringement and personal data violations may be treated as *misuse* of information. But the most important similarity between them is that *proof of damages* caused by misuse and of their exact amount *is extremely difficult* or even impossible, either because of the intangible nature of the damage, or because the claimant lacks the necessary information, or because the damage is remote from the actual misuse.

These similarities justify the application of similar remedies. If a new special type of remedy has been devised for copyright infringement in order to offset the ineffectiveness of the existing remedies, why can it not be applied also to cases in which the conventional remedies are ineffective and the object (information) is of the same kind? Furthermore, case law on copyright has already acknowledged its usefulness in protecting privacy interests [See for details: Samuelson P., 2013: 191–198].

That there are substantial difficulties in the definition of harm (damages) in data privacy cases and consequently for an individual to prove such harm has already been mentioned, and that problem has been thoroughly examined in legal literature. As a specialist in privacy issues and the internet observed in a US-based law journal, "A privacy harm must be 'cognizable,' 'actual', 'specific,' 'material,' 'fundamental' or 'special' before a court will

[61] Decree of Plenum of the Supreme Court of the Russian Federation "On application of part four of the Civil Code of the Russian Federation". 23 April 2019. No. 10.

consider awarding compensation. Leading commentators question whether privacy harm is much of a harm at all."[Calo R., 2011: 1132]. The author of a book on EU data protection law argues that "it is not possible to develop an exhaustive taxonomy of harms caused by unregulated data processing." [Lynskey O., 2015: 211].

The peculiar nature of privacy harms is recognized in case law as well. The European Court of Justices alluded to it specifically in its *Digital Rights Ireland Ltd* v *Minister for Communications* judgement, which found that personal data processing may have a chilling effect on individual behavior because it gives individuals the impression that they are being surveilled or monitored; and that in turn has both an inhibiting and a controlling effect on them. The current ubiquity of information technology, as well as the ability use it to aggregate the data gathered, has blurred the lines between information gathering and surveillance [Austin L., 2003: 119, 151]. Some scholars have even coined the term "dataveillance" for this topic, which they define as "the systematic use of personal data systems in investigation or monitoring the actions or communications of one or more persons [Clarke R., 1991: 496]. Most courts operating within a conventionally established framework for damage compensation would not recognize a "chilling effect" as a legally significant harm, and the data subject would be denied just redress. Courts persuaded by the arguments of some authoritative scholars that human access to sensory or other personal information is a necessary condition for privacy harm and that processing alone, if never "displayed to a human," leads to "no adverse consequence of any sort" [Goldman, E., 2005: 228], would be even less inclined to provide that redress. In an article by a prominent US judge and author of books on invasion of privacy, there is this opinion that computer searches do not invade privacy because programs are not sentient beings." [Posner R., 2008: 254]. However, studies of automated decision making [Pasquale F., 2015:14; Keats D., 2008: 1249][62], which is becoming commonplace now, have pointed out the error here. The fact that much information processing now occurs outside human sensory and temporal awareness does not mean that it cannot lead to negative consequences and deprive person from protection, as

[62] "The success of individuals, businesses, and their products depends heavily on the synthesis of data and perceptions into reputation. In ever more settings, reputation is determined by secret algorithms processing inaccessible data. Few of us appreciate the extent of ambient surveillance, and fewer still have access either to its results — the all-important profiles that control so many aspects of our lives."

long as we continue to recognize that an unconscious patient in a hospital bed is entitled to the same suite of rights and level of privacy protection as that patient had when fully aware.

One solution would be to stretch the concept of damage to somehow accommodate this particular privacy-related type of harm. But this may distort the regulation of claims for damages in general and have unintended negative consequences for the legal system. It is also highly unlikely that the situation could be corrected merely through some guidelines issued by a supreme court or other authoritative body to the effect that the courts are to award more compensation for moral harm. That would not make it easier to ascertain the fact of moral harm and trace out a causal link between it and a violation. A better response would be to exclude any kind of damage from the burden of proof and create a new alternative remedy. This would also align with the established position of the ECHR, according to which "the applicant cannot be required to furnish any proof of the non-pecuniary damage he sustained"[63].

This alternative remedy could be named "statutory compensation for violation of the individual's data protection rights" or just "statutory compensation" to distinguish it from statutory damages for copyright infringement and other customary damage claims.

3.2. Human rights justification for statutory compensation

The right to personal data and its role in representation of a person in a digitalized world is fundamental to the exercise of freedom in digital society and managing one's digital identity. Manipulation with figures and data relating to the individual leads to manipulation of people. Conferring a remedy for violation of the individual's data protection rights on the individual and making it applicable even in the absence of tangible or intangible harm serves the general interest. That general interest is similar to the general interest in protecting liberty. One of the clearest illustrations of this thesis is in UK case law pertaining to the tort of false imprisonment. In *Murray* v *Minister of Defence* the House of Lords noted *obiter dictum* that neither consciousness of confinement nor proof of special damage was a necessary ingredient of the tort. Lord Griffiths emphasized that "the law attaches su-

[63] Artyomov v Russia, No. 14146/02, 27 May 2010, §218; Antipenkov v Russia, No. 33470/03, 15 October.2009 §82; Gridin v Russia, No. 4171/04, 1 June 2006, § 20.

preme importance to the liberty of the individual and if he suffers a wrongful interference with that liberty it should remain actionable even without proof of special damage"[64].

As legal scholars have commented, "there is a general interest in upholding individual liberty, which goes above and beyond the individual consequences"[65]. It is possible to draw an analogy here, as Orla Lynskey does, with personal data regulations because a similar general interest in granting individuals control over their personal data exists, irrespective of whether they suffered harm or not in a particular case [Lynskey O., 2015: 196]. Lynskey argues further that granting control to individuals over their personal data may constitute the latest step in the evolving expansion of the individual's sphere of control. In the past, individuals have been given control over their property or personality, and data protection legislation extends this individual control to encompass digital manifestation of personality[66]. Other scholars also have found similar analogies between personal data and other freedoms. For example, the philosopher Boudewijn de Bruin argues that processing personal data can result not merely in an immediate loss of freedom for an individual; it can also bring about a future loss of "negative freedom" — the freedom to act without external impediments [Boudewijn de Bruin, 2010: 505, 514]. This is especially true when personal data is used for profiling, which may lead to discrimination or automated decision-making with regard to an individual.

If we accept that control over personal data is the essence of the fundamental right to manage personal data and privacy, then we should also apply the principle of international law that an effective remedy should be attached to that right and accept that the remedy may become an important component of a data controller's accountability.

The ECJ underlines the special importance of private enforcement of data protection legislation because "legislation not providing for any possibility for an individual to pursue legal remedies…, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter"[67].

[64] Murray v Minister of Defence, 1998, 1 WLR 692.

[65] Markesinis and Deakin's Tort Law. Oxford, 2008, p. 465.

[66] Idem.

[67] Schrems v Data Protection Commissioner, Case C–362/14, 6 October 2015, para 95.

Some traces of this thinking may be found in the European Commission's claim mentioned earlier that the UK had not implemented Data Protection Directive of 1995 correctly because the UK Data Protection Act of 1998 did not provide for "moral damages". An extract from one of the sources mentioned by Court of Appeal of England and Wales speculates that the Commission's view is

> that "an effective remedy" must include some element of compensation for any breach (*emphasis added.* — A.S.) of the (Data Protection Act) and therefore where a breach has caused a hurt to feelings or dignity but no actual loss a remedy in damages should be provided by the UK courts. On the other hand, it can be strongly argued, that there is no such obligation as long as the domestic legal system provides an effective set of remedies[68].

3.3. Functions of statutory compensation

Introducing a new type of remedy for violation of data subjects' rights becomes especially attractive when we consider the functions which statutory damages play in the enforcement of copyright law and understand their relevance to data protection.

Paula Samuelson has outlined the following functions of statutory damages as: (1) a rough approximation of the compensation due for actual harm and/or profits lost; (2) a deterrent sufficiently large to discourage the defendant in a particular case from infringing again; (3) retribution for the defendant's misconduct; and (4) a general deterrent. The general deterrence rationale can be further separated into: (1) the general deterrent value in punishing defendants fairly, including retribution, in proportion to their own conduct and in such a way that other similarly situated potential defendants would fear being punished;, and (2) punishing defendants with an award beyond what their conduct individually merits in order to set an example that will deter the public at large [Samuelson P., 2013].

In Russian academic literature there is no common approach to the nature of statutory damages, whether punitive or compensatory, although there is an attempt in case law to reconcile them in practice [Starzhenetskiy V., 2015]. It seems that the Council of Europe's Modernized Convention No. 108 adopts a similar stance, according to which "in any event, any sanc-

[68] Google Inc v Vidal-Hall, para 70.

tions imposed need to be effective, proportionate and dissuasive"[69]. One interpretation could be that requiring the sanction to be proportionate refers to its role as compensation; that the requirement of dissuasiveness pertains to its punitive or deterrent function; and that meeting both requirements makes the sanction an effective one.

If there is anything about which regulators and data protection specialists agree, it is that protection of data subjects' rights and the overall level of enforcement of data protection regulations has much room for improvement. Underresourced DPAs and data subjects lacking effective remedies and motivation to protect their rights cannot facilitate effective enforcement, while data controllers have too little incentive to comply with data protection regulations voluntarily. Instead of making a sustained effort to comply with data protection regulations, many of them are erecting so-called Potemkin villages to give the illusion of compliance[70]. Introduction of a new remedy with a punitive element and administered in a decentralized way by data subjects may change the situation. Statutory damages may make data protection enforcement more uniform and successful.

This argument becomes even more persuasive in view of the conclusions reached by the EU FRA study on access to data protection remedies in the EU. It states that "financial compensation was not a motivating factor to seek redress… *they sought redress to ensure that similar data protection violations do not recur* [emphasis added]"[71]. In other words, the deterrent

[69] Explanatory Report to Convention of the Council of Europe No. 108+ (Convention for the protection of individuals with regard to the processing of personal data). 2018, p. 29. Available at: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (accessed: 01.08.2020)

[70] The term comes from reports of a fake portable village built solely to impress Empress Catherine II by her former lover Grigory Potemkin during her journey to Crimea in 1787. While modern historians claim accounts of this portable village are exaggerated, the original story was that Potemkin erected phony portable settlements along the banks of the Dnieper River in order to impress the Russian Empress; the structures would be disassembled after she passed and re-assembled farther along her route to be viewed again as if there were another settlement. This term is widely used in the US case law, e.g. in the 2018 lawsuit filed against Exxon for fraud relating to the discrepancy between the published cost of climate regulations and the internally calculated costs. New York Attorney General Underwood's complaint alleged, "Through its fraudulent scheme, Exxon in effect erected a Potemkin village to create the illusion that it had fully considered the risks of future climate change regulation and had factored those risks into its business operations." See: Summons and Complaint in *People of the State of New York* v *Exxon Mobil Corporation*, Supreme Court of New York, 24 October 2018, p. 11.

[71] EU FRA, Access to data protection remedies, p. 8. A high proportion of survey respondents wanted to minimize the risk that other individuals would become victims of data protection violations. They most frequently mentioned "prevention of future violations of rights", "awareness rais-

function is one of the features of the effective remedy most demanded by individuals. This becomes especially understandable once we realize that certain types of privacy damage cannot be remedied; unlawful disclosure and distribution of sensitive medical information would be one example. As patients' rights advocate Deborah Peel observes, "with consumer credit cards, it is possible to close accounts, terminate authorization, and reissue credit cards… breaches of electronic health records cannot be fixed, and privacy cannot be restored" [Peel D., 2015: 178].

3.4. Criteria for definition of appropriate amount of compensation

What criteria courts should apply in setting the appropriate amount of statutory compensation is one of the basic questions about how to implement it. Here again we can turn to many of the already established precedents in case law pertaining to copyright infringement. As one example, the following criteria taken from copyright infringement cases may be used as guidelines for data protection cases:

the scope of the infringement;

how long the infringement continued;

the severity of the infringement;

the actual injury caused to the claimant according to the assessment of the court;

the benefit derived by the defendant from the infringement, according to the assessment of the court;

the nature of the defendant's activity;

the nature of the relationship between the defendant and the claimant;

the good faith of the defendant.

Some of these criteria are already used by the courts in privacy-related disputes. For example, the Supreme Court of Korea outlined the following factors for assessment of circumstances under which mental distress arising from data leaks may be compensated even in the absence of pecuniary damage:

the type and characteristic of the personal information leaked;

whether a third party accessed the leaked information and, if not, whether there is a probability that a third party had such access or will have it in the future;

---

ing", "stopping the wrong practice", "standing up for fundamental rights", "teaching a lesson to concerned authorities", "obtaining an acknowledgement of the violation from a competent authority" or "imposing a sanction on the perpetrator" (p. 29).

to what extent the leaked information was disseminated;

whether the leak caused any additional infringement of rights;

the actual way in which personal information was managed by the defendant;

any specific circumstances in which the information was leaked;

what measures were taken to prevent injury caused by the leak and to prevent the dissemination of the information[72].

In other words, while maintaining the necessary degree of flexibility, it is possible to outline a number of factors which should be considered by courts in order to ensure some degree of uniformity and predictability in the application of statutory compensation for violations of data privacy rights.

The problem in applying statutory compensation to multiple violations of data subjects' rights committed by a data controller may be solved in different ways. The first approach would be to treat all violations undertaken as part of a single set of activities as a single infringement for the purposes of statutory damages. A second possibility would be to establish a cap on the overall award. Finally, there could be a cap which would apply in the absence of any evidence that the plaintiff's actual loss exceeded that amount. The first approach looks the most promising, at least while the new remedy is still in "test mode".

3.5. Not-for-profit organizations as the key player in enforcement of the new remedy

As was illustrated above, the costs, timing and overall efforts associated with protection of data subjects' rights in court proceedings are a substantial barrier to private enforcement of those rights. Lawyers and specialized organizations in many cases lack the financial motivation to engage in disputes of that kind.

[72] GS Caltex Data Breach Case, Supreme Court decision 2011Da59834,59858,59841. 26 December 2012. Available at: http://library.scourt.go.kr/jsp/html/decision/9-69%202012.12.26.2011Da59834.htm (accessed: 15.07.2020). Ultimately, the Court dismissed the claim on the ground that emotional distress cannot be assumed merely due to the existence of a large data spill. Either actual damage or emotional distress would have to be proven and shown to have been caused by the data spill. This is one more illustration in support of the position that effective remedies which empower data subjects to seek redress for violations of personal data regulations should be free from the requirement to prove the fact of privacy harm.

Article 80 of the GDPR provides an important foundation for bringing a new type of claimant to bear on privacy matters. It gives the data subject "the right to mandate a not-for-profit body, organization or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data … to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law."

According to the EU FRA, this would:

> enable civil society organisations and other bodies working in the data protection field, and having the necessary expertise and knowledge of the legal rules and situation in practice, to take a more direct role in litigation. This would in turn help to ensure better implementation of the data protection law, in particular where certain practices affect a multitude of individuals and/or where the victims of a breach of data protection rules are unlikely to bring individual actions against a data controller, given the costs, delays and burdens they would be exposed to. The introduction of broader legal standing rules would have to be done hand in hand with specific safeguards to preserve the fine balance between preventing abusive litigation and effective access to justice for data subjects[73].

But as this paper argues, these beneficial effects will appear only when accompanied by a new kind of remedy available to data subjects. That change may indeed bring about a kind of collective approach to enforcing data protection rights in the sense that a data subject is not left on their own in opposing a powerful data controller. This would provide an additional incentive for data controllers to take privacy commitments more seriously and put appropriate measures in place, especially if the activities of these institutions are followed by noticeable sanctions for any breaches of privacy.

To a certain extent this reform may also improve some long-standing problems with privacy policies. As Daniel Solove observes: 1) people do not read privacy policies; 2) if people read them, they do not understand them; 3) if people read and understand them, they often lack enough background knowledge to make an informed choice; and 4) if people read them, understand them, and can make an informed choice, their choice might

[73] EU FRA, Access to data protection remedies, p. 32.

be skewed by various difficulties in reaching a decision [Solove D., 2013: 1881]. This exposes an interesting paradox explained by Omer Tene in a US-based law journal: "if information is simplified, individuals will not be fully informed; if information is detailed, individuals will not understand." [Tene O., 2013: 1246].

When a statutory compensation remedy is available, it creates an additional incentive for certain individuals to dig deeper into privacy policies accepted by them because it may result in a direct monetary reward. It also provides a financial motivation for active privacy activists and institutions that defend human rights and/or data subjects' rights to analyze and monitor compliance with them. This may breathe new life into privacy policies and the overall transparency of personal data processing.

3.6. The new remedy may be a strong weapon, but not a magic bullet

The new remedy cannot by itself address all the data protection problems which are often rooted in the limitations of human nature. Based on research in behavioral economics, cognitive sciences and human-computer interaction, arguments have been made that the complexity of data management matters is such that our judgments about it are prone to errors stemming from lack of information or computational ability, problems with self-control, and biased decision-making processes. For instance, time and attention are limited; it is impossible to control every single piece of information about oneself which circulates on the networks through myriads of channels and databases. Another consequence of the emphasis on active choosing or control is the difficulty raised by people's preference not to choose. Indeed, the costs imposed on data subjects can be so high in complex and technical areas they are unfamiliar with that the majority of them tend to stick with the default options instead of exercising their freedom of choice and being in control of the situation [Lazaro C., Le Métayer D., 2015: 32]. Lazaro and Le Métayer "believe that it is nearly impossible for data subjects to really measure the breadth of their disclosure and the long-term effects of their actions. It is thus very unlikely that they do not suffer harm even from a potentially informed, autonomous and responsible decision." Therefore, as Solove suggests, it is still necessary to "continue to engage in an elaborate dance with the tension between self-management and paternalism." [Solove D., 2013: 1990].

These complications do indeed substantially decrease the potential for active participation by most data subjects in defending their rights as data subjects. Nevertheless, introducing statutory compensation for data protection violations may become an important part of the overall enforcement of data protection regulations and management by individuals of their digital personae and reputations. It may prevent or at least slow down their commodification in the digital era. Ultimately, it may help to overcome the shortcomings from underenforcement of existing data protection regulations by the data subjects and underresourced DPAs.

References

Acquisti A. (2010) The Economics of Personal Data and Economics of Privacy. Paper presented at the OECD Round table, p. 26.

Austin L. (2003) Privacy and the Question of Technology. *Law and Philosophy*, no 22, pp. 119, 151, 196.

Bogdanova O.V. (2017) *Protection of Copyright with Civil Law Remedies.* Moscow: Ustitsinform, 211 p. (in Russian)

Calo R. (2011) The Boundaries of Privacy Harm. *Indiana Law Journal*, vol. 86, p. 1132.

Citron D. (2008) Technological Due Process. *Washington University Law Review*, vol. 85, p. 1249.

Clarke R. (1991) Information Technology and Dataveillance in: *Computerization and Controversy: Value conflicts and Social Choices*. Academic Press, p. 496.

Bruin B. (2010) The Liberal Value of Privacy. *Law and Philosophy*, no 29, pp. 505, 514.

Erdelevskiy A. (1999) *Compensation of Moral Harm: Analysis and Commentary on the Legislation and Case Law*. Moscow: VEK, p. 192 (in Russian)

Fried C. (1984) Privacy (A Moral Analysis) in: *Philosophical Dimensions of Privacy*. F. Schoeman, ed. Cambridge: University Press, p. 209.

Goldman E. (2005) Data Mining and Attention Consumption in: *Privacy and Technologies of Identity*. K. Strandburg & D. Raicu, eds. Boston, MA: Springer, p. 228.

Greenleaf G. (2014) *Asian Data Privacy Laws: Trade and Human Rights Perspectives*. Oxford: University Press, pp. 115, 132, 151, 268, 283, 313, 519.

Kuner C., Bygrave L. et al (2020) *The EU General Data Protection Regulation: A Commentary.* Oxford: University Press, p. 1135.

Kuner C. (2013) *Transborder Data Flows and Data Privacy Law*. Oxford: University Press, pp. 30 ff.

Lazaro C., Le Métayer D. (2015) Control over Personal Data: True Remedy or Fairy Tale? *SCRIPTed*, vol. 1, pp. 10, 32.

Lynskey O. (2015) *The Foundations of EU Data Protection Law*. Oxford: University Press, pp. 196, 209, 211.

Marchenko S.V. et al (2004) Compensation for moral harm in the mirror of Russian law, *Advokatskaya praktika*, no 5, pp. 20–23 (in Russian)

O'Dell E. (2017) Compensation for Breach of the General Data Protection Regulation. *Dublin University Law Journal,* vol. 1, p. 3.

Pasquale F. (2015) Privacy, Autonomy, and Internet Platforms in: *Privacy in the Modern Age: The Search for Solutions*. M. Rotenberg et al, eds. New York: New Press, pp. 14, 166.

Pasquale F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press, p. 47.

Peel D. (2015) The Future of Health Privacy in: *Privacy in the Modern Age: The Search for Solutions*, p. 178.

Posner R. (2008) Privacy, Surveillance, and Law. *University of Chicago Law Review*, vol. 1, p. 254.

Rule J. (2007) *Privacy in Peril: How We are Sacrificing a Fundamental Rights in Exchange for Security and Convenience*. Oxford: University Press, p. 192.

Samuelson P. et al (2013) Statutory Damages: A Rarity in Copyright Laws Internationally, But for How Long? Berkeley Public Law Research Paper No. 2240569, pp. 191–198, 530.

Solove D. (2013) Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, no 126, pp. 1881, 1888, 1900.

Starzhenetskiy V. (2015) Statutory Damages in the Intellectual Property Law of the Russian Federation. *Vestnik ekonomicheskogo pravosudia*, no 10, pp. 116–147 (in Russian)

Tabunschikov A.T. (2017) *Compensation of Moral Harm.* Moscow: Prospect, p. 29 (in Russian)

Tene O. (2013) Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws. *Ohio State Law Journal*, no 74, p. 1246.

Truli E. (2017) The General Data Protection Regulation and Civil Liability in: M. Bakhoum et al , eds. *Personal Data in Competition, Consumer Protection and Intellectual Property Law — Towards a Holistic Approach?* New York: Springer, p. 312.

Von Bar C., Clive E., et al (2009) *Principles, Definitions and Model Rules of European Private Law. Draft Common Frame of Reference*. Munich, pp. 3040, 3052.

Westin A. (1967) *Privacy and Freedom*. Toronto: McClelland and Stewart, p. 7.

Ylan Q. Mui (2011) Little-Known Firms Tracking Data Used in Credit Scores. *Washington Post*, July 16.

AI-Generated Inventions and IPR Policy During the COVID-19 Pandemic

Chhavi Sharma

Research Officer, Indian Institute of Public Administration, PhD. Address: Indraprastha Estate, Ring Road, New Delhi 110002, India. E-mail: chhavi.mail@gmail.com.

Reeta Sony

Assistant Professor, Centre for Studies in Science Policy, School of Social Sciences, Jawaharlal Nehru University, PhD. Address: New Mehrauli Road, JNU Ring Rd, New Delhi 110067, India. E-mail: reetasony@msil.jnu.ac.in

> «Actions are right in proportion as they tend to promote happiness; wrong as they tend to produce the reverse of happiness. By happiness is intended pleasure and the absence of pain».
>
> *John Stuart Mill*

Abstract

According to the World Health Organisation's (WHO) official website for coronavirus, the disease has spread to approximately 214 countries and regions. While the disease is spreading mercilessly around the world, science and technology are giving it an equal fight. The pandemic is a test of governments' medical capacity and their political will; it also raises several philosophical questions. It is a test of humans as a unit. A test of humanity as a whole. Artificial Intelligence (AI) is intended to imitate human cognitive functions. It will bring significant change to health care, driven by the growing accessibility of healthcare data and rapid advancement of analytics practices. During the current COVID-19 pandemic, AI is being used to assist and advise doctors in establishing a diagnosis, to support radiologists in refining image explanation, and help in the advancement of drug discovery research. The upsurge of new technologies gives rise to new questions. There is still considerable uncertainty in the field of Intellectual Property (IP) protection of AI-generated works. AI does not have legal personhood, so the question remains about whether it holds any IP rights. In this article, we discuss the IP rights of AI-generated works with respect to the COVID-19 pandemic. The objective of this study is to determine the impact of international and national laws and treaties on IP rights for AI-generated solutions to the pandemic, as well as to study an alternative temporary mechanism to make IP widely available to mobilise resources and manufacture critical products to prevent, diagnose or treat COVID-19. The paper attempts to strike a balance between the needs of health care, life-threatening emergencies and IP rights by applying a utilitarian theory of IP law that denotes the «utility» of all people, aiming to secure «the greatest good for the greatest number».

Keywords

Pandemic, COVID-19, AI-generated Work, Intellectual Property, Data Protection, Privacy, Health Care, Crisis, Patent Pool, Open Access, Cooperation, Harmony.

For citation: Sharma C., Sony R. AI-Generated Inventions and IPR Policy during the COVID-19 Pandemic // *Legal Issues in the Digital Age*, no 2, pp. 63–91.

DOI: 10.17323/2713-2749.2020.2.63.91

Introduction

Ever since the first case of coronavirus[1] (COVID-19)[2] occurred in Wuhan, China, it has spread to about 216 other regions and countries. As various countries initiated their response to the virus, they leaned heavily on the technology sector and specifically on artificial intelligence (AI), data science, and technology to track and fight the pandemic. Tech start-ups are intrinsically involved with academics, clinicians and government entities around the world in order to stimulate technology as the virus continues to spread.

Technology and medical companies around the world are intensifying their efforts to tackle the effects of the COVID-19 pandemic. Life-saving treatments for the disease are being developed using Artificial Intelligence (AI) and supercomputers. The COVID-19 High Performance Computing Consortium[3], introduced in late March by the White House[4], aims to bring together industry leaders in AI, national laboratories and academics to "significantly advance the pace of scientific discovery in the fight to stop the virus"[5]. Against the back-

[1] Corona viruses are a large family of viruses which may cause illness in animals or humans. In humans, several coronaviruses are known to cause respiratory infections ranging from the common cold to more severe diseases such as Middle East Respiratory Syndrome (MERS) and Severe Acute Respiratory Syndrome (SARS).

[2] The most recently discovered coronavirus causes coronavirus disease COVID-19.

[3] The COVID-19 High Performance Computing (HPC) Consortium is a unique private-public effort spearheaded by the White House Office of Science and Technology Policy, the U.S. Department of Energy and IBM to bring together federal government, industry, and academic leaders who are volunteering free compute time and resources on their world-class machines

[4] White House Announces New Partnership to Unleash U.S. Supercomputing Resources to Fight COVID-19. Available at: https://www.whitehouse.gov/briefings-statements/white-house-announces-new-partnership-unleash-u-s-supercomputing-resources-fight-covid-19/ (accessed: 23.05.2020)

[5] Marr B. Coronavirus: How Artificial Intelligence, Data Science and Technology is Used to Fight the Pandemic. Available at: https://www.forbes.com/sites/bernardmarr/2020/03/13/coronavirus-how-artificial-intelligence-data-science-and-technology-is-used-to-fight-the-pandemic/#6f966c0e5f5f.) (accessed: 23.03.2020)

drop of COVID-19, industries are looking to AI for predictive modelling, tracking, diagnosis and prognosis. While the use of AI will unquestionably result in credible invention, data, test results, and any inventions resulting from its use will raise questions about how to best protect these innovations and who should receive credit as an inventor.

Science, Technological Inventions and Pandemics

Technologies in earlier pandemics

"A pandemic is the worldwide spread of a new disease. An influenza pandemic occurs when a new influenza virus emerges and spreads around the world, and most people do not have immunity"[6]. The world has seen several pandemics in the past, which are indicated in the table below. The development of science and technology and their application to health care was rare in earlier times.

Table 1. Global pandemics

The Plague of Justinian
Black death
Smallpox (15th–17th centuries)
Cholera (1817–1823)
Spanish Flu or H1N1 (1918–1919)
Hong Kong Flu or H3N2 (1968–1970)
HIV/AIDS (1981 — present)
SARS (2002–2003)
Swine Flu or H1N1 (2009–2010)
Ebola (2014–2016)
Coronavirus, or COVID-19 (2019 — present)

In contrast, with today's pandemic, COVID-19, the genome was sequenced within a short span of time after the disease spread in the Chinese city of Wuhan. Scientists in China demonstrated that it was a totally new virus, despite being closely related to the coronavirus (CoV) that led to severe acute respiratory syndrome (SARS).

[6] What is a pandemic? Available at: https://www.who.int/csr/disease/swineflu/frequently_asked_questions/pandemic/en/ (accessed: 23.03.2020)

Pandemics in India

Prior to the COVID-19 pandemic, India has encountered numerous pandemics and epidemics like influenza, cholera, dengue, smallpox and others throughout history. While some could be eradicated, others posed a public threat. Some of the persistent causes of these pandemics were lack of sanitation, incompetent health care, and malnutrition. While vector-borne outbreaks attributed to the tropical climate and seasonal rains[7]. The two primary pandemics in Indian history were the recurrent cholera outbreaks in the 19th century and the Spanish flu of 1918.

In the 19th century, six major cholera pandemics broke out in 1819 to 1899. The first pandemic in 1817 was probably the most terrifying when the first case was witnessed on August 23. The worst affected people were the poor and slum- dwellers.

Influenza, caused by the H1N1 strain of influenza and also known as the «Spanish Flu of 1918–1919", caused approximately 20–50 million deaths worldwide. The disease spread globally, and India was assumed to be the epicentre. Crucial factors leading to the brutality and spread of the flu were the higher virulence and rapidity of the virus strain along with the humidity caused by monsoons. It spread quickly in India and distressed the economy. Social distancing was the only well recognised way to reduce the effects of earlier pandemics.

During all of these earlier pandemics, India had been following the British patenting system where IPR laws were stringent which led to a stringent patenting regime. Product patents were challenging to acquire. Furthermore, India practised a traditional or alternative medicine system.

COVID-19

COVID-19 is a communicable disease caused by a recently discovered coronavirus that originates from a virus family that also causes Severe Acute Respiratory Syndrome (SARS) and the common cold. COVID-19 virus infection in most people causes mild to moderate respiratory illness.

Common symptoms of the disease include:

Fever
Dry cough
Fatigue

[7] Mehta K. What we can learn from earlier pandemics in the history of India. Available at: https://www.timesnownews.com/india/article/what-we-can-learn-from-earlier-pandemics-in-the-history-of-india/574255 (accessed: 23.03.2020)

Less common symptoms are:
- Aches and pains
- Sore throat
- Diarrhoea
- Conjunctivitis
- Headache
- Loss of taste or smell
- Rash on skin
- Discolouration of fingers or toes

Less prevalent serious symptoms include:
- Difficulty breathing
- Shortness of breath
- Chest pain or pressure
- Loss of speech
- Loss of movement [Wu Y. et al, 2020: 217–220; Huang C. et al, 2019]

Role of data-centric technologies in pandemics

Data will remain significant for thousands of years. It was as important many years ago as it is today. Data collection methods and techniques continue to improve. Each day we open our eyes, and we are flooded with information about the world around us, which gives us the perspective we need to keep moving. This process of collecting data about the world around us gives us an idea about how to get what we want. In a similar manner data-driven technology help us obtain data and help to put it into a perspective we can apply in order to envision a clear path from Point A to Point B.

Although data-driven decision making has existed for many years, several new technologies are coming out of the woodwork that have begun changing the game.

Data-driven technologies are crucial in pandemic responses. Population and individual data advance the investigation and identifications of disease, understandings and testing of treatments, and execution of public health measures. The Covid-19 pandemic has established a host of data-intensive initiatives, projects and schemes, which often involve pioneering uses of existing datasets, supported by rapid advances in technologies, including machine learning, and enabled through data sharing across organisations and countries, exploiting the global nature of the pandemic, an increase in public-private partnerships and worldwide collaborations.

The imperative to ensure access to data is clear but not straightforward as demonstrated by controversies relating to contact tracing apps and proposed[8] 'immunity passports'[9]. Such technologies are often developed rapidly, in conjunction with commercial organisations and with little opportunity for public deliberation over whether such uses are acceptable. Such data uses raise various important regulatory concerns, including ethical, legal and social implications for such things as privacy, trust, transparency and equality. These can have immediate and long-lasting consequences for both individuals and populations. Some of the recent data-driven technologies are based on big data, business intelligence, analytics and artificial intelligence.

Artificial intelligence (AI)

Artificial Intelligence denotes computer systems that are proficient in executing tasks such as speech recognition, visual perception, decision-making and translation that otherwise would require human intelligence. Weak AI systems are incapable of thinking for themselves but can revert to explicit situations. Robust AI systems are being developed in a way that involves learning from prior practices and while reasoning and performing like humans[10].

AI is developing so rapidly that related legal regulation is falling behind. This radical technology causing radical innovations[11] will be incorporated in nearly every area of life, and the need for legal guidance on this topic is increasing significantly, particularly as it relates to intellectual property law. Developers and inventors have gained the capacity to create machine learning technologies that can autonomously generate inventions. A new issue of inventorship has appeared, with the question being: Do computers have the

[8] Edmond C. What is an immunity passport and could it work? Available at: https://www.weforum.org/agenda/2020/06/immunity-passport-quarantine-work-covid-19/ (accessed: 11.07.2020)

[9] Among the measures being considered by governments, including Chile, Germany, Italy, Britain and the US, are immunity passports – a form of documentation given to those who have recovered from COVID-19.

[10] White House Announces New Partnership…

[11] Occasionally a technology dislocates established framework events; the technology has the capacity to redesign and refine the space and the boundary. This is a radical technology that causes radical innovations.

ability to be inventors? If not, who can claim the rights to inventions that result from AI inventors?

AI is a data-centric technology

The open-source community[12] has been the chief technology driver behind the big data push. It is a group of individuals who (often voluntarily) work together to develop, test of modify open source software products. It has provided the skills for an added data-centric approach, which is the ability to generate a working model that might predict future inferences grounded in previous actions. Adding original data improves the process. Big data signifies the volume of data that is being made daily and the speed (velocity) at which that data is generated; it also signifies diverse sorts of data formats, such as structured or unstructured, with a distinction in data quality.

AI builds on top of HPC for large-scale computer processing and on big data with the support of the open-source community. Data is the real IP and the key distinguishing factor between competitors. The algorithms used in AI are software frameworks that are formed and collectively shared by many people. The allocation of notions and perceptions is a key component of the growing success of AI.

With the democratisation of data comes the possibility for non-data scientists to gather and analyse data with little assistance and without the need for a science degree. There are abundant guides and tutorials that can be used as an introduction to working with AI. Today, the data central to AI is mostly trivial, but in the future, the data used will define triumph or disaster.

How AI is helping in the fight against COVID-19?

The Centre for Disease Control and Prevention (CDC) and the World Health Organization (WHO) have implemented analytics and big data in their attempts to review pandemics and to find a lasting solution. AI is being used as a tool in the fight against the viral pandemic. The press and the scientific community are highly anticipating that data science and AI can be used to counter the coronavirus. Michael Kratsios, the US chief technology officer, said, «with data scientists and machine language experts mining the literature compilation known as COVID-19 Open Research Dataset, experts

[12] A group of individuals who (often voluntarily) work together to develop, test, or modify open source software products.

and White House officials expect to get help developing vaccines, forming new guidelines on how long social distancing should be maintained and other insights.» In a time of crisis, Chinese tech companies such as Alibaba and Baidu are offering free AI technologies and computing capabilities in order to aid public research institutions and buy time to combat the coronavirus. AI has also helped on the frontline. Chatbots lessen the pressure on hospital and government personnel by robotically answering queries from members of the public, and even counselling individuals about whether they need to undergo screening in hospital or stay at home for a 14-day quarantine. In the face of an abrupt attack from COVID-19, China's ability to adjust and fight back with AI is an indication that the country's investments in AI and related technologies are paying off. This is the first time that AI has been used so extensively to combat a pandemic. Without AI[13], the spread of the novel coronavirus [Cutillo C. et al, 2020: 1–5] would have been much quicker and more damaging[14]. Table 2 below provides detailed description of various companies and their efforts to combat COVID-19.

The COVID-19 detection neural network (COVNet), a deep learning model, was developed to extract visual features from Computed Tomography (CT) exams to detect and diagnose the presence of the COVID-19 virus[15, 16, 17, 18, 19, 20] [Li L. et al, 2019]. As the world races to find a cure for Covid-19, a Mumbai-based data scientist and his team have discovered three molecular

[13] Ratnam G. Government Technology. Available at : https://www.govtech.com/products/Can-AI-Fill-in-the-Blanks-About-Coronavirus-Experts-Think-So.html (accessed: 25.03.2020)

[14] Senior A. et al. Deep Mind. Available at: https://deepmind.com/blog/article/AlphaFold-Using-AI-for-scientific-discovery (accessed: 25.03.2020)

[15] Chun A. Available at: https://www.scmp.com/comment/opinion/article/3075553/time-coronavirus-chinas-investment-ai-paying-big-way?fbclid= IwAR3JdxPGOGaZ641HBCA-t2aasnXM9VgOSSZMYCtSfb2eGZDinOOpSWyJeVo. (accessed: 25.03.2020)

[16] Sagar R. 11 Ways AI is helping fight Coronavirus. Available at : https://analyticsindiamag.com/ai-corona-covid19-fight-deepmind-alibaba-baidu-algorithm/ (accessed: 01.06.2020)

[17] Yakobovitch D. Medium. How to fight the Coronavirus with AI and Data Science. Available at: https://towardsdatascience.com/how-to-fight-the-coronavirus-with-ai-and-data-science-b3b701f8a08a (accessed: 01.06.2020)

[18] Imaging Technology News. Researchers use AI to detect Covid -19. Available at : https://www.itnonline.com/content/researchers-use-ai-detect-covid-19 (accessed: 01.06.2020)

[19] Johnson A. How Artificial Intelligence is aiding the fight against Coronavirus. Available at: https://www.datainnovation.org/2020/03/how-artificial-intelligence-is-aiding-the-fight-against-coronavirus (accessed: 01.06.2020)

[20] Scedullari M. Five Companies Using AI to fight Coronavirus. Available at : https://spectrum.ieee.org/the-human-os/artificial-intelligence/medical-ai/companies-ai-coronavirus (accessed: 01.06.2020)

compounds with the help of AI; it is claimed that these compounds can be synthesised and tested more in order to find a novel drug to fight Covid-19.

Table 2. Description of various companies and their efforts to combat COVID-19

Organisation	Attempt/ Solution to combat Covid-19
DeepMind	AlphaFoldSystem — used to predict the protein structure that may help in research
AliBaba	The organisation claims that its new AI system can detect coronavirus in CT scans of patients' chests with 96% accuracy in a record time of about 20 seconds.
Baidu research	Their team has released a tool — LinearFold — which has the ability to reduce 2019-nCoV prediction time to 27 seconds from 55 seconds. This may help reduce prediction time for the virus and accelerate drug discovery.
Harvard Medical School	John Brownstein of Harvard Medical School is associated with an International team that is deploying machine learning to skim through social media data from official public health channels and data from healthcare providers in order to prepare real-time health analytics of the outbreak.
BlueDot Surveillance	This organisation has also contributed by collecting disease data from various online sources, and hence deploying airline flight information in order to generate predictions about where infectious diseases may appear next; air routes are a common disease vector.
Insilico	Insilico Medicine is using Generative Adversarial Networks (GANs) to filter molecule designs.
inferVision	Doctors in China have been using a tool to assist them in quickly diagnosing potential coronavirus patients. This AI-based software is called inferVISION, and can quickly highlight potential troubling cases in record time. It deploys NVIDIA's Clara SDKs, which is NVIDIA's AI healthcare application framework for AI-powered Medical Imaging.
BenevolentAI	With the aid of BenevolentAI's software, researchers have identified a possible drug called 'Baricitinib'.
SenseTime	Application of AI to scan faces of people with masks. Contactless identification of patients using their temperature detection software in parts of Beijing, Shanghai and Shenzhen
Pudu Technology, Micro-MultiCopter	The companies' drones are deployed to monitor the outbreak in various parts of China
UVD Robots	Using robots to disinfect patient rooms with zero human interference

CORD-19 dataset description

In response to the COVID-19 pandemic, the White House and an alliance of leading research groups have prepared the COVID-19 Open Research Dataset (CORD-19). CORD-19[21] is a dataset of 134,000 scholarly articles about COVID-19, SARS-CoV-2, and related coronaviruses; 60,000 of the articles have full text. This dataset is freely available to the global research community. Recent advances in natural language processing and other AI techniques can be applied to the dataset as a way of generating new perspectives to support the continuing fight against this infectious disease. There is increasing urgency for these tactics given the rapid development of the novel coronavirus literature, which makes it difficult for the medical research community to keep up.

Applications of AI to COVID-19

The applications may be categorised as follows:
Detecting and diagnosing infections
Monitoring treatment
Tracing contact of individuals
Predicting cases and fatality
Assistance in developing drugs and vaccines
Reducing the workload of healthcare workers
Preventing disease occurrence

Artificial intelligence is a tool that can benefit in its ability to recognise early coronavirus infections and also help with intensive care of infected patients. It can advance stable treatment and decision making by developing useful algorithms. AI helps treat patients infected with COVID-19 and ensures proper health monitoring for them. It can trace the COVID-19 crisis at diverse levels, such as through molecular, medical and epidemiological applications. It also helps ease research on this virus by analysing available data. AI can support the development of proper treatment regimens, inhibition strategies, as well as drugs and vaccines.

The drawbacks of using the technology are simply legal and intellectual property rights issues with AI.

[21] COVID-19 Open Research Data Challenge (CORD-19). Available at: https://www.kaggle.com/allen-institute-for-ai/CORD-19-research-challenge (accessed: 01.06.2020)

Intellectual property

Intellectual property (IP)[22] are the creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce. IP is protected in law by, for example, patents, copyright and trademarks, which enable people to earn recognition or financial benefit from what they invent or create. By striking the correct balance amid the benefits of innovators and the wider public interest, the IP system aims to create an environment in which originality and novelty can flourish.

AI-generated works[23] and IPR

Owners of AI-generated work

To answer the question about the ownership of AI-generated works, we need to know who is the author of a work is. The author is the person who creates the work. The creation of a work is essentially a human activity.

In most countries' jurisdictions, if no human author can be identified for a work, no copyright will exist, and hence it will fall into the public domain. There may be copyright in an AI algorithm itself; for example, computer programs are protected by copyright, which are separate works whose authorship (and ownership) is different from the work it creates[24].

In the UK, lawmakers in Parliament wanting to encourage investment in AI in the 1980s formed a category of «computer-generated works» in section 9(3) of the Copyright Designs and Patents Act 1988 (CDPA). These are works that are generated by a computer with no human author. The author is therefore considered to be the person «by whom the arrangements necessary for the creation of the work are undertaken.»

Overlaps between AI and IP can be discussed as:

AI as a technology that may contribute to managing IP rights

IP as a regime for the shield of AI

IP as an obstacle to the transparency of AI systems

[22] What is Intellectual Property. Available at: https://www.wipo.int/edocs/pubdocs/en/intproperty/450/wipo_pub_450.pdf (accessed: 01.06.2020)

[23] Artificial intelligence is being used to generate works in music, journalism and gaming. These may be termed as AI generated works. Available at: https://www.wipo.int/wipo_magazine/en/2017/05/article_0003.html#:~:text=Artificial%20intelligence%20is%20already%20being,used%20and%20reused%20by%20anyone (accessed: 01.06.2020)

[24] Lexology AI and copyright authorship: still mind over matter? Available at: https://www.lexology.com/library/detail.aspx?g=404f4311-bcc4-4049-b62e-d521ccca90e1 (accessed: 05.06.2020)

Hence, the relationship between AI and IP is mutual: IP impacts AI and AI affects IP. Patent and copyright codes are the most relevant systems of protection for AI, mainly when AI can freely generate inventions. There are numerous cases of applications for patent protection where applicant have named an AI application as the inventor. The question that arises in the scenario is whether the law should permit an AI application to be the inventor or should whether it should be obligatory for a human being to be named as the inventor. Should the law give suggestions on how to decide the human inventor or let the stakeholders decide through private arrangements? Additionally, the main question is who should be documented as the owner of a patent concerning an AI application? Do current legal provisions suffice to consider the specificities of inventions generated by AI, or should explicit legal provisions be introduced? Should the availability of patent protection of autonomously generated inventions by an AI application be excluded by the law?

Additionally, one can raise the question of the explanation of patentability, specifically an inventive step or non-obviousness. In particular, what art does the standard refer to? Finally, the condition of disclosure could be challenging for an invention generated by an AI application. Given that the algorithms of machine learning change over time, how can the condition of disclosure be fulfilled? Must the data used to train an algorithm be revealed or defined in the patent application? Based on the answers to these questions, lawmakers may be led to consider that a sui generis system of IP rights for AI-generated inventions should be developed to adjust innovation incentives for AI[25].

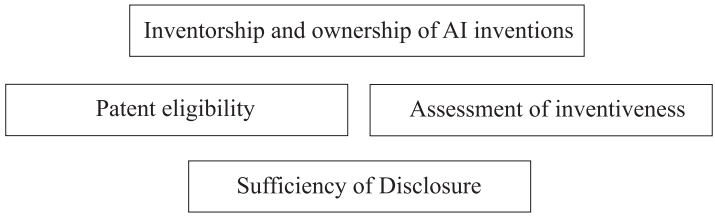
The promise of AI does not exist exlusively in either machines or people; instead, it arises from their interplay. AI-generated work and inventions pass the Turing Test, but AI's real test is whether legal architecture built around the foundation of human artistic and advanced endeavours may hinder its evolution. Copyright law and patent law must address this reality head-on [Lim D., 2018: 813].

Who is the owner of an AI-generated invention?

AI poses 4 challenges to patentability

The four challenges outlined above are further discussed and elaborated below:

[25] WIPO. Conversation on Intellectual Property and Artificial Intelligence: Draft Issues Paper on Intellectual Property Policy and Artificial Intelligence. WIPO IP/AI/2/GE/20/1, 13 December 2019. Available at : https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/pdf/ms_switzerland.pdf (accessed: 05.06.2020)



Inventorship and ownership of AI inventions

An inventor is a person who creates or generate an invention by applying their creative action. It can be proposed that an inventor is a human being or a legal person.

Patent eligibility

It has been debated whether AI-generated inventions are computer-implemented inventions.

Assessment of inventiveness

Application of AI may cause an upsurge in skilled people's knowledge, which might be problematic to establish. Skilled people should form an interdisciplinary team that is capable of using AI. A policy question arises here: Can a machine be acknowledged as a skilled person?

Sufficiency of disclosure

It is believed that an invention must be appropriately disclosed in a manner that is clear and complete by a person skilled in the art. In the case of AI, the following problems arise:

Describe how an AI algorithm functions is challenging.

Protecting the method as well its generated output is challenging[26].

Practically no law exists for the patentability of AI-generated inventions. All jurisdictions require patent applications to reveal an inventor who is a natural person. This prerequisite is intended to protect and recognise the rights of human inventors. However, inventors do not inevitably own their patents; in fact, patents are usually owned by businesses. Ownership rights may be passed on to a legal entity from an individual by means of contractual assignment or otherwise by the benefit of the law. It may be considered as an example that in numerous jurisdictions, ownership is transferred mechanically to an employer if the invention is formed inside the scope of employment. Additionally, even if an inventor does not possess a patent,

[26] Heli Pihlajamaa Director Patent Law, Dir. 5.2.1 Committee on Patent Law, 20 February 2019. Legal aspects of patenting inventions involving artificial intelligence (AI) Summary of feedback by EPC contracting states.

people are assured of receiving due credit given laws requiring a natural person to be recorded as an inventor. Nevertheless, the above laws were created without accounting for the prospect of creative activity by machines.

Legal personhood of AI

The legal personhood of artificial intelligence [Solum L., 1991: 1231] can be addressed by considering three relevant background issues [Kurki V., 2019]. These focus on the moral value of AI, i.e., ultimate-value context; on whether AI can or should be held accountable (responsibility context); or on whether AI can obtain a more sovereign role in commercial transactions (commercial context). This paper claims that strong AI, which is as proficient in executing parallel tasks as human beings, can undoubtedly function as legal persons regardless of whether such AI is worthy of moral consideration. If AI can function as a legal person, it can be granted legal personhood on somewhat similar grounds as a human. The majority of this chapter focuses on the role of AI in commercial contexts, and new theoretical tools are proposed that would help distinguish among different legal personhood arrangements for commercial AI.

DABUS Patent Application

In November 2019, a patent application was filed with the European Patent Office. The applicant claimed the following:

The patent application specified 'DABUS' (which is a type of connectionist AI) to be chosen as 'the inventor'.

The applicant would obtain the right to European Patent for the solitary motive that he is 'the employer' as well as 'the successor in the title'.

European Patent Office (EPO) — Decision on DABUS

The EPO was rejected the DABUS patent application on the basis of noncompliance with Article 81 and Rule 19 of the European Patent Convention. To be more precise, the office emphasized that the prevailing legal framework of IP is applicable only to legal persons, natural persons, or bodies' equivalent to legal persons. Clearly, 'artificial intelligence' does not fall within any of the categories mentioned above.

The decision, in brief, rested on the concept of 'legal personhood' and how it is not applicable to 'AI Systems' since it has not been accredited the same by virtue of any legislation or jurisprudence. Furthermore, the judgement also drew that 'AI Systems', having no legal personhood, have no rights; consequently, they cannot have legal title over their output or invention or transfer it or even be employed for the sole reason of absence of rights that flow from legal personhood[27].

IPR for AI-generated works

Uncertainties in AI-generated works

Since AI systems are not natural persons and AI-generated works are regarded as computer-generated under Section 2(d) of the Copyright Act, ambiguity exists regarding the identification of the «person who caused the work to be created». Is it the person who created the AI system or the person who programmed it? Should it be the owners of the AI system or companies and financial stockholders in the AI sector? Or will it be the end-user who uses the AI system to produce a certain output? The lack of accuracy and the particulars involved in defining the author of an AI-generated work make it problematic to determine the 'first owner' of copyright under Section 17 of the Copyright Act.

Under Indian copyright law, in some situations copyright ownership may be approved for non-natural, legal or juristic persons (e.g., companies, organisations or the government). Consequently, if impending AI systems are recognised as legal or juristic persons, they could be granted copyright ownership in some circumstances; however, this would create challenges relating to copyright transferability and the financial and commercial aspects of copyright ownership.

Since AI systems are not considered natural persons (thereby removing the issue of affording AI systems copyright authorship), the lines appear to be distorted concerning the acknowledgement of AI systems as legal persons.

Indian courts have yet to address these intricate matters concerning AI-generated works and copyright authorship and ownership.

[27] Shah S. Dabus Machine: The Harbinger to Debates on Artificial Intelligence as an 'INVENTOR' under patent laws. Available at: http://rsrr.in/2020/02/22/dabus-machine-the-harbinger-to-debates-on-artificial-intelligence-as-an-inventor-under-patent-laws/ (accessed: 12.06.2020)

IPR for AI-generated works under global jurisdiction

Name of the National Jurisdiction	Comments
US Patent and Trademark Office (USPTO)	An AI system cannot be credited as an inventor in a patent[28]
UK Intellectual Property Office (UKIPO)	AI cannot be considered as an inventor[29]
Europe Patent Office (EPO)	An AI entity cannot be an inventor[30]
India	AI cannot be an inventor according to Section 3(k) of the Indian Patent Act, mathematical and business methods, computer programs or algorithms are defined as non-patentable[31]

Copyright law and AI-generated works

AI-generated works and copyright law have been discussed quite frequently. In 1988, the United Kingdom became the first country to offer explicit copyright protection for AI or «computer-generated» works. When a copyrightable work is created, but no natural persons are found to be suitable as authors, the «producer» of the work is considered to be the author.

On the other hand, the United States Copyright Office (USCO) has adopted the reverse approach. Since 1973 the office has practically applied a «human authorship policy[32]» [Ginsburg J., 2018: 131–135].

The human authorship policy was seen with the «Monkey selfies» case Naruto v.Slater[33]. This case concerned a sequence of images clicked by an Indonesian crested macaque named Naruto. People for the Ethical Treatment of Animals (PETA) litigated on Naruto's behalf, using the argument

[28] Porter J. The Verge,: US patent office rules that artificial intelligence cannot be a legal inventor. Available at: https://www.theverge.com/2020/4/29/21241251/artificial-intelligence-inventor-united-states-patent-trademark-office-intellectual-property (accessed: 12.06.2020)

[29] McKenna C. Lexology : UK Intellectual Property Office finds that patent law does not cater for inventions created by AI machines and calls for debate inventor. Available at: https://www.lexology.com/library/detail.aspx?g=ad32b072-23d3-4db4-95f5-bb71c0826dc5 (accessed: 10.06.2020)

[30] Olvi G., Massalongo S. Mondaq. Italy: Artificial Intelligence: What kind of IP Protection. Available at: https://www.mondaq.com/italy/trade-secrets/767332/artificial-intelligence-what-kind-of-ip-protection?login=true (accessed: 01.06.2020)

[31] Lazaro L. Mondaq. India: Artificial Intelligence in the world of IP. Available at: https://www.mondaq.com/india/patent/892134/artificial-intelligence-in-the-world-of-ip (accessed: 10.06.2020)

[32] This policy forbids copyright protection in case the works are not generated by a human author.

[33] Naruto v. Slater, No. 16-15469 (9th Cir. 2018).

that he should possess the copyright to the photographs. But the case was terminated, as the United States Congress did not authorise animals to file suit under the Copyright Act. As a consequence, the advantages of the human authorship prerequisite have never been tested in court.

Patent protection for AI-generated works

Patent protection should be obtainable for AI-generated works because it will encourage innovation. The vision of holding a patent will not unswervingly motivate AI, but it will incentivise some of the people who develop, own, and use AI. Permitting patents for AI-generated works, consequently, will promote the growth of inventive AI, which will eventually lead to more innovation for society.

Patents can encourage disclosure of information and the commercialisation of socially valuable products. Patents for AI-generated works will achieve these targets as well as any other patents. On the other hand, not permitting protection for inventions generated by AI would lead to businesses not being able to deploy AI to invent. The inability to submit a filing based on an AI-generated invention would cause situational gamesmanship with patent offices.

Apart from providing fortification for AI-generated inventions, AI should be listed as an inventor when it is inventing, as this would shield the rights of human inventors. Listing a person as an inventor of an AI-generated invention would cause no harm to AI, which ultimately is not interested in being recognised. On the contrary, permitting people to own credit for work they have not done would undervalue human inventorship[34]. It would put the work of a person who simply asks AI to resolve a problem on an equal foothold with someone who is lawfully and justifiably inventing something new. AI can definitely not own a patent. AI systems have a dearth of both moral and legal rights; hence, they do not possess the ability to own property. There would be no advantages or benefits, but substantial costs in order to allow AI to have ownership. Again, citing an AI as an inventor does not mean providing rights to machines, but it would lead to protection of the moral rights of traditional human inventors and the verac-

[34] Inventorship is an important concept in patent law. Inventors are those who contribute the ingenuity necessary to create an invention. Quinn G. Inventorship 101: Who are Inventors and Joint Inventors? Available at: https://www.ipwatchdog.com/2018/03/09/inventorship-joint-inventors-co-inventors/id=94592/ (accessed: 10.06.2020)

ity of the patent system. It is often the case that the inventor of a patent is not its owner[35][Feldman R., Thieme N., 2019]; [Firth-Butterfield K., Chae Y., 2019].

Technology has a propensity to advance more rapidly than the law. As AI-based technologies and machine learning continue to be considered other industrial areas, the need for legal supervision on this subject will increase exponentially[36] [Fenwick M. et al, 2016]. The prime area of legal study that is disposed to the range of legal intricacies associated with this technology is the field of intellectual property (IP). While much has been discussed about the effects of computer-authored work in copyright law, less discussion has taken place regarding how analogous technologies will dislocate patent law [McLaughlin M., 2018]. «As developers gain the ability to create machine learning technologies capable of independently generating inventions, experts must examine the legal scope of inventorship by looking toward the text of the constitution, judicial decisions, legislative actions, and the philosophical reasoning behind such jurisprudence.» [Fisher W., 2001].

Today, machine learning can be used for computer-generated patent claims; this computer-generated content has a wide variety of latent applications that could bring chaos to the patent legal system [Plotkin R., 2009]. There have been no known instances of an independently computer-generated invention. These expansions raise the following question: If machines can compose patentable subject matter entirely independent of human intervention, should they be granted property rights and under what circumstances should these rights be granted?

A vital understanding of inventorship will be assessed as society looks toward the predictable depths of the «artificial invention age» in order to determine whether inventions that are computer-assisted or computer-generated and made with the aid of AI should result in patents. To evaluate this subject, two issues must be considered. First, a range for analysing the degree of human intervention that occurs throughout a given inventive process will be established. Machine learning could be an enormously useful instrument to assist inventors. In addition, it would enable computers

[35] Abott R. The Artificial Inventor Project. Available at : https://www.wipo.int/wipo_magazine/en/2019/06/article_0002.html#:~:text=People%20have%20claimed%20to%20have,in%20such%20a%20patent%20application.&text=However%2C%20these%20laws%20were%20created,of%20inventive%20activity%20by%20machines (accessed: 10.06.2020)

[36] Heath N. What is AI? Everything you need to know about Artificial Intelligence. Available at: https://www.zdnet.com/article/what-is-ai-everything-you-need-to-know-about-artificial-intelligence/ (accessed: 05.06.2020)

to make inventions without any human intervention or influence. Computer-assisted and computer-generated inventions could also be examined through a philosophical lens to determine the point along the spectrum at which human intervention is so minimal that the right to a patent is relinquished.

«The time has arrived for our federal courts and legislature to begin more carefully considering how computer-generated inventions should be treated in the patent ecosystem» [Hattenbach B., Glucoft J., 2015: 19, 32].

Can the Copyright Act handle the future of AI systems?

As AI systems develop competences conventionally attributed to humans, such as creativity and autonomy, predetermined notions about human intelligence and creations of the mind are defied, which in turn puts pressure on prevailing legal frameworks to grow.

With the decrease in human intervention in AI systems and AI-generated works, policymakers worldwide may ultimately have to create systems and codes that consider the moral, commercial and accountability aspects of copyright protection in AI-generated works as well. It would be interesting to see how the law evolves to protect and encourage AI developers and users on the one hand and AI systems and their potential juristic personality on the other.

One of the prime objectives of this research paper is to determine the impact of International and National laws and treaties on IP rights for AI-generated solutions for the pandemic

«WIPO is an agency of the United Nations that represents the global forum for IP services, policy, information and cooperation for its Member States.» WIPO champions the expansion of a balanced and effective international IP system that allows innovation and creativity for the benefit of all. The scope of this mandate is the objective of promoting invention and creativity for the economic, social and cultural development of all countries; the Member States have requested that WIPO provide a forum leading the discussion on AI and IP policy.

The ongoing WIPO conversation on AI policy is the first step in this process.

A distinction must be made between human-created works or inventions and machine-created works or inventions. The works and inventions created by humans are protected by the prevailing IP frameworks, which

include patents, copyright, industrial designs, and trade secrets. The debatable question is whether these existing frameworks and systems need to be altered for works and inventions by machines. In broad terms, the deliberations regarding machine-made inventions or works focus on:

Possible protection for the actual machine created work/invention itself. This leads to an emphasis on the question of whether AI can be an inventor or creator within the current IP frameworks.

Possible protection of AI algorithms and software.

Possible rights regarding the primary training data and data inputs.

There is also a debate concerning the line between human-made and machine creation, i.e., what amount of human input or supervision may be required to fall within one or the other. The WIPO Technology Trends 2019[37] report on artificial intelligence offers data and analysis that classify key trends, crucial players and the geographical spread of AI-related patents and scientific publications.

Policy recommendations and alternative mechanisms

Patent pooling

«A patent pool is well-defined agreement between two or more patent owners to license their patents to one another or to third parties.» Patent pools mostly come into view when some inventor gets trapped in a multifaceted technology that needs a complementary patent to achieve efficacy; however, the complementary patent belongs to another patent holder.

Patent pools are may be termed as private arrangements that allow participants to function under each other's' patent rights in order to manage and control the pooled rights on a central basis, as well as to grant licenses of the pooled patents to third parties, with the profits split amid the pool members according to a settled formula. Patent pools have existed for more than a century in various industries ranging from oil refining, to aircraft to semiconductors and even digital media. In all of these cases, pools have allowed the efficient alliance of patents in a manner that has eased licensing and commercialisation.

[37] WIPO Conversation on Intellectual Property and Artificial Intelligence. Draft Isues Paper on Intellectual Property Policy and Artificial Intelligence, prepared by WIPO Secretariat. Available at: https://www.wipo.int/meetings/en/details.jsp?meeting_id=51767 (accessed: 10.06.2020)

Patent pools have also been recommended as instruments to address severe public health emergencies such as disease outbreaks and pandemics. Patent pooling structures were vigorously deliberated and considered in the SARS outbreak in 2002–2003, the H5N1 influenza outbreak in 2005, and the H1N1 influenza pandemic of 2009. However, regardless of the apparent need for aggregation of distributed patent rights in order to battle these diseases, patent pools were never formed. The reason that patent pools may not have effectively formed in these areas may be associated with antitrust law. A patent pool essentially comprises a variety of patents held by diverse owners. But when a pool aggregates rights including technologies that may be substituted for one another, for example, patents covering various types of vaccines, innovation could be abridged (i.e., why attempt to develop an enhanced vaccine when all vaccines are licensed under the pool?). When pooled patents are complementary (e.g., many patents casing aspects of the equivalent vaccine), pools are regarded as enhancing proficiency and innovation. For this reason, most antitrust enforcement agencies harmonise over the fact that the patents included in a pool should mostly be complementary and not substitutes for each another.

In 2010, the Unitaid initiative of the United Nations World Health Organization (WHO) formed the Medicines Patent Pool (MPP). The mission of MPP is to cumulate patents, clinical trial data and additional IP relating to HIV/AIDS, Tuberculosis and Hepatitis-C medications. It also aims to make all these available at minimal or no cost to manufacturers that promise to produce and offer drugs at wholesale prices to users in low-income countries[38, 39].

MPP acts as a clearinghouse or intermediary that obtains inbound licenses from prepared IP holders and then leases those rights to generic drug manufacturers operating in developing nations. These licenses can be royalty-bearing or royalty-free, are available on an *a-la-carte* basis, and do not essentially combine the rights licensed to MPP (which avoids some of the antitrust issues).

Advocates have proposed that an MPP-like patent pool be formed to fight the Covid-19 pandemic. The President and Health Minister of Costa

[38] Patent Pooling: A boon amidst COVID-19 Pandemic. Available at: https://www.lexology.com/library/detail.aspx?g=ba09f470-2269-4ae3-92c0-c52f769633ac (accessed: 10.06.2020)

[39] OECD. Why Open Science is critical to combatting Covid-19. Available at: http://www.oecd.org/coronavirus/policy-responses/why-open-science-is-critical-to-combatting-covid-19-cd6ab2f9/ (accessed: 10.06.2020)

Rica requested that the WHO «undertake an effort to pool rights to technologies that are useful for the detection, prevention, control and treatment of COVID-19.» According to the application, the projected pool «should include existing and future rights to patented inventions and designs, as well rights to regulatory test data, know-how, cell lines, copyrights and blueprints for manufacturing diagnostic tests, devices, drugs, or vaccines. It should provide for free access or licensing on reasonable and affordable terms, in every member country.»

An IP pool administered by a United Nations agency, especially if it is truly global in scope, could lessen many patent-related obstacles to the development, production and distribution of vaccines, diagnostics, therapeutics and equipment in the fight against Covid-19. To ensure that such a pooling effort is operative, the WHO must act quickly and conclusively in defining the details of the proposed arrangement and in persuading patent holders in both the public and private sectors to join the effort.

If executed properly, a COVID-19 patent pool could reassure innovation and advance the accessibility of life-saving medications, boost further innovation, as well as restructure and quicken the adoption of diagnostic standards.

Patent pooling can quicken the development of a medicine for COVID-19 while being clear about all the legalities, patent rights and bringing together big pharma companies with generics companies in order to create the required medicine(s) for low- and middle-income countries. It would be a win-win situation, because the patent holders will receive royalties for their innovations, thus upholding their income influx while low- and middle-income countries would gain access to medications at reasonable prices[40].

Compulsory licenses

The Bayer vs Natco[41] case for a compulsory licence (CL) for a drug to treat kidney and liver cancers was among the first CL cases in India. Leena Menghaney of Médecins Sans Frontières' Access Campaign said it in a public statement. This decision affirmed that courts can and should act in the

[40] UNESCO. Open Access to facilitate research and information on COVID-19. Available at: https://en.unesco.org/covid19/communicationinformationresponse/opensolutions (accessed: 10.06.2020)

[41] 2013 Indlaw IP AB 20.

interest of public health in the case of pharmaceutical products.» The primary goal is to strike a balance between patents, patients and profits. Past cases in the emerging economic power of India have raised the challenge of striking a balance between public and private interests where, unexpectedly, the vast mainstream is still not protected by health insurance and where most people have to pay for their own treatment.

Open science and open access technologies

In the coronavirus (COVID-19) pandemic, open science policies can eliminate obstacles to the free movement of research data and ideas, and thus fast-track the pace of research critical to battling the disease. Although the global sharing of research data and collaboration have reached extraordinary levels, challenges remain. There are trust issues with data, lack of specific standards, co-ordination and interoperability, as well as data quality and interpretation. To reinforce the contribution of open science to the COVID-19 response, policymakers must conform to acceptable data governance models, interoperable standards, sustainable data-sharing agreements involving the public sector, private sector and civil society, incentives for researchers, sustainable infrastructure, human and institutional capabilities and mechanisms for access to data across borders.

There is a need for science communication to be transparent and open, without invading people's privacy. It is imperative to control scientific innovations and support principles of openness and inclusiveness in processes that generate solutions to severe health hazards that are likely to bring substantial adversity to humanity.

Scientific communication, research and data offer key structures for creating novel scientific knowledge. It is imperative to recognize that the creation of new scientific knowledge to handle the urgent risk management rests upon creating an open and level playing field and providing absolute access and allocation of scientific contents, technologies and processes to the entire scientific community from developed and developing countries. Access to verified and peer reviewed data, journal articles and laboratory log books is thus essential to finding a remedy to the ongoing crisis. Proven information and scientific research can also keep the public updated on the situation and dispel fears that may be caused by a lack of awareness or misinformation.

Discussion and conclusion

Artificial intelligence technologies, despite having been developed through R&D and related investments, use both primary and secondary open knowledge sources and public domain knowledge for machine learning and therefore act as a data-centric technology. AI technological applications are but virtual platforms that aggregate knowledge, which constitutes the core of big data. Hence, the data that are studied by AI technologies are not the IP of the AI machine as such but of the human generators of the related knowledge (COVID-19 in this case). They are an algorithmic compilation of mined information from the literature that is published by scientists, research scholars, medical practitioners, survey analysts, pharmaceutical experts, etc. into a dataset of filtered and enhanced knowledge. It is this enhanced dataset that could possibly give the AI domain holders (individual or public institutions) a variety of scientific knowledge domains and deeper insights into COVID-19 virus strains that are intended to ultimately develop a vaccine, which is in the public interest. This is indeed an AI-enabled 'deductive methodology' where complex algorithms from diverse sources of information give rise to effective immunisation against the COVID-19 virus strain. Would it be a mistake to consider AI as a tool of research methodology? If so, the IP owner of the AI algorithm that has been used for this specific 'AI induced work' can claim to be a part of the research but not as an owner of the work as such. The mentioning of the AI research tool is also deemed ethical. The authors of the AI induced work are those who have contributed the algorithms i.e., the original authors are multiple individuals or participating research institutions that have either participated in, hosted or funded the crucial preliminary research and have contributed much important algorithmic data which forms the core of the big data on COVID-19. Therefore, the IP ownership of any resulting primary knowledge that has been induced by AI technologies must trickle down to its contributing individuals and institutions. This is because the AI systems can neither defend the knowledge produced by their algorithms nor can a single human or a private entity claim IP ownership for the aggregation of knowledge for having operated or programmed the AI systems at the backend. Therefore, this gives rise to the collective IP ownership of the knowledge on COVID-19 through 'patent pools' where AI has enabled effectiveness in identifying creators of knowledge and effective knowledge creation in such a short span of time and that in a foolproof and trans-

parent manner where every contribution is acknowledged for its share of primary data. This can be portrayed as an example of cooperative knowledge sharing that can be channelled for the betterment of the 'commons'. Whether or not the AI technology holders socialise or commercialise this 'enhanced knowledge' post aggregation is a question for ethics and morality. But a critical scenario where a vast number of lives are lost and the global economy is in continuous decline would need a change in perception on the usage of AI-induced knowledge irrespective of IP ownership concerns. The COVID-19 pandemic provides an opportunity for AI-induced works in the advanced areas of bioinformatics and virology wherein a partial automation process (AI induced) in vaccine manufacturing gives rise to a paradigm shift in the field of advanced medical science, which is fuelled by machine-learning with as much practical effectiveness as one can imagine. Combining this aspect with the growing importance and relevance of affordable 'universal healthcare' and public health at the crucial juncture of the COVID-19 pandemic brings us to the theory of utilitarianism wherein maximum benefits are accorded to the maximum number of people. The magnitude of the pandemic requires the unified effort of all stakeholders across the globe in arriving at an ever-lasting vaccine solution of at the shortest possible interval. This must be void of any private interests for commercialisation, giving AI the ability to lead global institutions and governments in terms of inclusivity, accountability and transparency in this regard towards affordable vaccination.

According to the World Intellectual Property Organisation (WIPO) Technology Trends report, which considers AI patents for the world in order to paint an inclusive picture pertaining to growth in the field, almost half of the AI patents were filed after 2013, with the numbers totalling around 170,000.

The report also states how India has developed among the top 10 countries for filing AI patients. According to the report, India ranked eighth in 2015 and says that the country has seen a high rate of annual growth in this respect in the previous years.

To claim IP protection, Indian companies should follow these guidelines:

Define the hardware, for example, sensors, servers and the computer system in addition to AI algorithms in the patent.

Describe the procedure or working method used for developing the AI application.

Refrain from putting the spotlight only on programming codes or algorithms of the AI application.

The reason why United States Patent and Trademark Office (USPTO) looks to collect public information on AI patents is because varying levels of potential uncertainties in such patent filings exist.

The coronavirus pandemic has been unparalleled in its impact, leaving no lives unaffected since it started in late 2019.

It has affected day-to-day work, school, social gatherings, and travel, and it has produced shockwaves to the world's economy and healthcare systems. It is a once-in-a-lifetime kind of crisis occurring on the global stage.

Difficult questions based on ethical dilemmas are being raised by the same.

For different people, there are different questions.

Healthcare workers need to decide how to allocate scarce resources when treating patients suffering from coronavirus.

Government leaders need to look at the allocation of the coronavirus vaccine once it is developed and becomes available.

Businesses where revenues are falling need to decide their focus group. Should shareholders be their target group even after COVID-19?

Above are a few of the numerous ethical challenges raised by this pandemic, as stated by Wonyong Oh, Lee Professor of Strategy at University of Nevada.

In countries such as Italy, China, the United Kingdom, and Spain, frontline medical staff faced an impasse throughout the COVID-19 crisis: Which patients should be treated first when resources are strained to the limit? Should an attempt be made to save as many patients as possible, or save those with the most crucial and vital need?

From an ethical perspective, if the ethics of outcome (utilitarianism) are applied, the aim is to save the maximum number of lives, so the focus should be on patients who have better chances of healing. In contrast, if the ethics of morality (deontology) are applied, then the patients who are at risk, such as patients in serious conditions, elderly patients must be treated first.

The question remains unanswered. The important message is that it shouldn't just be left to just frontline healthcare workers. Strategies and rules can be suggested in order to ease the moral burden, so that they can better emphasise and pay attention to the treatment. Italy and the UK both offer guidelines for their health care professionals[42].

[42] Global Health New Wire. Covid-19 and the ethical questions it poses. Available at: https://globalhealthnewswire.com/policy-law/2020/04/22/covid-19-and-the-ethical-questions-it-poses (accessed: 10.06.2020)

The other question is when the vaccine is developed and made available, who would have access? The idea is if the vaccine would be first available to more susceptible people or people with high social efficacy like medical professionals? Advancement in vaccine development is vital, but once vaccines are available, the circulation of a vaccine is also an important moral question.

The masks, gloves and diagnostic kits distributed are determined by who pays the maximum amount. Hence, the supply and demand curve would not be able to create a solution to the prevailing distribution problem. If vaccines are also distributed in a similar way, poorer countries will regrettably get the vaccines last.

Richer and developed countries may attempt to stock up on vaccines for the welfare of their own citizens. They would be permitted to take this action since there is no regulatory force that requires countries that develop vaccines to share those vaccines with other countries. This is the prime reason why Bill Gates has recently lately for a global approach to combating COVID-19. He said that the vaccine should be a «global public good».

Real-time personal location data to trace and gauge the path of infection has been tried globally, especially in Asian countries like China, Korea, and Hong Kong. IT companies can track location statistics using smartphones to prevent the spread of the virus. However, this raises ethical and legal issues concerning the access to personal information.

If we look at utilitarian ethics, tracking this kind of personal data can be permitted with a belief in «maximum benefits for the greatest number.» It is for keeping society safe from infection by forgoing personal privacy. Recently, it seems that views on tracking personal information in the US. and Europe have begun to change. In several European countries, telecommunication companies have begun to use mobile phone data to fight COVID-19. In the US., Apple and Google are working together to track COVID-19 with Bluetooth. IT companies can help governments reduce the spread of the virus with their technologies. At the same time, tech companies need to balance that with protecting individual privacy, which is a new challenge.

The other main question is whether the pandemic will cause some businesses to reconsider the essential feature of the corporation?

The coronavirus pandemic has been unprecedented in its impact, leaving no aspect of life unaffected following its arrival in late 2019.

From day-to-day impacts on work, school, social gatherings, and travel, to larger shockwaves to the world's economy and healthcare systems, COVID-19 is a once-in-a-lifetime crisis on the global stage.

With such a large crisis comes even larger, albeit, difficult questions to answer.

How will corporate social responsibility change? This is another question prevailing to the pandemic. In recent years, vaccine development by pharmaceutical companies has decreased intensely. Pharmaceutical companies have also abridged their investment in generating new vaccines. The market for vaccines is minor compared to other drugs, and there is no market once the disease is over. Put simply, it's not a profitable attempt for pharmaceutical companies, which means they have no financial motivation to develop vaccines. How can this problem be addressed? Since market capitalism cannot solve it, and governments need to step in.

Sometimes, authors stated the significance of noting that every time a utilitarian solution to a dilemma is implemented, there will be greater well-being or happiness in the world. Characteristically, some people will be better off. There may be legitimate moral reasons to stray from a pure utilitarian approach, for example, in order to guard rights or endorse equality. However, seeing the alternative will help societies recognize and deliberate the necessary cost of these other ethical values[43].

References

Cutillo C. et al (2020) Machine intelligence in healthcare — perspectives on trustworthiness, explainability, usability, and transparency. *NPJ Digital Medicine*, no 1, pp. 1–5.

Feldman R. and Thieme N. (2019) Competition at the dawn of artificial intelligence. In: *Competition Law for the Digital Economy.* Cheltenham: Edward Elgar, 400 pp.

Fenwick M., Kaal W., Vermeulen E. (2016) Regulation tomorrow: what happens when technology is faster than the law. *American University Business Law Review*, no 6, p. 561.

Firth-Butterfield K. and Chae Y. (2018) Artificial Intelligence Collides with Patent Law. World Economic Forum. Available at: http://www3.weforum.org/docs/WEF_48540_WP_End_of_Innovation_Protecting_Patent_Law.pdf (accessed: 05.06.2020)

Fisher W. (2001) Theories of Intellectual Property. In: *New Essays in the Legal and Political Theory of Property.* R. Stephen, ed. Cambridge: University Press, pp. 168–199.

[43] Venkatpuram S. How Coronavirus is shaking the moral universe. Available at: https://economictimes.indiatimes.com/news/international/world-news/how-coronavirus-is-shaking-up-the-moral-universe/articleshow/74888344.cms?from=mdr (accessed: 23.06.2020)

Ginsburg J. (2018) People Not Machines: Authorship and What It Means in the Berne Convention. *International Review of Intellectual Property and Competition Law*, no 2, pp. 131–135.

Hattenbach B., Glucoft J. (2015) Patents in an era of infinite monkeys and artificial intelligence. *Stanford Technology Law Review*, vol. 19, p. 32.

Huang C. et al. (2020) Clinical features of patients infected with 2019 novel coronavirus in Wuhan. *Lancet*, vol. 395, pp. 497–506. DOI: 10.1016/S0140-6736(20)30183-5.

Hughes J. (1988) The philosophy of intellectual property. *Geo. LJ*, vol. 77, p. 287.

Kurki V. (2019) The Legal Personhood of Artificial Intelligences. In: *A Theory of Legal Personhood*. Oxford: OUP, pp. 175–189. DOI:10.1093/oso/9780198844037.003.0007.

Li L. et al (2020) Artificial intelligence distinguishes COVID-19 from community acquired pneumonia on chest CT. *Radiology*, p. 200–205.

Lim D. (2018) AI & IP: Innovation & Creativity in an Age of Accelerated Change. *Akron Law Review*, vol. 52, p. 813.

McLaughlin M. (2018) Computer-Generated Inventions. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3097822 (accessed: 23.05.2020)

Plotkin R. (2009) *The genie in the machine: how computer-automated inventing is revolutionizing law and business*. Stanford: University Press, 2009, 270 pp.

Solum L. (1991) Legal personhood for artificial intelligences. *NCL Review*, vol. 70, p. 1231.

Wu Y. et al (2020) The outbreak of COVID-19: An overview. *Journal of the Chinese Medical Association*, issue 3, pp. 217–220. DOI: 10.1097/JCMA.0000000000000270

Telemedicine: Current State and COVID-19 Lessons

Mikhail Zhuravlev

Research Fellow, Lecturer, Law Faculty, National Research University Higher School of Economics. Address: 20 Myasnitsky St., Moscow 101000, Russia. E-mail: mzhuravlev@hse.ru

Olga Blagoveshchenskaya

MA Student, Institute of Economics and Management, National Research Tomsk State University. Address: 36 Lenin Ave., Tomsk 634050, Russian Federation. E-mail: 89528075555O@gmail.com

Abstract

The pandemic is a watershed event that has prompted both an evaluation of the achievements of information and communications technology (ICT) and also a re-evaluation of the prospects for developing social processes compatible with ICT. Much has been already been accomplished in Russia and throughout the world. But in the current pandemic, telemedicine is facing new challenges. This article discusses the state of the art in telemedicine and the prospects for its development in the changing conditions wrought by the pandemic. Examples are provided of the solutions that telemedicine can offer in such a difficult period, and the risks due to widespread use of telemedicine are analyzed. The impact of telemedicine is extensive with consequences for technology, management, and law. This article is a multidisciplinary study of telemedicine from the perspective of management and law. The article examines how telemedicine technologies have been implemented and developed, the obstacles to telemedicine's advance in various countries, and the legislative frameworks that governs it. The article's interdisciplinary study is based on an integrated methodology which combines: a formal logical approach to analysis of the legislation concerning telemedicine; a comparison of the development of telemedicine across several countries; and a sociological method to identify the attitude of Russian medical staff toward telemedicine and its impact. Although telemedicine has been developed and regulated separately by each country, there are general development trends, such as collection and analysis of electronic health records (EHR), devices and systems to simplify communication between doctors and with chronically ill patients, and others. Legislation is one of the significant barriers to the development of telemedicine in different countries. However, the pandemic has been a catalyst for legislative change, and it is precisely those changes that will eliminate the key problem in telemedicine that beset Russia where telemedicine now resembles separate pieces in a puzzle.

Keywords

telemedicine, e-health, COVID-19 pandemic, personal data, electronic health records, cybersecurity, electronic document management, Big Data.

For citation: Zhuravlev M.S., Blagoveshchenskaya O.K. (2020) Telemedicine: Current State and COVID-19 Lessons // *Legal Issues in the Digital Age,* no 2, pp. 93–143.

DOI: 10.17323/2713-2749.2020.2.93.143

Introduction

The advances in telemedicine during recent decades have encouraged hope for reform of healthcare. The purpose of this article is to understand what the future holds for telemedicine in Russia after the pandemic. To do this, the current state of telemedicine, technological trends in it, and the barriers it is encountering have been analyzed along with the options for use of telemedicine during the COVID-19 pandemic and the distinctive features of Russian medicine in in general.

The pandemic has presented us with a fresh way to assess the importance of telemedicine and given us a test of its effectiveness in stressful circumstances. Healthcare systems will evolve faster in 2020 in order to adapt to new needs and to new opportunities for those who are willing to do more to attract healthcare consumers. These systems will reduce the time patients spend waiting to contact doctors and the time doctors spend gaining the confidence of their patients.

Partnerships between healthcare organizations and technology companies will progress rapidly after 2020 as healthcare providers will increasingly focus on innovative technologies and more competitive strategies to attract patients. Major players in the technology market will also concentrate more attention on healthcare and work closely with major healthcare providers and insurers to develop new technologies that will improve the quality of patient care.

1. Global Overview of Telemedicine

1.1. How Telemedicine is Defined

Which of telemedicine's particular features legislation incorporates in the legal concept of it is of paramount importance when telemedicine is introduced into a country and in choosing the path for its development. It should come as no surprise that the legislation of each country offers up its own concept of telemedicine.

The definition of telemedicine in the USA is established by each of its constituent state governments, although they base the definition on remote

provision of medical services using electronic means of communication to exchange data. For example, the Alaska State Administrative Code[1] defines telemedicine as "the practice of health care delivery, evaluation, diagnosis, consultation, or treatment, using the transfer of medical data through audio, video, or data communications that are engaged in over two or more locations between providers who are physically separated from the patient or from each other." The essential elements in this definition are: 1) the provision of medical services; 2) the use of communications for data transmission; 3) the remote nature of the interaction.

Telemedicine functions in the United States are regulated by the laws of each state in a special act on telemedicine[2] or in several acts devoted to certain aspects of telemedicine (licensing, insurance, etc.)[3]. Different US states have different approaches to the legalization of various telemedicine activities. Some states quickly recognized the potential for remote diagnosis and treatment, while other states took many years to do this, and in some states certain forms of telemedicine activity are still not legal[4].

US law on telemedicine is exceptionally diverse because each US state makes its own legislation, which means each state can impose its own detailed understanding of what telemedicine is. In Massachusetts law, telemedicine is defined as the provision of healthcare services using interactive audio, video, or other electronic communications for diagnostic, counseling, or treatment purposes. But in Massachusetts telemedicine does not include services that use only the telephone, facsimile or email[5].

---

[1] Alaska Admin. Code. Title 7, 12.449, quoted in *State Telehealth Laws & Reimbursement Policies*. Available at: https://www.cchpca.org/sites/default/files/2019-05/cchp_report_MASTER_spring_2019_FINAL.pdf (accessed: 01.07.2020)

[2] New Jersey's telemedicine law: What providers need to know, a commentary on the website of the Foley and Lardner LLP legal practice. Available at: https://www.healthcarelawtoday.com/2017/08/07/new-jerseys-telemedicine-law-what-providers-need-to-know/ (accessed: 01.07.2020)

[3] Current State Laws & Reimbursement Policies, Center for Connected Health Policy. Available at: https://www.cchpca.org/telehealth-policy/current-state-laws-and-reimbursement-policies (accessed: 01.07.2020)

[4] Regulatory approaches to telemedicine, General Medical Council. Available at: https://www.gmc-uk.org/about/what-we-do-and-why/data-and-research/research-and-insight-archive/regulatory-approaches-to-telemedicine (accessed: 01.07.2020)

[5] Annotated Laws of Massachusetts. Chapter 224, Sec. 158, *State Telehealth Laws & Reimbursement Policies*. Available at: https://www.cchpca.org/sites/default/files/2019-05/cchp_report_MASTER_spring_2019_FINAL.pdf (accessed: 01.07.2020)

A recent trend in the United States is to expand the concept of telemedicine. For example, in Arkansas[6], a 2015 law defines telemedicine as the use of electronic information and communication technologies to provide healthcare services, including and without limitation diagnosis, counseling, treatment, education, healthcare administration and patient self-management; telemedicine also extends to store-and-forward processing of medical information and remote monitoring of patient health. The Arkansas definition is not limited to the exchange of data for the provision of remote medical services, as it includes matters related to data storage and transfer, administration, education, etc.

The American Telemedicine Association (ATA) is now taking a broader approach to the definition of telemedicine. The terms "telemedicine" and "telehealth" are used by the ATA as synonymous, encompassing "technology-based service delivery and healthcare management that increase opportunities and accessibility". ATA notes that with the development of information technologies such as artificial intelligence and virtual reality, the concept of telemedicine is expanding even more[7].

The European Union (EU) in theory and in legal documents uses the term "telemedicine" along with the term "e-health". The European Commission defines telemedicine as:

> ...the provision of health services, through the use of ICT, in situations where the health professional and the patient (or two health professionals) are not in the same location. It involves secure transmission of medical data and information, through text, sound, images, or other forms needed for the prevention, diagnosis, treatment and follow-up of patients[8].

This definition implies a distinction between two types of telemedicine: 1) services involving medical action, such as interpreting X-ray images; 2) telemonitoring, which refers to remote monitoring of health status. However, neither electronic health records, nor electronic prescriptions, nor

[6] Arkansas Code Sec. 17-80-402, State Telehealth Laws & Reimbursement Policies. Available at: https://www.cchpca.org/sites/default/files/2019-05/cchp_report_MASTER_spring_2019_FINAL.pdf (accessed: 01.07.2020)

[7] Available at: https://www.americantelemed.org/resource/why-telemedicine/ (accessed: 01.07.2020)

[8] Report of the eHealth Stakeholder Group on implementing the Digital Agenda for Europe Key Action 13/2 'Telemedicine', an official website of European Union. Available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=5167 (accessed: 01.07.2020)

electronic referrals are regarded as part of telemedicine in the EU although they are part of e-health.

The European approach to the definition of telemedicine is narrow and comes down to providing medical services through data transmission. In this understanding, telemedicine is part of e-health, which is a combination of "tools and services that use information and communication technologies to improve the prevention, diagnosis, treatment of diseases, monitoring and administration in the field of healthcare". E-health covers the following areas: electronic document management between patients, medical organizations and doctors; telemedicine services; portable devices for monitoring patient health; planning software; robotic surgery, etc.[9]

The Russian equivalents of "e-health" and "telemedicine" are also somewhat vaguely defined. Earlier legal sources[10] use the terms "telemedicine technologies" and "internet medicine". Telemedicine technologies include diagnostic and treatment consultations and also managerial, educational, scientific and educational activities in the field of healthcare that are implemented using telecommunication technologies, Internet medicine is regarded as an integral part of telemedicine technologies and includes information support for clinical medicine in counseling patients; health service referrals; providing access to library databases, etc.

The Russian Health Fundamentals Act of 2017[11] introduced a new definition for telemedicine technologies, which came to be understood as information technologies that ensure remote interaction of medical workers with each other, with patients and (or) their legal representatives, identification and authentication of these persons, documentation of their actions during consultations, and remote medical monitoring of a patient's health. Although Russian legislation does not provide a legal definition of telemedicine like the European one, the use of telemedicine technologies is subject to legal regulation.

---

[9] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on telemedicine for the benefit of patients, healthcare systems and society, European Union Law. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0689:FIN:EN:PDF (accessed: 01.07.2020)

[10] Ministry of Health of the Russian Federation. Order N 344, RAMS N 76 dated 27 August 2001 "On approval of the Concept for the development of telemedicine technologies in the Russian Federation and its implementation plan"/ Consultant Plus.

[11] Federal Law dated 29 July 2017 No. 242-FZ "On amending certain legislative acts of the Russian Federation on the use of information technologies in the field of health care", SZ RF. 31 July 2017, N 31 (Part I), Art. 4791.

It seems that a restrictive understanding of telemedicine in both Russian and foreign law has been mostly provisional because regulating interaction through telemedicine inevitably overlaps with other matters related to e-health, including health information systems, electronic health records, electronic prescriptions, etc. The concepts of telemedicine and e-health seem to be converging.

A 2007 World Health Organization (WHO) study identified 104 definitions of telemedicine[12]. To remedy the ambiguities in the definition of telemedicine, WHO has proposed using the terms "telemedicine" and "e-health" as synonymous in a broad sense[13]. In 2005, WHO defined e-health as "the cost-effective and secure use of information and communications technologies in support of health and health-related fields, including health-care services, health surveillance, health literature, and health education, knowledge and research"[14]. This way of framing e-health goes beyond the use of information technology to provide medical services directly and create the necessary infrastructure to do so by also including such areas as providing access to medical literature using ICTs, promoting a healthy lifestyle through e-learning, etc. The International Telecommunication Union follows a similar approach[15]. For the purposes of pursuing state policy in the field of health information, a broad approach of this kind seems very suitable for guiding governmental policy concerning healthcare that is mediated by digital information because it leaves room for a comprehensive consideration of the all the issues that need to be addressed.

It should be noted that in addition to the terms "e-health" (and sometimes "telehealth") and "telemedicine", other terms such as "mobile health" (or "Mhealth"), "electronic medicine" ("e-medicine"), interactive medicine and more are in use. By and large, they refer to the same concepts but are used in some situations to emphasize one aspect or another of e-health. For

[12] Telemedicine. Opportunities and development in member states. WHO report on the results of the second global survey in e-health, World Health Organization, p. 9. Available at: http://apps.who.int/iris/bitstream/10665/87687/1/9789244564141_rus.pdf (accessed: 01.07.2020)

[13] WHO Resolutions and Decisions. eHealth, World Health Organization. Available at: http://apps.who.int/iris/bitstream/10665/20378/1/WHA58_28-en.pdf (accessed: 01.07.2020)

[14] WHO Resolutions and Decision. Available at: https://apps.who.int/iris/bitstream/handle/10665/20378/WHA58_28-en.pdf;jsessionid=B45030782058B782F7C39CDDA68FBC00?sequence=1 (accessed: 01.07.2020)

[15] ITU-T SG 16 Work on E-health — Definition of some terms related to e-health technologies, International Telecommunication Union. Available at: https://www.itu.int/en/ITU-T/studygroups/2013-2016/16/Pages/ehealth_terminology.aspx (accessed: 01.07.2020)

example, the term "mobile health" is used to single out telemedicine based on wireless devices and mobile phones by emphasizing certain of the means for carrying out telemedicine. However, the particular means used in telemedicine do not have great legal significance. This is consistent with the principle that legal regulation should be technologically neutral.

For the purpose of this study it will be useful to condense all the concepts considered so far into the single term "telemedicine" which refers to the use of information and communication technologies for the provision of medical services, the creation and maintenance of a healthcare infrastructure, and improvement in the quality and accessibility of healthcare. In this sense, telemedicine includes health information systems, electronic patient health records, remote medical services, remote monitoring of patient health status, access to electronic documents (prescriptions, sick leave documentation, medical reports and certificates), electronic appointments with doctors, remote medical consultations and other forms of medical activity including medical research involving information and communication technologies. The defining features of telemedicine are the remote nature of the interaction between the participants in telemedicine activities and automated processing of information. Telemedicine and e-health will be used synonymously and interchangeably. A similarly broad approach to defining telemedicine is supported in Russian legal literature and has been prompted by the need to identify general trends in the application of information technologies to medicine and in their legal regulation [Putilo N.V. & Volkova N.S., 2018: 124–135].

Putilo and Volkova suggest that telemedicine be understood as a system for exchanging medical information through information and communication technologies and that it consist of the following elements: 1) training tools for medical workers (teleconferences, training programs, online training, etc.); 2) ways of transmitting information as part of patient counseling; 3) means for electronic interaction between participants in the healthcare system (electronic cards, electronic records, electronic prescriptions); 4) electronic means for monitoring the patient's health with direct surveillance of the patient by an agent in the information system or by the attending physician (e.g., via an electronic bracelet); 5) a special information environment (special sites created by public organizations to inform and advise patients and medical workers); 6) online sales of medicines and medical devices.

The concept of telemedicine is dynamic, and over time it will respond to new technological advances and changing health needs and also adapt to

new and changing social contexts. Thus, it is possible that new technologies will need to be included in the definition of telemedicine. For example, in Russia the concept of telemedicine had not previously included the delivery of medications but now does include it.

1.2 Telemedicine Law and Policy in Different Countries

As they understand the tremendous importance of information technology in modern society, many national governments are now pursuing a policy of comprehensive digital transformation or ways to relate to the public. Establishing e-health is one of the important goals for that kind of transformation.

Providing a high-quality and reliable IT infrastructure is important, but it is not the only element necessary for successful advancement of e-health. Some countries with relatively high rates of penetration of information technologies (access to broadband internet, mobile coverage, a high number of personal computers and mobile devices per capita and other similar indicators) are still lagging behind in developing e-health. For example, a study of e-health among EU countries found that Bulgaria is one of the most advanced EU countries in deploying information and communication technologies although it is far behind in developing e-health [Currie W. & Seddon J., 2014: 783–797]. One of the main reasons for Bulgaria's falling behind is lack of a national strategy for applying information and communication technologies to healthcare, including lack of regulation for it.

Telemedicine is definitely a field that requires governmental regulation because it must have high safety standards and protect the rights of patients, etc. The United States serves as an example of the inadequacy of market mechanisms to advance telemedicine. Although the e-health market, including electronic medical records and remote medical services, came about in the United States at the behest of economic actors (medical organizations and insurance companies) rather than because of any government prompting [Carlisle G. et al., 2013: 51], the need for government intervention in shaping the market for telemedicine services very soon became evident, mainly in matters of licensing, insurance, and protection of patients' personal data.

Many countries are adopting strategies and developing legislation to remove legal barriers to using digital technologies in various areas of interacting with the public, including in healthcare.

In the European Union the key strategic document aimed at universal digitalization of European society is the Digital Agenda for Europe[16], which is part of the broader EU development strategy through 2020 (Europe 2020)[17]. Effective use of digital technology to improve the quality of healthcare is one of the goals of this strategy. For telemedicine the Digital Agenda emphasizes the importance of ensuring trust and security because it cannot exist without reliable and trustworthy information technologies (Section 2.3). An important condition for the success of e-health is to ensure that patients may safely store their personal health records in health information systems that are available online (Section 2.7.2). The strategy states that the realization of the full potential of information technology in healthcare requires removing legal and organizational barriers, as well as strengthening cooperation between EU member states, in order to form a single market for digital services including telemedicine services. The document states that the potential of ICT can help solve important problems for the EU such as an aging population, increasing healthcare costs, and integrating people with disabilities into society.

More specific steps for the development of e-health in the EU were set forth by the first Action Plan for the Development of eHealth for 2004-2011 (eHealth Action Plan 2004-2011)[18] and also developed after the adoption of the Digital Agenda by the second Action Plan for 2012-2020 (eHealth Action Plan 2012-2020)[19]. The first Action Plan mainly covered ways to implement electronic prescriptions and electronic maps and to ensure interaction between health information systems. The second Action Plan was focused on implementing the provisions of EU Directive 2011/24/EU on

[16] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe, European Union Law. Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52010DC0245 (accessed: 01.07.2020)

[17] EUROPE 2020 A strategy for smart, sustainable and inclusive growth, European Union Law. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52010DC2020 (accessed: 01.07.2020)

[18] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions — e-Health — making healthcare better for European citizens: an action plan for a European e-Health Area. Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52004DC0356 (accessed: 01.08.2019)

[19] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions — eHealth Action Plan 2012–2020 — Innovative healthcare for the 21st century. Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012DC0736 (accessed: 01.08.2019)

the application of patients' rights in cross-border healthcare[20], which sought to enhance cooperation between EU member states in order to maximize the social and economic benefits of e-health development throughout the Union. The second Action Plan builds upon the progress achieved, but it acknowledges that significant barriers still remain in the path to full implementation of e-health.

While the first stage of establishing e-health in the European Union was aimed at creating an e-health information infrastructure, the second stage is already directly involved in organizing telemedicine services as well as the use of modern information technologies to improve the quality of healthcare. Hence, one of the key goals of the second Action Plan is to stimulate research through telemedicine technologies (Section 5.1). The European Commission recognizes the importance of health research and innovation in both the short and long term. Information technology and science can have a synergistic effect and contribute to improving the effectiveness of healthcare. To support research and innovation in e-health, the development of various forms of public-private partnerships and government funding of e-health research projects has been proposed.

Within EU member states some aspects of telemedicine are regulated by national legislation on health protection and other legislative acts[21]. Some countries have adopted separate laws on telemedicine. For example, Germany in 2016 passed a law on secure digital communications and software in the healthcare system[22], which establishes the legal framework for handling electronic patient health records, health information systems and electronic document management in the healthcare system when providing telemedicine services.

German federal law does not prohibit making a diagnosis and prescribing therapy remotely and permits them at any time convenient for the patient rather than only during usual reception hours. By May 2018 legislative

[20] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0024 (accessed: 01.08.2019)

[21] Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services. Final report and recommendations, European Union. Available at: https://ec.europa.eu/health/sites/health/files/ehealth/docs/laws_report_recommendations_en.pdf (accessed: 01.07. 2020)

[22] E-Health law in Germany, a commentary by the Taylor Wessing legal practice. Available at: https://www.lexology.com/library/detail.aspx?g=83f3f929-7be7-4383-a66b-ed1dedeb912d (accessed: 01.07.2020)

restrictions on remote diagnoses had been removed with the caveat that a remote diagnosis can be made if there is objective evidence for it. At present a ban on prescribing treatment remotely has been retained only in states of Brandenburg and Mecklenburg-Vorpommern [Wernick A. & Klünker I., 2019: 169–177].

In contrast to the countries of the European Union, the USA has no uniform strategy for developing telemedicine and e-health.

The United States regulates a small range of issues pertaining to telemedicine at the federal level. In 1996 the United States passed the Health Insurance Portability and Accountability Act (HIPAA)[23], one of whose provisions set requirements for the confidentiality and security of personal health information about patients in electronic form. In 2009 the Health Information Technology for Economic and Clinical Health Act (HITECH Act)[24] introduced a government incentive program for the introduction of electronic health records (EHRs). The law entitled physicians who use information technologies to improve medical services (meaningful use) to receive a government subsidy of up to US$63,750 under certain conditions.

The regulation of most issues, such as licensing requirements for doctors, liability issues, health insurance, and a number of other aspects of telemedicine, falls within the purview of each individual state government. Even the federally enacted HIPAA does not ensure the uniformity of state regulations in protecting patient data because states have the option to apply stricter rules for such data when processed by information systems. All this creates additional barriers to the development of telemedicine throughout the United States.

1.3. Electronic Health Records, Data Sharing and Resistance to Telemedicine

Up until 2019 and before the pandemic, the electronic health record (EHR), which is already being used by Austria, France, Israel, Japan, Singapore, Estonia, Finland, Slovakia, Spain and Sweden had been the focus of development in telemedicine. EHR is also in place partially, but not everywhere in the UK and in its public hospitals.

[23] Health Insurance Portability and Accountability Act of 1996, US Congress. Available at: https://www.congress.gov/104/plaws/publ191/PLAW-104publ191.pdf (accessed: 01.07.2020)

[24] What is the HITECH Act?, *HIPAA Journal*. Available at: https://www.hipaajournal.com/what-is-the-hitech-act/ (accessed: 01.07.2020)

An EHR system typically consists of data protection features, information received by doctors, and establishment of a unified set of terms and common standards.

The telemedicine services market has made the most advances in the USA, and as a result information systems there are increasing their integration into healthcare more than in the rest of the world. The HITECH Act (Health Information Technology for Economic and Clinical Health Act)[25] in the United States was providing government incentives for introducing EHR as early as 2009.

A study by Grand View Research showed that the global EHR market in 2016 amounted to US$23 billion and that by 2025 it would increase to US$33 billion. Most of this amount is concentrated in the USA where companies like Epic have dominated the EHR systems market (at 26.7% in 2016), while Cerner (24.8%), Meditech (17%) and Centricity Practice Solution (10.3%) together accounted for almost half of the market[26].

In addition, the U.S. Department of Health and Human Services and the National Institute of Standards and Technology are involved in the development, support and standardization of digital medicine, while Brazil, India, Russia and Asian countries are also actively developing it.

EHRs can contain a complete history of people who visit various medical institutions, including test and immunization charts as well as data on allergies and all illnesses. This allows doctors to quickly obtain comprehensive information about patients and more accurately prescribe treatment and at the same time reduces the amount of paperwork.

The EHR has become a key to the development of telemedicine because of the advantages it offers. One primary and very important benefit is security: patient status data is archived safely in a secure cloud storage system. This ensures that complete information about all the illnesses and individual characteristics of patients will not be lost or misplaced and will be available in any treatment facility. This method of data storage includes proper encryption and is extremely reliable because it is relatively invulnerable to external physical factors such as a physical server's malfunction or failure.

Another feature of EHRs is that the records contain a history of changes in the patients' condition throughout their lives. The doctor can see the pa-

[25] Ibid.

[26] Digital medicine as a way to reduce healthcare paperwork, a presentation at the M-Health Congress. Available at: https://mhealthcongress.ru/en/article/tsifrovaya-meditsina-kak-sposob-sokratit-bumagnuyu-rabotu-v-sfere-zdravoohraneniya-96477 (accessed: 29.04.2020)

tient's reaction in the past to various therapies, and this information will help indicate the most suitable treatment in the current situation. Complete information with immediate access to it will help doctors conduct better analyses and make more accurate diagnoses.

Systematic information stored in digital form instead of on paper permits medical organizations to make research both broader and more refined. This is especially helpful with statistics concerning diseases.

EHRs can be used to implement programs for controlling the quality of healthcare in a country, and it can also facilitate use of digitized data derived from older paper records in the database in order to make more accurate forecasts based on this retrospective big data.

For the patient an EHR makes it easier to choose from among a broader range of doctors and specialists without being tied to one medical institution.

In different jurisdictions two legal arrangements for creating electronic health records have become widespread — opt-in and opt-out[27]. The opt-in provision (used in France and until 2016 in Australia) involves obtaining prior consent from patients to create EHRs and distribute them through health information systems. The opt-out provision (used since 2016 in the UK, Singapore, Australia, etc.) involves creating EHRs without consent from patients although they retain the right to have them removed after they have been created.

The opt-in arrangement is designed to increase the autonomy of patients by having them make an informed choice to participate in the electronic exchange of medical information. The use of the opt-in method accords a higher degree of responsibility to patients themselves for their choice, including the choice of which person or organization they trust to store and manage their personal electronic health records. Despite the opt-in method's obvious positive features, it has a significant drawback in that it complicates the process of creating a unified field information for telemedicine, does not ensure that complete information on all patients in the system will be available and leaves all the medical data of a potentially large number of patients who do not opt in outside of electronic document management.

The opt-out mechanism permits electronic records on patient health to be created without their consent, but they can reject retention of their elec-

[27] EHR Systems—Opt in or opt out?, a commentary by the Accenture consulting firm. Available at: https://www.accenture.com/es-es/~/media/Accenture/Conversion-Assets/DotCom/Documents/Local/es-es/PDF_3/Accenture-Health-Opt-In-Opt-Out.pdf (accessed: 29.04.2020)

tronic records and exclude them from electronic document management. This method comes under criticism for ignoring the preferences patients may have about the creation and handling of EHRs. However, the opt-out method has the best potential for keeping greatest possible amount of medical information under electronic document management and ensuring the completeness of the information stored in healthcare information systems. The benefits of having more medical information in electronic document management persuaded Australia after 2016 to replace the opt-in mechanism with opt-out (with a two-year period during which refusal to participate is permitted)[28].

In some countries, such as the USA[29] and Singapore[30], legislation establishes the obligation of medical organizations to create electronic records of patient health, but it still grants patients the right to refuse retention of electronic records.

The legislation of various countries shows a general preference for the compulsory creation of EHR, but the right of patients to refuse to include their personal health records in the electronic document management system is recognized. In what follows most of the comparative statistics concerning penetration of telemedicine and attitudes toward it in different countries is taken from surveys of 15,000 patients and 3,100 healthcare professionals in 15 countries. These surveys were commissioned and published by the Philips multinational corporation in an effort to assess the global market for telemedicine solutions and promote its advance.

The penetration of telemedicine and its subsystems can vary broadly among countries and even within a single country. While 84% of healthcare professionals in the USA use EHRs, only 46% of USA healthcare professionals use the full range of telemedicine, compared to a 15-country average of 61%; and only about 33% use AI-powered solutions in their practice or hospital[31].

---

[28] See the webpage description My Health Record posted by the Office of the Australian Information Commissioner (OAIC). Available at: https://www.oaic.gov.au/privacy-law/other-legislation/my-health-records (accessed: 29.04.2020)

[29] HHS: Everyone can opt out of government-mandated electronic health records system, CNS News. Available at: https://www.cnsnews.com/news/article/hhs-everyone-can-opt-out-government-mandated-electronic-health-records-system (accessed: 29.04.2020)

[30] Greater protection of patient data when national electronic medical records become mandatory, *The Straits Times*. Available at: https://www.straitstimes.com/singapore/health/greater-protection-of-patient-data-when-national-electronic-medical-records-become (accessed: 29.04.2020)

[31] Future Health Index 2019. Available at: https://www.usa.philips.com/c-dam/corporate/news-center/global/future-health-index/fhi2019/fhi-2019-report-united-states.pdf (accessed: 29.04.2020)

These indicators suggest that despite the increased use of AI techniques, which are viewed as the gateway to the next phase of telemedicine, the general acceptance of new technologies and solutions is lagging. Innovation in fields like healthcare and education is usually a long and difficult process even when its advantages are clear; and these statistics support that idea.

Countries like Germany (41%) and China (85%) surpass the U.S. in the use of AI technologies among healthcare professionals, even though the U.S. has one of the highest costs for use of AI for preliminary diagnoses per capita at US$ 0.06, while China's cost is US$ 0.002 per capita and Germany's is US$ 0.03 per capita[32].

This once again confirms that a high level of technological development, for AI in this case, does not directly ensure its implementation in such areas as healthcare.

The public still has questions about the introduction of EHR, and US healthcare professionals have not enthusiastically embraced EHRs, as a common assumption among healthcare professionals is that making these records adds administrative tasks to their workload and reduces time with patients. Healthcare professionals in the US using EHRs were among the most likely to believe that the adoption of EHRs in their hospital or practice had a negative impact on time spent with a patient (53%), healthcare professional workload (61%) and healthcare professional satisfaction (44%)[33]. These data are not merely concerns about future impact; they are a direct reaction to the systems that medical staff are actually using.

Introducing EHRs can also prompt resistance to them. In the Asian countries surveyed for the Future Health Index, healthcare professionals who do not share patient data outside their healthcare facility cite data privacy and security concerns as key reasons for their reluctance. Among European countries the Future Health Index surveys found interoperability and lack of access were more prominent objections.

Technology continues to evolve, and this will in turn drive continuous transformation in health systems around the world. Healthcare professionals that embrace the use of digital health technology are seeing a positive

[32] Transforming healthcare experiences, Future Health Index 2019. Available at: https://images.philips.com/is/content/PhilipsConsumer/Campaigns/CA20162504_Philips_Newscenter/Philips_Future_Health_Index_2019_report_transforming_healthcare_experiences.pdf (accessed: 29.04.2020)

[33] Ibid.

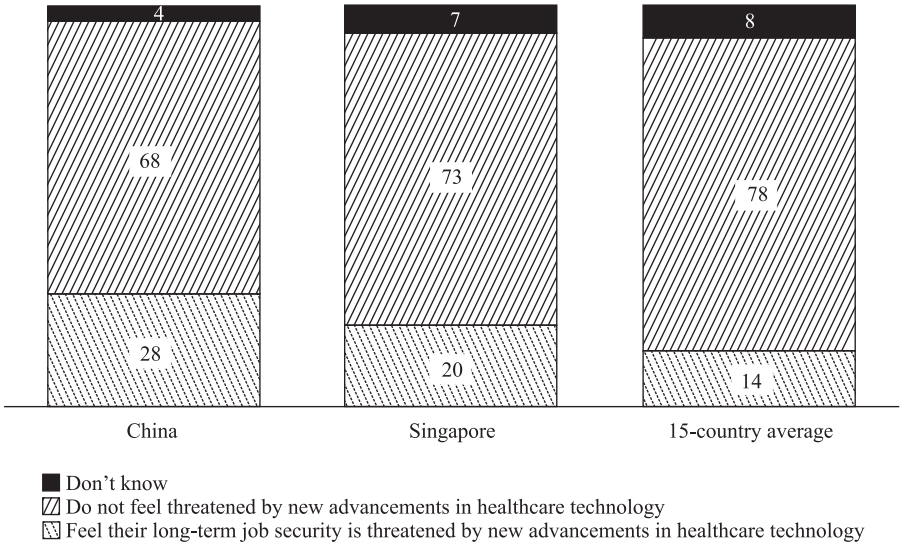


Fig. 1. Telemedicine Barriers (China, Singapore, 15-country average), %[34]

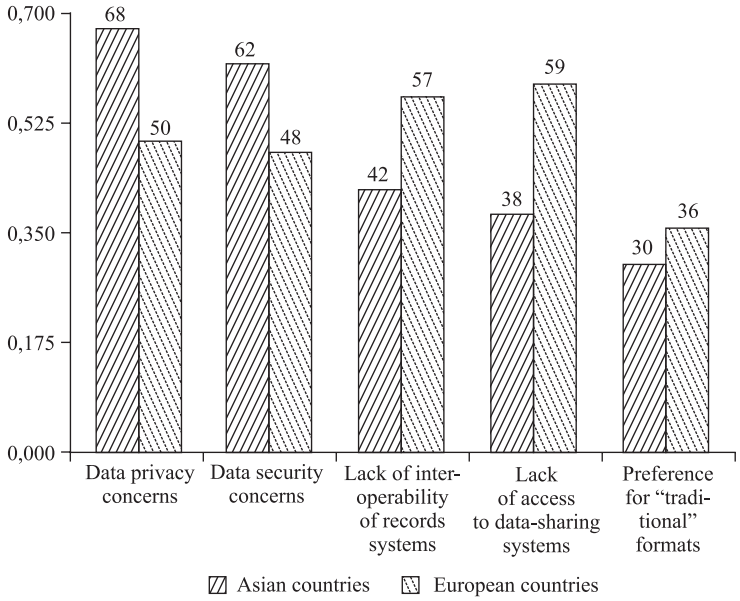


Fig. 2. Telemedicine Barriers (Asian and European countries), %[35]

[34] Ibid.

[35] Ibid.

impact on their own experience as well as on that of their patients. Digitally empowered patients who share their health data tend to have a stronger relationship with healthcare professionals. The forerunner countries that have leapfrogged over others in their adoption of digital health technology have solved many of the challenges that others are still grappling with, but they face new obstacles that come with the advanced use of digital health technology.

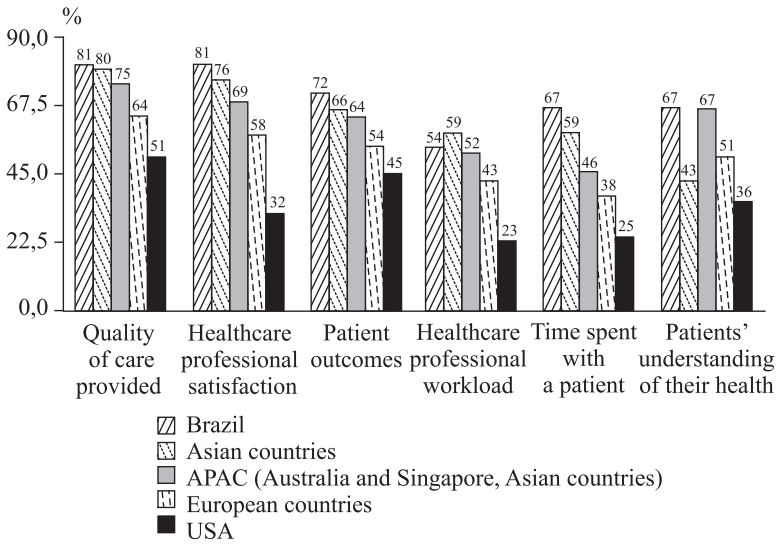


Fig. 3. Use of EHRs by medical staff from different countries[36]

While the forerunners have been moving steadily ahead with digital healthcare technologies, barriers to broader adoption remain. European countries especially stand out in the Future Health Index surveys: lack of access to data-sharing systems (of greater concern than in the Asian forerunners by 15%), lack of interoperability of records systems (of greater concern by 21%), preference for 'traditional' formats (more of a factor by 6%). The surveys also show that data privacy concerns (18% more prevalent than in European countries) and data security concerns (14% more prevalent) are greater drawbacks in Asian countries[37].

The aforementioned barriers hinder the development of telemedicine in general, even when the population (patients or medical personnel) is al-

[36] Ibid.

[37] Ibid.

ready ready to master the technology, realizing the ever-growing need. The demand for telemedicine may then decrease and prompt a wasteful search for new solutions by patients or medical personnel.

If all the barriers to the development and spread of telemedicine in different countries may be viewed generally without paying too much attention to particular cases, resistance falls into the following main groups:

1. Cultural differences. Some countries are not ready to adapt quickly because the traditional system of interaction with the doctor has developed over the years and decades (for example, the United States with its sophisticated legal system and larger differences between states.)

2. Legal barriers. Legislation is not a catalyst of change (as in Germany) but instead a limiting factor. Although the market may be ready for innovations and sees their beneficial impact, the law holds back (or again as in the USA where a complex legislative system interferes with applying the same measures immediately in all of its states).

3. Suspicion. The misgivings are not usually due to a distrust of technology in itself, which may arise from lack of awareness. Suspicion focuses mostly on the potential for theft of personal data or its improper use.

4. Systemic inconsistency. Medical professionals are often prevented from using all the telemedicine technologies because different software or upgrades do not interact as expected. The users cannot then enjoy the anticipated benefits.

1.4. Telemedicine Market and Innovations

The number of professionals using new technologies speaks for the assimilation of these technologies. In the healthcare sector, it is the medical professionals who set the pace for technology adoption and implementation. The very low percentage of healthcare professionals in Germany who currently use any digital health technology or mobile health apps (64%) is an outlier, given that the average for all countries is 78%. A lower rate is found only in South Africa (48%).

Such date shows which countries have been moving steadily from merely gaining access to digital health technology to actually implementing it. China, India, Italy and Saudi Arabia (more than 85%) stand out as consistent forerunners when it comes to the adoption and use of all new technologies[38].

[38] Ibid.

Some other emerging markets, including India and Russia, also excel in specific areas. Such countries can be considered "legislators" of development and trends in healthcare technologies.

Although there have usually been some problems in the use of telemedicine technology, it is continuing its rapid development. In 2019 and 2020 many interesting and innovative companies, technologies and applications have appeared. These innovations apply first to medical personnel. Of course, any technologies for improving the quality of doctor-patient interactions are bound to be used by medical personnel as well. But technologies created only for doctors have begun to appear on the market. There is Smartbadge Communicator[39], a large-screen device that provides access to various medical systems. It allows medical professionals from the same hospital to quickly communicate with each other by voice.

Other technologies augment the skills of medical professionals. One such invention is the Remedy platform[40] which uses AI. It allows medical personnel who are not qualified as physicians to access medical experience in order to detect hidden chronic diseases when interviewing patients by telephone or video; they can expedite treatment choices by collecting clinically relevant information outside the four walls of the hospital. This kind of early diagnosis helps in determining the best therapy for benefiting the patient's health while keeping costs lower.

There are other innovations that help patients with any illness. For example, Pria[41] is home care device that reminds patients to take medication, dispenses it and acts as a video call device. Pria can monitor patients and remotely inform the doctor about their condition through a smartphone application.

Chronically ill patients can benefit from devices that constantly monitor important vital signs. The Omron HeartGuide[42] is a smart watch which accurately measures blood pressure and sends data to a smartphone. The same application works for people with diabetes, asthma and other chronic diseases.

[39] Smartbadge Communicator website. Available at: https://www.vocera.com/vocera-smartbadge (accessed: 29.04.2020)

[40] Remedy platform website Available at: https://www.remedyhealthmedia.com/ (accessed: 29.04.2020)

[41] Pria website. Available at: https://www.okpria.com/ (accessed: 29.04.2020)

[42] Omron HeartGuide website. Available at: https://omronhealthcare.com/products/heartguide-wearable-blood-pressure-monitor-bp8000m/ (accessed: 29.04.2020)

Some devices help patients through everyday life. Heartbit[43] is a wearable device from Hungary for monitoring a person's ECG, which is then used to devise an effective training program that is suitable for a person's cardiac condition. Sensors are built into training t-shirts so that Heartbit smart algorithms can ward off arrhythmias, ischemia and other hidden heart conditions. A technology like this is an innovative supplement to treatment by a cardiac specialist.

One of the most urgent tasks facing telemedicine is to improve the accuracy of online consultations and simplify the process as a whole. The EYE-SYNC concussion assessment system[44] using VR glasses with sensors that monitor eye movement has been created to do that for one type of injury, and it can reach a diagnosis in the absence of a doctor. Tyto Care offers remote medical services in the USA, Japan and China. It allows patients to conduct their own medical exam using a device that combines a camera, a stethoscope, an otoscope, a thermometer and a tongue depressor. Tyto can take high-resolution images of moles, rashes, and other skin lesions so that a doctor can make a preliminary dermatological analysis. Other images can be made in order to diagnose optical conditions such as conjunctivitis or eye infections. All information is transmitted directly to a screen on which the doctor sees the whole picture. The Tyto platform also instructs the user by means of a smart guidance system that provides audible and visual cues that help the patient to capture a useful image or sound. There is also a way to save examination data in the cloud so that the doctor can later refer to the results.

Using these technologies yields impressive results [Flodgren G. et al., 2015]; [Moy F. et al., 2019]. Telemedicine technologies are particularly important in regions where there are problems with the availability of medicine, such as being far from a medical institution [Oliveira T. et al., 2012].

A few trends in the development of telemedicine technologies can be discerned after analyzing these innovations. First, there are devices and systems to facilitate communication between doctors and in particular to quickly arrange consultations with more specialized professionals. Second, there are devices that enable chronically ill patients to have the data necessary for analysis or rapid response continuously collected and transmitted

[43] Hungarian Heartbit website. Available at: https://theheartbit.com/ (accessed: 29.04.2020)

[44] EYE-SYNC website Available at: https://syncthink.com/2019/02/19/fda-grants-syncthinks-eye-sync-platform-breakthrough-device-designation-for-aid-to-concussion-assessment/ (accessed: 29.04.2020)

to doctors. This kind of device is for patients with cardiovascular diseases, diabetes, asthma, and persons with mental disorders. Third, there are home-use devices which increase the effectiveness of online examinations by enabling transmission of data to a doctor. Making online examinations as close as possible to an initial interview in person is especially important here.

Another outcome of all these technologies is the potential for collection and in-depth analysis of medical records and patient histories; this greatly simplifies the work of the doctor and reduces admission times, which is one way to increase the throughput of a specialist or hospital.

Extraordinary developments are appearing on the market horizon, such as robots that can maintain a conversation with elderly patients and track their condition. Robots could go beyond reminding a patient to take medication and dispensing it to send a report to the doctor and even call an ambulance. But these innovations are still in the future, and not all of them will prove truly valuable after they are extensively tested. The time for them will probably come, but for now the agenda is to increase the effectiveness of online consultations and create devices that continuously monitor important vital signs of people with health problems. Because the traditional legal provisions do not take into account the distinctive features of telemedicine, there is a need to adopt new legislation to protect the rights and legitimate interests of legal entities engaged in telemedicine and to remove unjustified legal barriers to the use of telemedicine technologies.

A leading example for combining all the technological solutions in a single location is the Ontario Telemedicine Network (OTN), one of the largest telemedicine networks in the world. More than 28,000 people, including over 10,000 physicians, are members of its online service — the OTNhub — which is a secure online environment that is home to several virtual care programs.

OTN's virtual service tools — secure video conferencing, remote monitoring, applications, and platforms — have great potential to influence and support important changes. This virtual assistance helps remove geographic, socio-demographic, and cultural barriers to help provide easier, smarter, and faster care. Collaborating with many partners, OTN continues to search, verify and implement virtual services and find options that solve key problems in the healthcare system.

OTN's goal is to improve the quality of patient care (modernizing access to services, developing special systems for chronically ill patients, improving home care systems). The goals described are closely connected with the

main issues in the field of telemedicine, which OTN will raise at conferences during 2020 and 2021.

Other goals of the clinic, such as reducing the cost of services and reducing waiting times, are also indicative of general trends in telemedicine; they bear on improving how the clinic functions as a whole. Such changes increase the overall performance of the clinic. The important point here is that both kinds of challenges for telemedicine are being addressed within a single medical institution.

Of course, achieving these goals requires an immense effort that focuses on the entire ecosystem of the clinic, and this can happen only over a considerable length of time. One step in the process was taken back in 2018 and 2019 when OTN integrated more than eight different electronic systems.

Apart from plans and ambitions, OTN points to statistics that show the results of that integration in 2017 and 2018[45]:

896,529 patient consultations;

21,498 video visits served to a patient's home;

570 million km in patient travel avoided;

$ 2,8 million saved to date via Virtual Critical Care;

$ 71,9 million saved in Northern Health Travel Grants.

All of these figures suggest what telemedicine can achieve. Of course, this is the most advanced telemedicine center in the world, and the success of telemedicine in general will be determined by opening more clinics of the kind or by its development throughout a particular region. But this is precisely the kind of system worth emulating. It covers all the health needs of the population even though it positions itself as a still developing treatment center.

2. Current State of Telemedicine in Russia

In Russia the impetus for implementing telemedicine came from the enactment of Federal Law No. 242-FZ dated 29 July 2017 "On amending certain legislative acts of the Russian Federation on the application of information technologies in the field of healthcare", which entered into force on 1 January 2018.

This law permits medical opinions, certificates, prescriptions for medicines and medical devices to be issued in electronic form, gives patients the

[45] OTN Annual Report 2017/18. Available at: https://otn.ca/wp-content/uploads/2017/11/otn-annual-report.pdf (accessed: 29.04.2020)

option to provide their informed consent to a medical intervention or refusal in electronic form, and establishes the legal basis for the creation and operation of information systems in healthcare.

The legislation of the Russian Federation also sets restrictions on the provision of remote telemedicine services to a patient. Patients cannot be diagnosed, nor can their treatment be prescribed or remote monitoring of the state of their health be set up without an appointment in person. Telemedicine technologies can be used only for the prevention, collection and analysis of patient complaints and medical history; assessment of the effectiveness of treatment and diagnostic measures; medical monitoring of the patient's health; making decisions on the need for an appointment in person (survey, consultation); in order to adjust previously prescribed treatment (parts 2-4 of the Federal Law No. 323-FZ dated 21 November 2011 "On basics of health protection of the citizens in the Russian Federation"). Online telemedicine services that operate in Russia, such as Yandex.Health[46] and Telemed Doctor Nearby[47], stipulate in their user agreements that only consulting services are provided to their clients and that they should contact a specialist in person in order to be diagnosed or have treatment prescribed.

Although remote consultation with a doctor is not the legal equivalent to a face-to-face appointment, significant steps have been taken for legally providing telemedicine. This law has laid the foundation for nationwide digitalization of healthcare in Russia. Electronic document management, healthcare information systems, remote monitoring of patients' health, identification and authorization of doctors and patients – these and other aspects of e-health have received regulatory support in the Russian Federation. In addition to that law, a number of by-laws and regulations have been developed building upon the foundations laid down by federal legislation (most of those regulations concern the establishment of the Unified State Health Information System). Nevertheless, developing telemedicine further will require solutions to a wider range of legal issues.

[46] f doubtful qualitytives thanrte.agraph becaues dy long as was introduced as approach. esentniation byd when medications go onlin Terms of use of the Yandex.Health service. Available at: https://yandex.ru/legal/health_termsofuse/ (accessed: 29.04.2020)

[47] Telemed: Terms and conditions of use of services. Available at: https://telemed.drclinics.ru/static/user_docs/terms_and_conditions/index.html (accessed: 29.04.2020). Based on the results of the consulting service, a medical report is drawn up — an electronic document compiled by the doctor containing the results of the medical consultation without arriving at or modifying the diagnosis and prescribing treatment.

In Russia the expectation is that every ruble invested in prevention and treatment can save at least 3 to 7 rubles of expense to other sectors of the economy[48]. For example, labor productivity should increase while mortality and disability will decrease, and the economy as a whole will be stimulated. This is happening because healthcare supports and creates labor potential.

Russian medicine tends to be more personalized and less cursory than in other countries. Russian doctors do not immediately prescribe antibiotics for everyone with a cough regardless of the reasons for it or the age of the patient. This approach, which diverges from medicine in many other countries, has long been the established tradition in Russia.

Another aspect of Russia's distinctive way of practicing medicine is that doctors are often more sympathetic and "hands-on". On a first appointment with a doctor, a Russian patient can expect to be touched, poked, tapped and so on. Not all countries take this approach.

Another feature of Russian medicine that is far from universal is that medical care is provided to citizens free of charge. In the USA by contrast every request for medical assistance must be paid for personally or through an insurance policy. Insurance packages vary widely depending on the medical services included and their cost.

The overall availability of medicine will affect the availability of telemedicine as well. The more people are able to use its innovations, the more involvement will increase, and that will become a catalyst for further development of technology. People's involvement is always a kind of feedback; the greater it is, the more the technology will adapt to the needs of society. That adaption will help to entrench telemedicine's popularity.

Russia also provides free medical examinations. These clinical examinations consist of a set of procedures that include a preventive medical exam and additional examination performed in order to assess the patient's state of health and provided for certain groups of the population in accordance with the legislation of the Russian Federation.

Telemedicine would streamline part of the medical examination (for example, filling out questionnaires) by allowing it to take place online; the results could also be received online results and shared with the patient's

[48] Russia's share in the global plastic surgery market remains at 5% (account of a press conference posted on the Russian Agency for Health Information). Available at: http://ria-ami.ru/2016/06/ekspert-dolya-rossii-na-mirovom-rynke-plasticheskoj-hirurgii-ostavlyaet-5/ (accessed: 29.04.2020)

doctor. Expanding functionality in this way would also increase people's involvement in using telemedicine technologies.

The ability to quickly make an appointment with a doctor is very important to patients. If a Russian patient needs to see a specialist, they can sign up for a visit at any local hospital in the next few days. In other advanced countries, it would be unusual even to see a general practitioner so quickly. In the UK, the patient is examined first by a nurse, who decides whether the patient needs an immediate medical examination or whether they can return the next day to wait in the general queue.

How quickly medical services are provided will also affect the speed of response during telemedicine interactions. Telemedicine has the potential to expedite medical care online so that it is even faster and available at any time of day. The speed with which medical procedures already happen in Russia will be further accelerated by the kind of turnaround that telemedicine will enable. A patient should be able to order a medicine, begin taking it and share information about how the treatment is proceeding without leaving home.

What is called traditional medicine also has a place in Russian medicine as it does in some Asian countries. Although it may sound fanciful or frivolous to some, there is considerable evidence that many illnesses can be treated with the proper intake of natural ingredients. If the effectiveness of traditional medicine continues on its path to recognition, that will spur doctor-to-doctor exchanges about its applications; and telemedicine should be able to facilitate that process as Russian doctors tap into the clinical experience and trials of their colleagues practicing traditional medicine.

One last feature of Russian medicine that sets it apart is a personal approach to patients. In Russia's medical practices, standard treatment protocols are not always relied upon or regarded as sufficient. More often a very personalized approach is used in which all aspects of the patient and their body are taken into account.

Standards are in place to regulate what kind of examination a patient should have and what medications should be prescribed for them. But doctors in Russia frequently make a diagnosis in the absence of all the recommended test results and may prescribe medications that are not on the list of standard treatments (but according to the doctor are more suitable for a particular patient). The standard procedures here point out a certain path for treatment, which the doctor may not entirely follow.

Of course, doctors must know the existing standards, protocols, procedures and clinical recommendations, but they may actually follow them or not depending on the clinical situation and their professional experience[49]. This kind of variability constitutes a challenge for digitalization and may delay its development to some extent. But with proper analysis and preparation of a compatible legislative base and regulations, this can become an advantage that will make Russian telemedicine stand apart from others by improving the quality of service while holding waiting times to a minimum and also taking the lead in developing and disseminating new technologies and kinds of treatment.

As telemedicine advances, all of this will become even more convenient. Patients will no longer have to visit the hospital many times to present their test results to the doctor; they will be able to make some measurements at home whenever convenient and then share the diagnostic results with a doctor just as conveniently.

One step along that path for telemedicine in Russia is the current development of the Unified State Health Information System (USHIS)[50].

The National Center for Informatization (NCI) has developed the Federal Register of Electronic Medical Documents (hereinafter — REMD) as a subsystem of USHIS in order to organize the collection of data from information systems in the health sector available in electronic medical documents created by medical organizations. One of its tasks is to ensure a comprehensive and smooth transition by medical organizations from a paper-based medical workflow to an electronic one with a legal structure. This transition will expand the use of interagency electronic interaction.

Legally structured electronic document management in healthcare will eliminate the possibility of losing or mutilating medical records. Medical organizations and doctors will, under lawful conditions, gain access to all patient medical documentation and thus improve the continuity of medical care. In other words, Russia's USHIS is creating its own version of electronic health records and a system to manage them.

At this stage it would come as a surprise if telemedicine in Russia would lag behind the rest of the world. All the countries that have placed a high

[49] The Code of Professional Ethics for a Doctor (adopted by the First National Congress of Doctors of the Russian Federation 5 October 2012). Available at: http://www.consultant.ru/document/cons_doc_LAW_174773/ (accessed: 29.04.2020)

[50] Unified State Health Information System. Available at: https://egisz.rosminzdrav.ru/ (accessed: 29.04.2020)

priority on telemedicine as Russia has are at the stage of implementation, testing or debugging electronic medical records. Russia's position at the forefront of this process is confirmed by the data of the Future Health Index 2019 report[51], in which Russia's way of introducing telemedicine is regarded as a valuable template that can be followed by all countries in improving their healthcare systems.

The report repeatedly refers to Russia as a forerunner and among the leading countries in telemedicine, and it notes the results that Russia has achieved in the dissemination of technology. Russia, along with some developing countries (India, Saudi Arabia, China), exemplifies the way that technologies are increasingly becoming part of the everyday healthcare experience for both health professionals and patients.

Russia is among the top countries ranked by the percentage of medical workers who currently use some kind of digital healthcare technology or mobile healthcare applications. The most common commercial telemedicine services at present are:

Yandex.Health[52] in which pediatricians, general practitioners, gynecologists, dermatologists, venereologists, gastroenterologists, neurologists, psychologists, pediatric psychologists, and cosmetologists make recommendations via chat or video links. They answer questions, create a medical record, and decrypt test results.

DocDoc (a project of Sberbank)[53] with a website and an application for smartphones. The service allows users to get advice and make appointments for diagnostics or examinations.

DOC + service[54] is available as a website and a mobile application. It receives a doctor's recommendations, can place calls to a doctor at a specific address, make an appointment, enable testing or other procedures at home, and order medicines from a pharmacy.

Medved.Telemed[55] is a system for remote consultation of doctors. In addition to the functionalities already described for the other services, this system has a convenient doctor interface that enables consultations and one-on-one chats.

---

[51] Ibid.

[52] Yandex. Health. Available at: https://health.yandex.ru/ (accessed: 29.04.2020)

[53] Docdoc service. Available at: https://docdoc.ru/ (accessed: 29.04.2020)

[54] Docplus service. Available at: https://docplus.ru/ (accessed: 29.04.2020)

[55] Medved. Telemed system for remote telemedicine consultations. Available at: https://telemed.mis-region.ru/ (accessed: 29.04.2020)

Qapsula[56] is an interactive support system for improving the effectiveness of prevention and treatment of various conditions. In addition to the option to consult with a doctor in any convenient format, the project has a program with a chat bot for webOS, iPhone and Android. It monitors physical activity and physical parameters, reminds patients of appointments with their doctors and when to administer tests and take medications.

Robomed[57] is an even more complex information system that, in addition to the usual telemedicine functionality, assists clinics in their business operations. The system automates and organizes the processes of a clinic by modeling its business in order to adapt quickly to the ever-present changes. The system stores all patient data in a single electronic chart, tracks rates of change and sets up a complete patient management cycle.

Medesk[58] automates a doctor's registry and workstation, online recording and telephone communications, cash flow and finances, warehouse and reporting, as well as more than twenty modules and extensions such as: online recording, registry, doctor's workplace, cash flow and finances, remote diagnostics, telephone communications, inventory accounting, and management reporting.

Other services such as Doctor Nearby, OnDoctor, Ok'Doctor, and Doctor Smart provide standard ways of consulting with a doctor.

Smartphone telemedicine applications in Russia as well as electronic devices for ECG, blood pressure measurements and various applications for chronically ill patients hold to the same standard of functionality as in other countries. Russia also has the Tyto Care apparatus that makes remote consultation more like a face-to-face visit.

Of course, not all the services now available will continue to advance and remain on the market. That depends to some extent on how telemedicine services develop. Will the doctor eventually have an option in the future to make a diagnosis and write prescriptions online? Will a patient be able to order medications at home?

Although telemedicine in Russia is relatively advanced in its pace of development, there are still problems that prevent those technologies from developing and penetrating faster. In a comparison of fifteen countries, Russians are among those who are most open to remote consultations as part of non-

[56] Qapsula personal assistant. Available at: https://qapsula.com/ (accessed: 29.04.2020)

[57] Robomed: about product. Available at: https://robo-med.com/about/ (accessed: 29.04.2020)

[58] Medesk Medical Information System. Available at: https://www.medesk.net/ru (accessed: 29.04.2020)

emergency care (55%). However, less than 25% of medical workers currently use telemedicine for doctor-patient interaction in their clinic or practice.

Doctors are more willing to interact online with another health professional (58% compared with the 15-country average of 47%) than with a patient (24% compared with the 15-country average of 30%)[59]. The main goal of doctors now is to use telemedicine to consult among themselves; doctors are just beginning to involve patients in remote processes. This is logical enough: first debug operating within an organization and then connect with its direct consumers.

Medical workers do not yet use all the capabilities of AI technology. Russian doctors use AI mainly for administrative tasks: recruiting staff and scheduling patients (70%), although the potential of AI is much greater when applied to telemedicine planning. AI has important uses in diagnosing patients, drawing up a treatment plan and recommending therapy. Here Russia is no forerunner when average AI use among the 15 countries surveyed is 45–47%, as in Russia it varies from 40 to 46%[60].

Despite the relatively high rate of using new technologies to track patients' health indicators (57% higher on average than in the 15 countries surveyed), 20% of patients do not exchange data with a doctor on an ongoing basis, and 50% of patients have never transmitted data to a doctor[61].

Lack of access to information exchange systems hinders the development of telemedicine technologies, and this means that potential users cannot see much advantage in using this kind of system. Of course, many of the holdouts are also concerned about privacy and data protection. But the main reasons why medical workers do not transmit data outside a medical institution (only 28% do so, but 80% transmit data within a medical institution) are a lack of access to a data exchange system (69%) and the lack of compatibility between different record-keeping systems (55%)[62].

Russian patients themselves note the importance of access to their medical data. Despite the fact that electronic medical records (EMR) are only 5% implemented, 68% of patients would like to have access to their data[63]. This indicates that providing Russian patients with access to their electronic medical records would improve public health.

---

[59] Future Health Index 2019. Report on Russia. Available at: https://www.philips.ru/c-dam/corporate/ru_RU/fhi/FHI_2019_Report_RUSSIA.pdf (accessed: 29.04.2020)

[60] Ibid.

[61] Ibid.

[62] Ibid.

[63] Ibid.

Despite the ease of use of EMR, security concerns remain the main obstacle; and this reluctance in turn slows down introduction of new medical technologies in everyday life. About 30% of those who have not yet used these technologies claim that they will start using them if they are sure that their medical data will be secure[64].

Table 1. SWOT analysis of the implementation of telemedicine technologies in medical organizations in Russia

Strength	1. Unified storage system 2. Instant access to patient information 3. Consultation for patients with disabilities 4. The possibility of early detection and diagnosis of patient conditions 5. Convenience for patients 6. Continuous monitoring of the health status of chronically ill patients 7. Improving compliance through 24-hour doctor communication
Weakness	1. Imperfect online diagnostic system (more details in section 3) 2. Low technical literacy of employees at medical institutions 3. Low technical literacy of older patients 4. Low internet availability in the regions 5. Difficulty in protecting patient personal data 6. Expensive equipment to ensure high quality data transfer (photos, videos) to doctors 7. Uncertainty about online consultation fees
Opportunities	1. Creation of a unified database of electronic medical records 2. Acceleration of medical diagnoses 3. Conducting consultations online 4. Simplified consultation with patients from remote regions 5. Effective use of human resources 6. Creating online training for medical staff 7. Creation of applications, devices with AI, simplifying diagnosis and making appointments for therapy
Threats	1. Dependence on smooth operation of hardware 2. Exposure to indeterminate financial and economic costs 3. Lack of a methodological base 4. Low awareness among telemedicine participants of its technological potential 5. False belief that telemedicine will replace health professionals 6. Complexity in system scalability 7. New legislation may introduce difficulties and restrictions on the functioning of the system.

[64] Ibid.

In the course of the research, the authors carried out a SWOT analysis was carried out to determine the current state of telemedicine in Russia. Table 1 presents the strengths and weaknesses of telemedicine as well as opportunities and threats to it. According to the results of the analysis, the goal of telemedicine should be "to make remote provision of medical services accessible and convenient."

In the course of the study, a survey was conducted of 264 medical staff (doctors, supervisors of doctors and deputies) at several medical institutions in Russia and in the city of Tomsk.

The questionnaire was provisionally divided into two blocks: an employee's experience in using telemedicine; and assessment of the outcomes of using telemedicine. The results of the questionnaire showed that telemedicine services were used by more than 80% of respondents.

Percentages of positive outcomes in using telemedicine are presented below (Fig. 4). The most positive is the ability to exchange experience with colleagues.

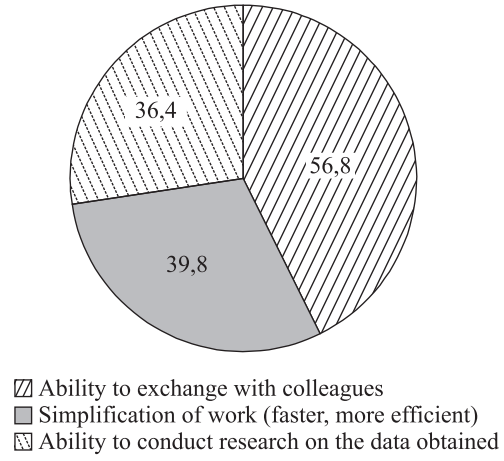


Fig. 4. Positive outcomes of using telemedicine

A part of the questionnaire addressed the best ways to use telemedicine (Fig. 5) and also difficulties in working with telemedicine technologies (Fig. 6).

The questionnaire showed that 80% of respondents use telemedicine technologies, but only 9% of them see any problems greater than system instability. That problem may prevent as much as 20% of the potential usage of telemedicine.

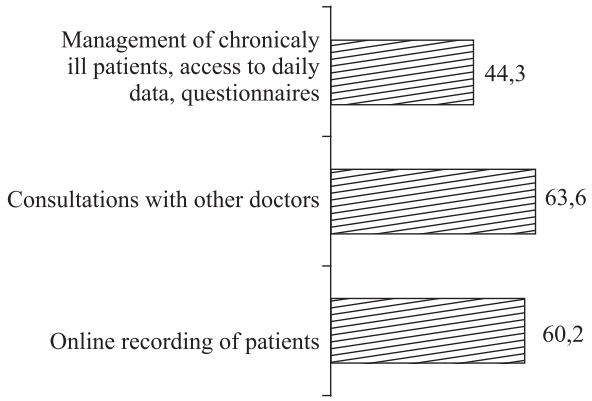


Fig. 5. The best ways of using telemedicine

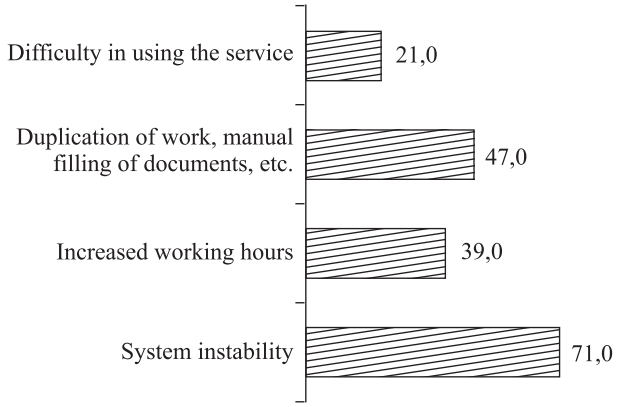


Fig. 6. Difficulties in working with telemedicine systems.

Despite the fact that 60% of respondents believe that telemedicine will increase the effectiveness of treatment (Fig. 7), medical personnel after the widespread introduction of telemedicine are apprehensive about increased work without increased wages and the likelihood that patient data will be leaked (Fig. 8).

These questionnaire results show that medical staff are generally ready to use telemedicine technologies.

During an interview one specialist respondent maintained that the development of telemedicine in Russia, more than in any other country, can and should be based on the long-standing traditions of layered healthcare, which has largely compensated for the negative effect of large distances and uneven development of regions with different population densities.

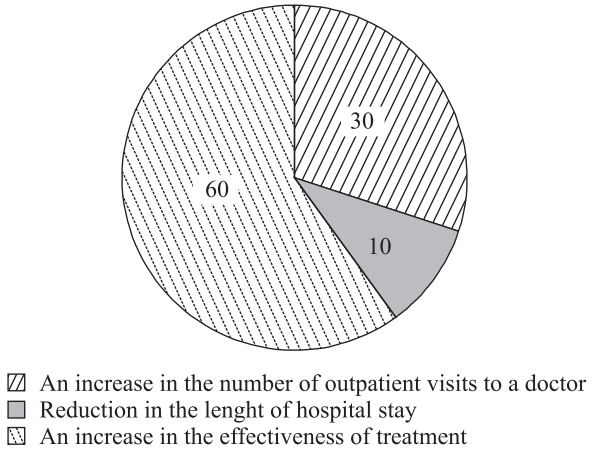


Fig. 7. Positive effects of telemedicine

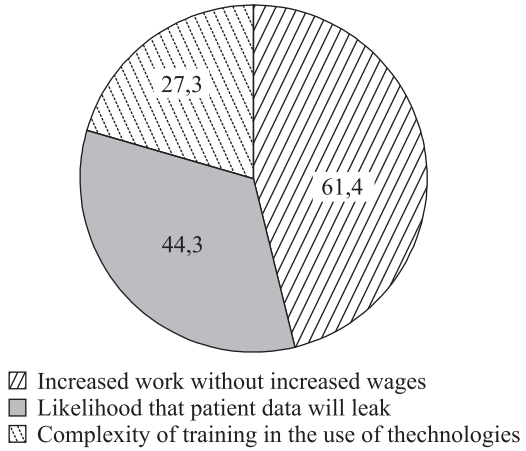


Fig. 8. Apprehensions of medical staff about more penetration by telemedicine

The development of telemedicine can have a significant impact on all the functions of the healthcare system, including the development and coordination of medical science, disease prevention, emergency and planned care, training and advanced qualification for personnel, and allocating material and technical resources.

Another specialist commented that the development of information technology opens up another prospect for the future, which would stand alongside remote consultations. This is the goal of forming a single history of human illness. When treating the same patient, doctors communicate with each other using extracts, which are clearly not enough. And even if

the patient has a consultation with the best possible specialist, all the data needed may still be lacking. In the future, when a unified medical telecommunication platform has been created, it would be realistic to arrange access to all of a patient's medical documents that are stored in various medical institutions for any location where those records are needed, including during telemonitoring of patients with special needs (physical disabilities, the elderly and others). In general, this task is much more complicated than arranging remote consultations, but it can be handled in stages.

These comments indicate that medical workers in Russia become quite ready to implement AI and other technologies into their usual processes once they understand how using them simplifies their work and they understand how to use them.

Unfortunately, the introduction of technologies in areas where doctors have always made decisions on their own (diagnostics, prescribing therapy, etc.) will take longer. Innovations of that kind will require a process of gradual familiarization and incremental experience in their use.

Patients are enthusiastic enough and are already using the new technologies at the same pace as doctors do for their administrative tasks (65-70%). But, as the statistics of the report show, the health professional is the weak link in doctor-patient interactions. Healthcare staff see working with devices for constantly monitoring the state of health as something new, and they still have little experience in using those technologies. Although the percentage of patients using technology is quit high (compared to other countries), the data generated is not transmitted probably because doctors will not handle it properly. One solution might be to recognize the importance of educating medical staff in the use of new technologies and motivating them, possibly through bonuses.

Judging by statistics and the results of surveys, telemedicine is coming together like the pieces of a puzzle: the way patients and medical workers are beginning to use telemedicine technologies quite extensively counts as a piece or two in place, but the lack of interconnections for information exchange is a piece still missing. The importance of patient access to their medical data is supported by evidence that patients with access to their EMR are more proactive (9%). And even those Russians who do not have access to EMR say they would like their doctor to have access to it when he is treating them. Patients are more likely to cooperate with medical workers when they have information about their health.

Doctors are beginning to use telemedicine, especially for doctor-to-doctor communication, but the development of doctor-patient telemedicine is

hindered by those missing puzzle pieces: everyone understands what the benefits of using it can be, but how to build it, how to make it work, how to connect systems, and how to set up the correct exchange of data between medical institutions are all pieces yet to be found.

To fill in the missing pieces, it is important to analyze all the systems in operation and determine a protocol of interaction common to them all so that the system chosen by a medical institution does not prevent its interaction with others. This process will have to avoid creating artificial barriers, gather information about the interactions that need to take place, and analyze those interactions in order to determine new paths for telemedicine's future.

3. Telemedicine vs COVID-19: Challenges and Opportunities

At a time when social distancing is one of the main ways to combat the COVID-19 pandemic, telemedicine is becoming a key technology for safe and effective communication. The World Health Organization has mentioned telemedicine[65] among its core services in the policy brief "Strengthening the Health System: A Response to COVID-19." This new WHO policy indicates that, as part of optimizing service delivery, telemedicine should become one of the alternative models for providing clinical services and supporting clinical decision-making.

The COVID-19 pandemic has taken telemedicine to a new level. As healthcare providers must remain healthy, the need for remote technology has increased by an order of magnitude. The Center for Disease Control and Prevention (CDC) and WHO advocate using telemedicine to monitor patients and reduce the risk of spreading the virus through visits to hospitals. The Academy of Family Physicians[66] and the American Medical Association (AMA)[67] have

[65] Strengthening the Health Systems Response to COVID-19. Technical guidance #1: Maintaining continuity of essential health care services while mobilizing the health workforce for COVID-19 response. Available at: https://euro.sharefile.com/share/view/sbc0659718fd4c8aa (accessed: 29.04.2020)

[66] Using telehealth to care for patients during the COVID-19 pandemic. Available at: https://www.aafp.org/patient-care/emergency/2019-coronavirus/telehealth.html (accessed: 29.04.2020)

[67] Key changes made to telehealth guidelines to boost COVID-19 care. Available at: https://www.ama-assn.org/delivering-care/public-health/key-changes-made-telehealth-guidelines-boost-covid-19-care (accessed: 29.04.2020)

issued similar guidelines. The US government has also taken significant steps[68] to expand telemedicine services.

The Centers for Medicare & and Medicaid Services (CMS) in the US have expanded Medicare coverage for telehealth visits, the Office for Civil Rights (OCR) under the US Department of Health and Human Services (HHS) announced it will waive potential HIPAA penalties for good faith use of telehealth during the emergency. One other US institution, the HHS Office of the Inspector General (OIG), provided flexibility for healthcare providers to reduce or waive beneficiary cost-sharing for telehealth visits paid by federal healthcare programs.

There are also telemedicine initiatives apart from the US government, such as the Bergen-New Bridge Medical Center, specializing in telemedicine for COVID-19[69]. With their partner Air Visits, Bergen New Bridge Cares offers urgent-care remote screening and assessment by a licensed physician of patients who have medical complaints and symptoms. Telehealth consultations with an infectious disease physician are available if necessary.

In the EU countries there is an imbalance and shortage of medical workers[70] as well as unequal quality and access to medical services. The number of doctors varies from 1.9 in Turkey to 5.2 in Austria per 1,000 people[71]. The health workforce structure is changing[72], as one in three doctors is over the age of 55. This situation has become especially critical and has yielded dire results during the pandemic. Healthcare professionals who are in the forefront of the fight against the COVID-19 epidemic have the highest risk of infection. Telemedicine can help reduce this risk by minimizing face-to-face interactions.

---

[68] Secretary Azar announces historic expansion of telehealth access to combat COVID-19. Available at: https://www.hhs.gov/about/news/2020/03/17/secretary-azar-announces-historic-expansion-of-telehealth-access-to-combat-covid-19.html (accessed: 29.04.2020)

[69] Bergen New Bridge Medical Center expand telehealth service for COVID-19. Available at: https://www.globenewswire.com/news-release/2020/03/03/1994551/0/en/Bergen-New-Bridge-Medical-Center-Expand-Telehealth-Service-for-COVID-19.html (accessed: 29.04.2020)

[70] Transformation of health and care in the digital single market — Harnessing the potential of data to empower citizens and build a healthier society. Available at: https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_ehealth_infographic_en.pdf (accessed: 29.04.2020)

[71] Strengthening the health system response to COVID-19. Recommendations for the WHO European Region Policy brief available at: https://euro.sharefile.com/share/view/s5af6405658d-4b0eb (accessed: 29.04.2020)

[72] Health Workforce. Data and statistics. Available at: http://www.euro.who.int/en/health-topics/Health-systems/health-workforce/data-and-statistics (accessed: 29.04.2020)

Telemedicine can provide more choices of effective measures to combat COVID-19 for different categories of people in the following ways.

For self-isolated citizens: remote monitoring of health status, online consultation with a doctor, the ability to order medicines at home; and the possibility of using online questionnaires and consultations to determine the need for hospitalization and ambulances.

For patients in home treatment (chronically ill, patients with COVID-19 or other mild diseases that do not require a hospital): remote monitoring of the disease 24/7 and monitoring of treatment by a doctor, online communication and video consultations.

And, of course, for doctors with mild symptoms of COVID-19: the ability to work with patients remotely and to consult doctors working in the hospital.

Special attention should be paid to staff training during the pandemic, especially for hospital recruits. This would include the ability to control information through a dashboard or automated matrix to assess the situation in real-time (with the ability to have a more experienced specialist intervene promptly in the treatment process), to create a plan for the incidence of disease (to simplify the control of the course of the disease), and to use of electronic textbooks and video broadcasts to bring new recruits up to speed.

The COVID-19 pandemic is a challenging test for all telemedicine solutions[73] as well as an opportunity to prove how reliable and flexible they are in the new environment.

Although telemedicine offers the many features and advantages already described, it has some drawbacks and associated risks. The first risk is of misdiagnosis because of the difficulty or impossibility of differentiating among diseases by relying only on patients' reports of their symptoms. In online consultations patients often cannot provide more than superficial and general symptoms that will be insufficient for detecting certain less obvious conditions. For example, if a parent informs their pediatrician that a child has a fever, a sore throat and a slight cough, then any treatment prescribed on that slim basis could be absolutely useless because no one has examined the child's mouth, throat, or skin. The symptoms would be consistent with a simple cold, but acute infections such as scarlet fever, measles, or diphtheria could not be ruled out and might prove fatal if not promptly diagnosed.

[73] COVID-19: A continuously evolving process that requires adapting by the hour. Available at: https://www.healthcareitnews.com/news/europe/covid-19-continuously-evolving-process-requires-adapting-hour (accessed: 29.04.2020)

Without the proper treatment the situation may have become irreversible in as little as two days. Doctors can diagnose such diseases or prescribe treatment for them with maximum accuracy only after a comprehensive physical examination and seeing the results from the necessary tests.

Another risk of misdiagnosis is that a symptom may go unnoticed online. A patient's appearance including their complexion and body position can be very informative. For example, if there are complaints of abdominal pain, then palpation is necessary in addition to hearing the patient's account of their condition. One of the symptoms of appendicitis is pain felt in the right iliac region when the front abdominal wall is tapped with one's fingertips. A person without a medical education will not be able to tap in the correct way and may leave out some significant details. Even body position is sometimes informative, but a patient will not always be aware of changes in it. If the patient is aware of some changes, a doctor who is new to video consultations and is used to observing body position during a face-to-face physical examination without needing to ask may overlook that point and not ask about it online.

Allergic reactions to medications constitute another major source of risk. Even if the doctor has asked all the appropriate questions during an online consultation, the patient may not be aware of an allergy, especially one to a medication being prescribed for the first time. At an appointment in person, emergency medical care (up to and including resuscitation) can be promptly given to a patient undergoing an allergic reaction; after an online consultation that will not be the case.

The patient also may not provide a complete and reliable history, since they may not understand what exactly is happening and can easily to underestimate the seriousness of their symptoms or exaggerate it. It goes with saying that patients are unlikely to accurately diagnose themselves. Even a patient's readings from measuring and monitoring devices may be doubtful, and telemedicine presupposes that the data sent using those devices will be correct and verifiable. However, the accuracy of the measurements sent to the doctor remotely depends on the patient.

When doctors cannot make a definite diagnosis, patients are tempted to use telemedicine not to get a referral to a specialist, but instead to avoid a stay in the hospital by picking up hints about possible diagnoses and self-medicating, which can cause patients a great deal of harm. The risks from self-medication are much greater in Russia because many medications that require prescriptions in the US or EU are available on-demand at any pharmacy in Russia.

The delivery of medications is the final area of risk that should be noted. The main problem is with quality of the medications delivered and the storage conditions during delivery. For example, a trained specialist should handle thermolabile preparations in order to ensure their effectiveness and safety. Prescription medication delivery must also involve a pharmacy or pharmacist. It is quite possible that medications delivered remotely will be of doubtful quality (if proper storage conditions are not provided) or that slow delivery or high cost for prompt delivery will make the service unsuitable for many patients.

The unprecedented acceleration in the development of telemedicine that COVID-19 has brought about should have happened many years ago. A better telemedicine system would have protected countless high-risk people from exposure to the coronavirus. But it took a pandemic to drive the change.

For many years, the advance of telemedicine has been inhibited by the inertia of regulations that are failing to keep pace with the development of information technology. Of course, it is not advisable to enact legislative acts for regulating telemedicine technologies in haste. Rushing into legislation will affect its quality and can harm the telemedicine system by forcing it to develop in ways that may sacrifice some of its advantages. But the current situation should become a catalyst for legislation to better accommodate telemedicine.

Measures to adapt healthcare legislation to the challenges of COVID-19 were quickly put in place in the first weeks of the pandemic in Russia,

First, the remote sale of medications was legalized[74]. Pharmacies licensed in Russia can now sell over-the-counter preparations remotely once they obtain official approval of the oversight bodies for this type of sale. In addition, in an emergency situation and (or) when there is a threat of the spread of a disease that poses a danger to others, the Government of the Russian Federation can establish a temporary procedure for the remote sale of prescription medications (with the exception of narcotic and psychotropic drugs, as well as preparations with ethyl alcohol content of over 25%) in additions to over-the-counter ones.

[74] Federal Law dated 3 April 2020 No. 105-FZ "On amending Article 15.1 of the Federal Law 'On information, technologies and the protection of information' and the Federal Law 'On distribution of medicines'". Available at: http://www.consultant.ru/document/cons_doc_LAW_349322/ (accessed: 29.04.2020)

Second, a bill was introduced in the State Duma of the Russian Federation that expands the capabilities of telemedicine during a pandemic[75]. Specifically, the bill establishes the right of the Government of the Russian Federation in emergency situations and (or) when there is a threat of the spread of a disease that poses a danger to others to establish the scope of medical care provided through telemedicine technologies. Russian law at present permits the use of telemedicine only for consultations on prevention and diagnosis and for monitoring a patient's health; it can also be used to decide whether a patient should be referred to a medical professional for an examination in person. At the same time, current law prohibits the use of telemedicine for an initial diagnosis and for prescribing treatment remotely.

It is noteworthy that the legislation expanding the use of telemedicine in Russia was being drafted before the pandemic, but progress was slow. The threat of COVID-19 instantly accelerated that process.

Changes in the health insurance system that explicitly included telemedicine services as covered expenses are another way to facilitate use of telemedicine in a pandemic. This path was followed by the US federal government with the announcement that it would waive restrictions on telemedicine services for the elderly under its Medicare insurance program. Some states in the USA have already passed laws requiring private insurance companies to reimburse the cost of telemedicine services on the same basis as conventional health services (parity private insurance coverage for telemedicine).

Nevertheless, optimal development of telemedicine cannot be assured with narrowly targeted or temporary measures. Standardization and comprehensive development of legislation is required, and this requires thorough analysis in order to determine which diagnoses can be made online and which require appointments in person. It is important to standardize the procedure for online consultations so that older doctors can quickly adjust to the new way of interacting with patients. This requires a sustained approach and will take some time.

Another deficiency in telemedicine that became obvious during the pandemic is the limited scalability of the system that was in place. This limitation became more acute because of the sharply increased demand for telemedi-

[75] The Government of the Russian Federation may receive the right to establish the features and procedures for the provision of medical care in emergency situations and in the event of a threat of the spread of a dangerous disease, including using telemedicine technologies. Available at: http://www.consultant.ru/law/hotdocs/61143.html/ (accessed: 29.04.2020)

cine during the pandemic. The technology was not ready for such a heavy load because the pandemic had not been anticipated. Prior to COVID-19 telemedicine was expanding at a steady but rather slow pace in keeping with the modest progress in changing its legislative framework.

The main requirement for telemedicine in a pandemic is to accommodate an increase in within a few hours, not over several days. When there are so many new users, telemedicine solutions should be an easy-to-use tool and accessible through any user device: computers, smartphones, laptops and tablets. The ability to integrate digital medical devices with telemedicine solutions would be an important step forward.

Cloud telemedicine services are the most effective tools at present. But cloud technology is not completely reliable and is therefore only a forced and temporary solution. The main problem with relying on cloud technologies is that they cannot properly guarantee the security of the large amount of personal data they contain.

If a large-scale telemedicine infrastructure had been created earlier, new and existing services would not have been overwhelmed by the unprecedented increase in demand. PlushCare reports that the number of appointments has increased by 70%; Amwell has confirmed that since the virus appeared in the USA in January, application use has increased by 158% nationwide and increased by 650% in the state of Washington[76].

Although the risks described above clearly require a thorough assessment and preparation of the legislative framework, the need to develop telemedicine technologies and apply them broadly has become apparent. In less than ten years, the world has encountered diseases such as the MERS virus, Ebola, Zika, and COVID-19. The prevalence of COVID has clearly underlined the importance of telemedicine, and key stakeholders must adopt the technology and make it an integral part of the healthcare system. This will advance the agenda for expanding digital healthcare in general while also preparing better for a potential emergency. Training and experience in using telemedicine will allow us, as far as possible, to survive such epidemics by reducing the burden on medical staff and enabling them to promptly suppress outbreaks or to avoid their rapid emergence and spread.

The pace of development of telemedicine should not be halted or slowed down after the world comes to terms with the pandemic. Telemedicine

[76] Telemedicine struggles to be an option for everyone in the wake of coronavirus. Available at: https://qz.com/1821549/telemedicine-faces-unprecedented-demand-in-the-wake-of-coronavirus/ (accessed: 29.04.2020)

should not be merely a temporary solution which falls short of its full potential and will not be ready to handle the next emergency. If that is allowed to happen, we can expect hospitals and doctors to be overloaded once again. The savings in time and the flexibility provided by telemedicine tools will benefit patients who are uncomfortable with visiting a doctor and also chronically ill patients who may experience panic, disorientation and trauma during transportation to a medical facility. The risk of contracting an infection while visiting a hospital will still be there after the pandemic.

This crisis gives us an opportunity to reorient healthcare and has shown everyone affected the convenience and potential of telemedicine.

4. The Future of Telemedicine in Russia: Integration, Data Analysis, and Personalization

Russia must first put the pieces of its telemedicine puzzle together by establishing communication and data transfer between medical institutions. Integration will be the first requirement for the future development of telemedicine.

Integration involves connecting the maximum number of providers and users of medical information to a unified system with both private and public healthcare organizations linked to it. The way electronic documents are managed in telemedicine should permit other organizations involved in research and developing innovative healthcare solutions along with others to connect to a single information system. Further integration of information systems and the involvement of new organizations in it will increase the availability, completeness and reliability of information about the health of the population.

In order for telemedicine to provide all the benefits claimed for it, medical workers should find that it eases their workload without introducing complications, Therefore integration should include electronic medical records (EMR), medical information systems (MIS), telepresence. and integration of data from mobile applications and patient devices.

EMR includes detailed documentation of visits, and their integration will prevent losing records and make the documentation more accessible to both doctors and patients. This will allow telemedicine to improve coordination of care and patient outcomes. It is also convenient for the patients themselves. With access to EMR, they can easily collect the necessary documents on the history of their condition at the request of a new or different doctor.

MIS is integration between different medical information systems (MIS) within the same medical institution or between different ones. This will allow sharing data quickly and make doctor-to-doctor interactions more productive by exchange of the results of clinical trials and other important statistics. The patient will no longer have to locate paper records of tests and other documents; they can be confident that their doctor will already have access to all the necessary data.

Telepresence and rehabilitation robotics refer to a whole range of technologies that multiply the effectiveness of medical professionals by letting them interact with patients who are elsewhere. This technology can be used, for example, for concussions or other diseases that require constant monitoring: a robot can monitor the patient's behavior, notify medical personnel of significant changes and send alerts to a medical officer or doctor. The patient's condition is continuously monitored, but the doctor can deal with other patients in another place.

The final piece of the integration puzzle brings in data from mobile applications and patient devices. This is especially valuable for chronically ill patients whose state of health can be constantly monitored. Many patients with diabetes, for example, must now manually transfer data to the doctor by sending complicated tables or files in formats which differ depending on the program and device. In addition to the inconvenience for patients, this reduces the efficiency of doctors because data analysis takes more time. Statistical analysis, if it can be done at all, is also more difficult than it would be with comprehensive integration of patient data into the physician's system so that all data is stored in EMR.

Of course, telemedicine has some definite limitations: doctors cannot conduct all diagnostic measures only by remote means. But modern technologies such as Tyto Care are making remote visits to a doctor as much like appointments in person as possible.

The integration that goes beyond the different systems used by medical institutions to incorporate applications for patients and various devices will permit continuously gathering vital data and monitoring a patient's health in a much more effective way, and it will be useful for some kinds of prevention.

Data collection and analysis stand out among the new possibilities for telemedicine that integration opens up. The concentration of the most complete amount of information about the health status of the population, preferably in a fairly structured form[77], will benefit from modern methods

[77] Existing cognitive technologies are already capable of working quite effectively with unstructured information; however, the more structured data is processed, the more accurate are the results of their processing.

of data analysis. Realization of this potential of electronic document management in telemedicine will make it possible to conduct minutely targeted medical research and process large amounts of medical information for socially significant purposes, which is a priority in building a digital economy in Russia and abroad.

Ensuring the mobility and responsiveness of data processed in health information systems is also necessary to maintain constant and ubiquitous access to relevant health information. For these purposes, it is important to ensure the technical compatibility of information systems with various types of devices, as well as to create opportunities for regularly updating information stored in these systems. These requirements are especially important in the dynamic monitoring of the health status of patients as dynamic monitoring is carried out by different devices. The information received from such devices needs to be synchronized, both between them and with information stored in information systems. At the same time, dynamic observation is useful for promptly taking emergency measures whenever necessary. Without constantly updating data in information systems, it is impossible to respond proactively to changes in the health status of patients. Of key importance in the legal provisions for the mobility and responsiveness of medical data are standards, technical regulations and other ways to unify the technical characteristics of medical devices and data processing.

Many companies such as Yandex. Health note that the motivation for large players to create telemedicine companies is not so much to add to their earnings by enabling remote consultations but rather to collect and analyze data. Yandex maintains that, after collecting millions or tens of millions of results from consultations or medical histories, processing technologies (such as AI) will make it possible to predict the course of diseases, the speed of recovery, and the reactions of a particular patient with a certain dataset to a prescribed medication.

This kind of analysis will take medicine to a completely different level. For example, it will be possible to use digital patient-oriented technology, as is done at the Teknon Medical Center in Spain[78]. When using it, doctors carefully examine each patient and build a 3D model; they can then compare the patient's indicators with those from the existing database in order to objectively choose the best treatment technique and avoid medical errors.

Data collection will also enable technologies that track patient compliance. Compliance is the degree of correspondence between the patient's be-

[78] Available at: http://www.teknonbarcelona.com/en/hospital (accessed: 29.04.2020)

havior and the recommendations received from the doctor. This is an important issue for medicine in general, and doctors are making attempts to predict compliance, although it is very difficult to do this on their own. The more data there is to process, the more possibilities it will generate.

If we attempt to foresee what telemedicine will become over several generations (and not over a one-year horizon), then in this future we might reasonably expect that patients will be able to find out their prognosis for inherited illnesses and a recommendation of the most suitable treatment. The earlier a disease is diagnosed, the easier and faster it can be cured or prevented. With better knowledge about susceptibility to diseases, better measures could be taken to prevent them.

Therefore, data analysis will make telemedicine as personalized as possible and select the treatments that are most likely to work for a particular patient. In the past doctors would arrive at treatment plan for a patient based on the results of detailed questioning that went beyond the immediate effects of the disease to inquire about the patient's way of life, career and family history as a supplement to a thorough physical examination and the targeted use of measurements and laboratory tests. The integration of data with patient applications and devices feeding in analyzed information about the course of any of a patient's diseases throughout their life will make that process many times faster and more accurate. This is especially important for cancer, cardiovascular diseases, and metabolic diseases, that is, for those diseases that have the greatest negative impact on health and life expectancy.

Personalized medicine is the most valid way to construct a plan for examining and treating a patient, predicting the course of a disease, determining the effectiveness and possible side effects of medications, and also for selecting personalized treatment regimens, such as the chemical or biological products that are best for reaching molecular targets like the cell receptors of a particular tumor in a particular patient [Bodiroga-Vukobrat N. et al., 2016: 6].

Robust ways of processing information (collection, storage, transmission, etc.) will be needed to realize the potential advantages of telemedicine. Information in telemedicine can be collected from various sources and even without the direct involvement of a person through sensors and other devices through what is called "machine-generated data" [Drexl J., 2016]. It can have both a structured and unstructured form, be stored in different formats, and processed by different persons and organizations for various purposes. The lack of a unified technical, organizational and legal foundation for processing medical data in health information systems is a signif-

icant barrier to information exchange and the successful development of telemedicine.

The key modern legal challenges for the development of telemedicine are information security and the protection of personal data.

E-health is one of the areas most prone to cyberattacks. For example, in the Australian Notifiable Data Breaches Report for 2018, the largest number of cybersecurity incidents among all vulnerable areas was recorded in healthcare [Burke W. et al., 2019]. Statistics show a rapid increase in the number of cyberattacks on health information systems worldwide, and the total damage from incidents for the industry is measured in billions of US dollars. According to a global study by Cybersecurity Ventures in 2017, between 2015 and 2017 the number of fraudulent cyberattacks in the healthcare sector increased 15 times, and it will probably increase another 4 times in 2020[79].

The main kinds of cyberattacks on medical facilities are infection with malware and hacking employee accounts[80]. In Russia there has been an increase in the number of internal leaks of medical data due the negligence of employees at medical institutions[81], and this underlines the need to defend against both internal and external threats to data security.

To ensure information security in telemedicine, it is important to verify that medical equipment and the devices (medical devices) and applications (software) used to transfer information between nodes of telemedicine services and the processing of data are also protected. Data security should be a top priority in applying the "internet of things" to medicine, perhaps through devices implanted in the human body that would make up an "internet of people" [Burleson W. et al., 2014], whose architecture still requires additional solutions for information security [Sicari S. et al., 2017: 39–74].

To increase the information security of medical devices, the principles of built-in security [Babar S. et al., 2011: 1-5] and privacy by design [Demetrius K., 2014] should be applied, taking into account the risks of violating the integrity and confidentiality of information and also incorporating mechanisms to counter these violations as the technical architecture of the products is designed and built [Purtova N. et al., 2015: 61]. These principles

[79] Global Ransomware Damage Costs Predicted To Exceed $5 Billion In 2017. Available at: https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/ (accessed: 01.10.2019)

[80] Actual cyber threats. Q1 2019. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1-2019/ (accessed: 29.04.2020)

[81] The number of domestic leaks of medical data has risen sharply in Russia. Available at: https://www.osp.ru/medit/2018/08/13054369.html (accessed: 29.04.2020)

should be considered when developing standards and technical regulations and in preparing technical specifications for product development, etc.

Ignoring the problems of information security cancels out all the advantages of telemedicine technologies because the degree of information security will determine people's trust in the new technologies and their willingness to pass an extremely important part of their lives into the "hands" of computers, communication networks, information systems and algorithms. The physical security of patients ultimately depends on information security in telemedicine. Only high standards of information protection and a reasonable balance between public and private interests concerning information can legitimize the use of new technologies in healthcare.

The bulk of the information processed in telemedicine is information about individuals, which makes it necessary to comply with the requirements for the protection of personal data when processing it. Moreover, such information is mainly personal health information, the processing of which is subject to even more stringent legal requirements. The requirements for processing personal data protect the right to privacy, but they also act as restrictions on the widespread use of telemedicine technologies for various purposes including in medical research.

Addressing issues in processing personal health data for research purposes, as well as issues in the legal system for handling anonymized personal data, should have a high priority because the options and conditions for using medical data in the digital economy and consequently the potential level and paths of development in e-health depend on the market for telemedicine services.

Legal regulation of personal data processing (including medical data) for research purposes is a problem both in Russia and in other countries. EU countries have made attempts to set conditions that allow more liberal processing of personal data for research purposes (Sjöberg C., 2017), and the problem was raised during the development of EU Regulation 2016/679 (GDPR).

The new European regulation establishes a broader basis for processing sensitive personal data without the consent of the subject. In particular, that data can be processed when it is serves a significant public interest as identified in the legislation of the EU and EU countries (paragraph 2(g) of Article 9 of the GDPR); in the provision of medical care, management of the healthcare system and healthcare services (paragraph 2(h) of Article 9); for the realization of public interest in healthcare (paragraph 2(i) of Article 9); and for the purpose of scientific, statistical research (paragraph 2(j) of Article 9). Also,

paragraph 4 of Article 9 of the Regulation allows EU countries to establish in national legislation other conditions for processing personal health data.

These new foundations were reflected in the Regulation in response to the needs of the digital age and in connection with advancing information processing capabilities such as ways of processing Big Data and machine learning. The codification of valid grounds for processing special categories of personal data without the consent of its subject, as conceived by the developers of the Regulation, should contribute to a more efficient use of data for socially useful purposes. The fundamental rights and freedoms of the subject of personal data when processing their data is justified on these grounds should be ensured by observing organizational and technical data protection measures and ethical standards. Processing of personal data about state of health for scientific or statistical purposes should comply with the principle of minimization (Article 89(1) of the GDPR). If the goal of data processing is attainable without identifying its subjects, then measures must be taken to anonymize or pseudonymize data so that processing does not diminish the essence of the right to protect personal data, and it must be carried out with the adoption of measures to protect the fundamental rights and interests of the personal data subject.

Russian legislation on personal data permits processing personal data for statistical or other research purposes without the consent of the personal data subject only for ordinary personal data and only subject to their depersonalization. With regard to special categories of personal data, which include health data, processing for statistical and other research purposes is possible only with written consent, regardless of the depersonalization of data. It seems advisable to extend permission to process those special categories of personal data for statistical and other research purposes on a similar depersonalized basis. That would require clearly defining the depersonalization of personal data which makes processing personal data without consent permissible. Accreditation of data operators or processors and enforceable ethical standards for data processing are additional ways to safeguard the interests of personal data subjects

Conclusion

Although telemedicine is developing and regulated differently in each country, there are some common trends: the collection and analysis of medical records and patient histories; devices and systems to simplify commu-

nication between doctors, home-use devices for chronically ill patients; and efforts to increase the effectiveness of online examinations.

Telemedicine also has obstacles to development common to all countries: a country's culturally determined attitudes, legislative barriers, distrust of new technologies, and incompatibilities in information systems.

A key development trend for telemedicine globally is EHR. And there are a number of sound reasons for this: data on the patient's condition are stored in a safe place, contain a history of changes in the patient's body throughout their lives, and systematize all information; this enables the implementation of particular programs to monitor the quality of healthcare in a country.

Because traditional legal provisions do not take into account the distinctive features of telemedicine, new legislation must be enacted to protect the rights and legitimate interests of legal entities in telemedicine and remove unreasonable legal obstacles that impede the use of telemedicine technologies. How long those legislative changes will take and whether they will keep pace with the development of telemedicine remains an open question.

Russia is no exception in its adjustment to telemedicine: it has its own characteristic medicine and telemedicine, but legislation is more an obstacle to development than a catalyst. Once the legislative issues are resolved, Russian telemedicine should reach a new level because of its special features: free medical care and medical examination, rapid availability of appointments with doctors, access to medicines, acceptance of alternative medicine, and a personal approach by health professionals.

The COVID-19 pandemic may be acting as another kind of catalyst for telemedicine because social distancing is one of the main measures used to combat it. Telemedicine fits in as a key technology for safe and effective communication concerning diagnosis, treatment and monitoring. The world is now considering the benefits of telemedicine that it previously neglected. Of course, telemedicine has its risks and disadvantages, but its usefulness in combatting a pandemic are undeniable.

Survey results showed that in Russia medical workers are ready to implement AI and other technologies in their usual workflow, provided that they understand how this simplifies their tasks. And patients in turn are ready to use new technologies and already are using them to about the same extent as doctors do (65–70%).

Judging by statistics and the results of surveys, telemedicine is developing like pieces in a puzzle: various providers, patients and medical workers are beginning to use telemedicine technologies quite frequently, but the interconnections for information exchange have not yet been set up.

In order to assemble all the pieces of the puzzle, it is important to analyze all the systems in operation and determine a protocol of interaction common to all of them so that the system chosen by a medical institution does not interfere with its interaction with others. This will prevent creating artificial barriers, and at the same time the data collected on interaction and its analysis can point the way to new paths for the development of telemedicine.

For many years telemedicine was held back by regulations that failed to keep pace with the rapid development of information technology. But now it is very important to resist the urge to hastily draft legislative acts for regulating telemedicine as a response to an emergency; what is needed is a sound legislative framework for telemedicine on an ongoing basis. Otherwise, the rush to legislate may result in regulations of low quality, which may impair the telemedicine system by forcing it to develop along lines that prevent it from providing all its potential benefits.

The pace of development of telemedicine should not be halted or slowed down after the world comes to terms with the pandemic.

This article is an attempt to discern the future for telemedicine in Russia and has identified key areas in it: integration, data analysis, and personalization. These development paths will open up completely different possibilities for using telemedicine: it will be possible to analyze data and use the analysis to predict any disease of any person for their whole life. That kind of forecast will make it possible to prevent the occurrence of a disease rather than combat it after it has taken hold. The population will be healthier and therefore more productive, which will certainly have a positive impact on the well-being of the country as a whole.

References

Babar S. et al (2011) Proposed embedded security framework for Internet of Things (IoT), 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), Chennai, pp. 1–5.

Bodiroga-Vukobrat N. et al (2016) *Personalized Medicine. A New Medical and Social Challenge*. New York: Springer, 278 pp.

Burke W. et al (2019) Cybersecurity Indexes for eHealth, pp. 1–8. Available at: https://www.researchgate.net/publication/330371852_ (accessed: 01.10.2019)

Burleson W. & Carrara S. (eds.) (2014) *Security and Privacy for Implantable Medical Devices*. Berlin: Springer-Verlag, 205 p.

Carlisle G., Whitehouse D. & Duquenoy P. (eds.) (2013) *eHealth: Legal, Ethical and Governance Challenges*. New York: Springer, 396 pp.

Currie W. & Seddon J. (2014) A cross-national analysis of eHealth in the European Union: Some policy and research directions. *Information & Management*, vol. 6, pp. 783–797.

Davis K. et al (2014) Mirror, mirror on the wall. How the performance of the U.S. health care system compares internationally. Available at: http://www.commonwealthfund.org/~/media/files/publications/fund-report/2014/jun/1755_davis_mirror_mirror_2014.pdf (accessed: 01.08. 2019)

Demetrius K. (2014) *Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century*. Berlin: Springer, 338 pp.

Drexl J. (2016) Designing competitive markets for industrial data: Between propertisation and access. Max Planck Institute, Research paper no 16, 70 pp.

Flodgren G. et al (2015) Interactive telemedicine: effects on professional practice and health care outcomes. *Cochrane Database of Systematic Reviews*, issue 9. Art. No.: CD002098. DOI: 10.1002/14651858.CD002098.pub2/ Available at: https://www.cochrane.org/CD002098/EPOC_interactive-telemedicine-effects-professional-practice-and-healthcare-outcomes) (accessed: 12.05.2020)

Moy F.et al. (2019) Techniques of monitoring blood glucose during pregnancy for women with pre-existing diabetes. *Cochrane Database of Systematic Reviews*, issue 5, CD009613. DOI: 10.1002/14651858.CD009613.pub4. Available at: https://www.cochrane.org/CD009613/PREG_methods-monitoring-blood-glucose-pregnant-women-diabetes-improve-outcomes (accessed: 12.05.2020)

Oliveira T., Branquinho M. & Gonçalves L. (2012) State of the art in telemedicine. Concepts, management, monitoring and evaluation of the telemedicine program in Alentejo. *Studies in Health Technology and Informatics*, vol. 179, pp. 29–37.

Purtova N.N., Kosta E. & Koops E. (2015) Laws and regulations for digital Health. In: S. Fricker et al (eds.) *Requirements Engineering for Digital Health*. Berlin: Springer, pp. 47–74.

Putilo N.V. & Volkova N.S. (2018) Telemedicine: Societal Needs and Possibilities of Legislation. *Zhurnal rossiyskogo prava*, no 6, pp. 124-135 (in Russian)

Sicari S. et al (2017) A policy enforcement framework for Internet of Things applications in the smart health. *Smart Health*, September 2017, pp. 39–74.

Sjöberg C. (2017) Swedish Proposal for Research Data Act. Paper presented at XXXII Nordic Conference on Legal Informatics. Available at: http://www.jus.uio.no/ifp/om/organisasjon/seri/arrangementer/2017/sjo%CC%88berg.pdf. (accessed: 29.04.2020)

Wernick A. & Klünker I. (2019) Prohibitions on long distance treatment: Historical roots and continuities in limiting the use of electronic telemedicine. In: T. Bächle & A. Wernick (eds.) *The Futures of eHealth. Social, Ethical and Legal Challenges*. Berlin: Humboldt Institute for Internet and Society, pp. 169–177. Available at: http://doi.org/10.5281/zenodo.3297377 (accessed: 12.05.2020)

E-Customs and Customs Regulation in the Russian Federation

Aleksander N. Kozyrin

Professor, Administrative and Financial Law Department, Russian University of Peoples Friendship (RUDN), Doctor of Juridical Sciences. Address: 6 Mikluho-Maklaya Str., Moscow, Russia. E-mail: kozyrine@mail.ru

Abstract

The rapid development of information technologies and digitalization of the global economy is compelling the Russian customs service to quickly create an electronic customs system that can coexist alongside the traditional paper customs control. The creation of electronic customs aligns with the development strategies outlined in Presidential Decree No. 204 "On national goals and strategic development tasks of the Russian Federation through 2024" of 7 May 2018. Electronic customs contributes to the development of international cooperation, exports, and an attractive investment climate. The first results of electronic customs are impressive: more than a third of all customs declarations are registered automatically, and more than a quarter of all low-risk declarations are issued automatically with the average release time reduced to about five minutes. The creation of electronic customs is an integral part of the digitalization processes in Russian economy. Customs operations are being automated and modern information and communication technologies are being introduced, and these changes provide significant savings in both time and money. The article discusses new approaches in electronic customs operation: the risk management system, personal accounts for foreign economy actors, and unified personal accounts. It also points out the main difficulties in digitalizing customs operations (lack of preparation for e-customs among Russian organisations, the low level of existing digitalization in many EAEU countries, etc.). All organisations, regardless of their economic clout, may now take advantage of digitized customs operations (reduced customs procession times, lower overhead costs, no appearance in person at customs offices, etc.), but the true winners are small and medium-size businesses, many of which formerly could not bear the high overhead costs associated with customs clearance and control and were in effect barred from accessing foreign markets. The article discusses the main institutions of modern electronic customs, how electronic customs may contribute to effective resistance to corruption in public service, as well as prospects for further digitalization of customs operations.

Keywords

digitalization of customs operations, electronic declaration, electronic customs, electronic declaration centre, risk management in customs control, personal account of person engaged in foreign economic activities, single account, artificial intelligence in customs.

Acknowledgments: The study was supported by the Russian Foundation of Basic Research, project No 20-011-00668.

For citation: Kozyrin A.N. (2020) E-Customs and Customs Regulation in the Russian Federation // *Legal Issues in the Digital Age*, no 2, pp. 144–162.

DOI: 10.17323/2713-2749.2020.2.144.162

1. Introduction. Customs Regulation in Russia: Fiscal or Administrative Focus?

The customs service in Russia underwent an unprecedented transformation during the 1980s and '1990s. How customs were levied had been determined throughout the Soviet era (1917–1991) by the state monopoly on foreign trade. Foreign trade operations were carried out exclusively through authorized state bodies. In the final stage of the state monopoly on foreign trade, those bodies were foreign trade associations that were part of the USSR Ministry of Foreign Trade. The function of the customs department itself was carried out by the Main Directorate of State Customs Control within the Ministry of Foreign Trade. At that time the main activity of customs was administrative (policing) control over the established procedure for moving goods across the customs border. It is no coincidence that customs themselves were called "suitcase fees" and not perceived as a source of fiscal revenue[1].

The perception of customs changed completely after the lengthy process of abolishing the state monopoly on foreign trade was completed in 1991. What was formerly a governmental body supervising border policing became the main fiscal organ of the state. The budget of the Russian Federation received 50-60% of its revenue from customs. From the very first years of its existence, payments collected by the post-Soviet customs service (import and export tariffs, VAT and excises levied on imported goods, as well as customs duties) became the main source of state revenue, surpassing even the receipts from the tax authorities. The significance of the customs service as a policing body simply faded away.

The situation began to change again in 2014 when Russia's economic situation was affected by extremely unfavourable external conditions. The share of payments received through the Federal Customs Service of Russia (hereinafter FCS) fell to 30–40% of total federal budget revenue. In 2014 the

[1] For the Soviet state, collecting customs payments from state-owned foreign trade associations meant merely shifting money from one pocket to another and obviously had no fiscal purpose.

FCS contributed 7,1 trillion rubles to federal budget revenue, but by 2017 that figure dropped to 4,5 trillion rubles. At the same time, such factors as the sanctions imposed by a number of Western states, and expanding trade wars intensified administrative regulations in global commerce. The role of the FCS as a border policing institution once again became prominent, although the high expectations for fiscal contributions from its operation remained the same. The concept of "electronic customs" was developed to meet the new challenges in customs regulation from the world economy and international trade so that the customs service could fulfil both its fiscal goals and manage the operations imposed by new foreign trade regulations.

With the creation of electronic customs and the digitalization of the tools for regulating customs, a movement to form a single channel for fiscal receipts in Russia began. As a result, the main types of fiscal payments such as taxes, customs, and insurance contributions began to be administered centrally by the Ministry of Finance of the Russian Federation (hereinafter Ministry of Finance) and regulated solely by the Tax Code of the Russian Federation. One more highly effective measure was to unify the information resources of the Federal Tax Service (hereinafter FTS) with those of the FCS. Along with other factors, the ongoing reforms to customs administration and the use of digital technologies have led to positive results: payments received by the FCS increased by 32% in 2018, increasing from 4,5 trillion rubles in 2017 to 6.06 trillion rubles the next year[2].

Russian customs currently acts both as an administrative and a fiscal regulator, and both functions are equally important. New features offered by current digital technologies help ensure its successful operation.

2. Electronic Customs as a Response of the FCS to the National Priorities of the Russian Federation

Russia adopted e-customs in the course of modernizing its international customs services under the auspices of the World Customs Organization, but the transition was facilitated by the application of digital technologies to public administration and to the Russian economy in general [See: Belick-

[2] Available at: https://tass.ru/ekonomika/5986624 (accessed: 01.06.2020). For more detail see Federal Customs Service of Russian Federation in 2018, p. 9. Available at: https://www.minfin.ru/common/upload/library/2019/04/main/06_Federalnaya_tamozhennaya_sluzhba_v_2018_godu.pdf (accessed: 01.06.2020)

aya A.V., Belyh V.S., Belyaeva O.A., 2019; Saurin A.A., 2019; Arabyan M.S., Gilmanova K.M., 2019; Tregubov A.N., 2020].

However, there was also a definite political reason to apply electronic customs in Russia. The customs service reforms were prompted by the national priorities formulated in the well-known Presidential Decree No. 204 "On National Goals and Strategic Development Tasks of the Russian Federation through 2024" dated 7 May 2018. The introduction of electronic customs serves several aims outlined in the Presidential Decree: international cooperation and export, development of the digital economy, and growth of small and medium-size enterprises.

Concerning the first aim — international cooperation and export — the introduction of electronic customs was expected to create the most favourable conditions possible for improving international trade and foreign economic relations, as well as to provide a good investment climate that includes not only legislation guaranteeing a stable investment regime and protection of foreign investors' rights and legitimate interests, but also a trade-friendly administration of customs and a fully developed foreign trade infrastructure. Russian customs strived to present an entirely new image — called "customs without fists" — and adopted a client-friendly approach that would regard foreign economic actors as partners rather than targets for various liabilities.

E-customs has become extremely efficient; it processes 39% of all declarations and issues 29% of low-risk declarations automatically. The average time to clearance has been reduced to some 5 minutes[3]. By 2020, 99% of all declarations will be registered automatically, while 80% of the declarations by low-risk foreign economic organisations will be issued automatically. In addition, 64% of all declarations will be issued automatically in 2020. The average time for any import consignment to clear customs will be 1 hour and 29 minutes and for export consignments 40 minutes.

In order to contribute to the second goal — developing the digital economy — customs institutions have to automate their operations and make use

[3] The statistical information used here and in what follows is from: International Customs Forum 2018. Panel discussion "Electronic customs". Available at: https://www.youtube.com/watch?v=FCPcJlO-q4) (accessed: 01.06.2020); A speech by the Head of the FCS at the Moscow Finance Forum 2018; Gaidar Forum 2019. Customs administrating in Russia. Available at: https://www.youtube.com/watch?v=5sO_TQ7FdxA) (accessed: 01.06.2020); Plenary session of the International Customs Forum 2019. Customs 2030:Trajectory of the Future. Available at: https://www.youtube.com/watch?v=CEUGyQurYww) (accessed: 01.06.2020). Customs service development strategy through 2030. Available at: https://www.youtube.com/watch?v=DJ84eglc43I) (accessed: 01.06.2020).

of the latest information and communication technologies available. While this will result in enormous savings in both time and money, digitalization itself will require major expenses for software, telecommunication equipment, and computing infrastructure, etc. [See: Belickaya A.V., Belyh V.S., Belyaeva O.A., 2019].

Digital technologies are an integral part of the risk-based management system that places foreign economic actors into low-risk and high-risk categories as they interact with customs services. Over the past three years, the number of low-risk declarants has almost tripled, accounting for up to 60% of all declarations and about 80% of all payments contributed to the federal budget by customs.

The use of digital technologies is bringing about a rapid change in the interaction between customs and other federal structures, which have enabled customs at present to have remote access to the information gathered by 32 federal executive bodies. [See: Romanovskaya O.V., Romanovskij G.B., 2019; Zubarev S.M., 2020]. The information exchange system supported by various governmental agencies processes over 70,000 requests every day and returns replies to them in a matter of seconds. As a result, the effectiveness of customs control has increased considerably as is clearly demonstrated by higher rates of customs payment.

One of the indicators of the quality of the digital technology used for customs is the accessibility of the information system. The current standard holds inactivity of the information system caused by all types of preventive maintenance, backup operations, and emergency situations to a total of no more than three days and 15 hours in a year. By 2020 this indicator is expected to increase accessibility to 99.99% of the time, which means that interruptions should not exceed 40 minutes per year.

Although customs has charged ahead in adopting highly digitalized and automated procedures, many foreign economic actors still fail to take full advantage of them and so interfere with the smooth operation of the innovations. The advantages derived from the new customs administration technologies may be dissipated by foreign economic actors unable to keep up with the pace now possible. For example, a shipping container that arrives by sea may clear customs in a couple of hours and then be left in the port area for weeks waiting for its owner or carrier to pick it up.

The divergent degree of digitalization and automation of customs operations within the countries of Eurasian Economic Union (EAEU) present one more problem which interferes with digitalization of customs and may

well retard integration within the EAEU to create a unified customs zone and common customs regulation. The head of the department of customs legislation of the Eurasian Economic Commission (EEC) commented on the situation of "digitalization at different speeds" as follows: "One of the primary tasks in developing customs enforcement interaction in the EAEU is to create a single digital realm. With that said, the countries of the Union differ in how quickly they are digitalizing customs administration. Any change needs time and money and is constrained by the basic level that already exists. We are certainly striving to reduce that gap"[4]. In his speech at the Digital Almaty Forum on 31 January 2020, the Russian Prime Minister said that the different degrees of digitalization among national economies threaten the Union with disintegration[5].

Turning to the third strategic development aim highlighted by Presidential Decree No. 204, let us see how the digitalization of customs contributes to the growth of small and medium-size enterprises. One answer is that the automation of customs operations together with the introduction of modern information and communication technologies has dramatically reduced the processing time needed to complete all the customs procedures and has thus cut overhead costs for foreign economic actors. In addition, declarants using e-customs are no longer required to appear in person in order to have their consignments clear customs. All foreign economic actors, regardless of their size and capitalization benefit from this streamlining of customs, small and medium-size businesses derive the most benefit from it because their overhead costs for dealing with customs in the past were unacceptably high and constituted an obstacle to accessing foreign markets.

3. Expected Benefits from E-Customs

The use of e-customs is expected to provide a broad range of benefits. First, academic consultants and professional customs expediters hope that e-customs will help optimize the management system for customs. This is still a task of great importance for Russia with its vast territories, the long

[4] Using artificial intelligence to process large arrays of data for customs operation is in the planning stage. Press service of the FCS, 12.09. 2019. Available at: https://www.tks.ru/news/nearby/2019/09/12/0012 (accessed: 01.06.2020).

[5] Available at: https://www.youtube.com/watch?v=3P0a7r4sT34 (accessed: 01.06.2020). A report on his remarks is available at: https://mail.kz/ru/news/kz-news/mishustin-rossiya-gotova-delitsya-tehnologiyami-so-stranami-eaes#hcq=3arlFPr. (accessed: 01.06.2020)

border with many entry points, and now that the Russian Federation has entered the Eurasian Economic Union and is forming a single customs zone within it, optimization has become even more urgent. Moreover, the technological features of digital customs make it possible to redistribute the declaration data in accordance with the real economic needs of the Russian regions [Arabyan M.S., Gilmanova K.M., 2019]; [Tregubov A.N., 2020].

Second, academic consultants and professional customs expediters see advantages in digital customs as they build and update more effective and efficient customs controls. At present, Russian customs control faces a number of challenges because commodity nomenclature is steadily diversifying and cargo turnover is increasing significantly in various geographical areas. However, the customs authorities have few options for adding personnel to meet the additional responsibilities. This leaves more automation of the customs operations and remote release of goods as the only way to improve customs control. An additional benefit will also come from using various information resources and modern risk management techniques. Increasing the number of customs inspectors and other staff as a comprehensive solution for customs control is no longer an adequate and competitive approach.

Third, electronic customs should make enforcement of customs more uniform. As odd as it may seem at first glance, removing the law enforcement officer (the human factor) from these processes (administrative decisions on customs clearance, customs control, or verification of declared value and of the completeness and timeliness of customs payments) would vastly improve uniform enforcement throughout the customs zone.

4. E-Customs: How it Works

Electronic customs in Russia first appeared in 2018, and the Volga Customs Service was the first to introduce it. The advantages of the new system became clear on the very first day of its operation: out of 1,000 registered declarations, 140 were issued without a customs inspector. And such automatic release of declarations took merely five to ten minutes.

There was nothing haphazard about the introduction of electronic customs; it was carried out according to by a carefully drawn up plan. In response to a governmental order, the Ministry of Finance approved a roadmap for the transition to electronic customs, and the FCS developed a detailed implementation plan for it.

The FCS's draft order "On Approval of the General Regulation concerning Customs (Electronic Customs)" provides the definition of e-customs: "Electronic customs is a specialized customs authority which is part of the unified and centralized federal system of customs authorities and which ensures the implementation of the FCS's tasks and functions, including those related to customs operations for declaring goods electronically and for currency control, in the regions where electronic customs are within the limits of powers as established by this Regulation"[6]. Electronic declaration centres are subordinate to electronic customs, which manages their activities. The FCS determines the region in which e-customs is to operate.

The creation of a unified network of electronic customs throughout the Russian Federation is planned to include:

eight electronic customs services with subordinate electronic declaration centres,

seven electronic declaration centres at specialized customs, and

one electronic aviation customs service.

Electronic customs are being created in almost every federal district (usually in their district centres). An electronic declaration centre is formed as part of the electronic customs structure, whose staff includes customs inspectors responsible for checking declarations submitted and issued digitally.

Electronic customs, as follows from the definition above, perform customs operations related directly to declarations in electronic form, and they include functional units related to electronic declaration: control of customs value, control of compliance with non-tariff measures, etc.

All personnel and logistical issues relating to electronic customs are delegated to the regional customs offices. In this way, electronic customs are freed from personnel matters and other administrative duties in order to focus exclusively on the use of new technologies related to the digitalization of customs operations and electronic declaration.

Electronic declaration centres at specialized customs gateways are established in combination with traditional "paper-based" customs. These centres will be established during 2020 in seven customs authorities: the Central Energy Customs, the Central Excise Customs, the three Maritime Customs (Baltic, Novorossiysk, and the Russian Far East), as well as in the Kaliningrad Regional Customs and the Moscow Regional Customs. Kalin-

[6] The text of the draft order has been posted on the federal website of draft regulations as well as in the Consultant Plus commercial legal database.

ingrad Customs were established because Kaliningrad is an exclave and as part of a special economic zone is free of customs. The creation of a special electronic declaration centre within the Moscow Regional Customs is due to the region's strong economic potential.

Along with electronic customs and electronic declaration centres at specialized customs gateways, a single electronic aviation customs service is being created for the whole country. It will be located in Moscow because 86% of Russia's foreign air cargo lands at Moscow airports and clears customs there.

5. Electronic Customs as Another Way to Combat Corruption

Corruption is the greatest affliction of modern public services in general, and it poses a particular threat to customs because customs officials are perceived as more susceptible than most others. Almost all the functions of the customs authorities are vulnerable to corruption. The broad discretion they have in making important decisions about various types of non-tariff restrictions and fiscal taxation levels (determining the classification of goods, verifying the calculation of customs value, identification of country of origin, etc.). Irene Hors of the OECD Development Centre notes that all the principal ways in which public services become corrupt are present in customs affairs. Those kinds of corruption are:

routine corruption — when foreign economic players pay bribes to expedite ordinary customs procedures;

malicious corruption — when a customs officer is "motivated" to turn a blind eye to illegal actions aimed at reducing tax and customs payments, circumventing administrative barriers, etc.;

criminal corruption — when a bribe is offered to carry out an illegal but extremely profitable operation (smuggling weapons, drugs, animals listed in the Red Book, etc.)[7].

The likelihood of corruption increases when customs officers and entrepreneurs meet at privately owned commercial facilities where it is easy for them to agree on reducing the fees for a foreign economic transaction and this is exactly the way corruption usually occurs in Russia because customs

[7] De Wulf L. & Socol J. (eds.): Customs modernization handbook (World Bank). This article refers to its Russian translation (Moscow, 2007, pp. 67, 69).

control usually takes place at locations owned by businesses (as their storage facilities or administrative offices). In order to reduce such opportunities, the Russian customs service is now trying to minimize contacts between declarants and customs inspectors, and it has also announced that customs operations will be relocated to avoid privately owned sites. The use of e-customs certainly will help to complete this task.

Electronic customs is quite compatible with locating the customs authorities exclusively in state-owned facilities. However, this desideratum is one of the main reasons that electronic customs are being put into practice so slowly in Russia. The lengthy public procurement procedures involved in setting up customs offices has delayed implementation of electronic customs and electronic declaration centres for a number of specialized kinds of customs operations. [See: Truncevskij Yu.V., 2019; Koval V.D., 2018].

For anti-corruption purposes, electronic customs can easily be arranged in such a way that any direct contact between declarants and customs inspectors is avoided. Foreign economic actors would submit all the necessary supporting documents to a customs authority[8] distinct from the customs officer who carries out the actual inspection.

Finally, electronic customs facilitate highly automated operations and administration. The latest version of the Arusha Declaration approved by the World Customs Organization in 2003[9], classifies automation as one of the key weapons in combatting corruption in customs operations. Automating customs will minimize the human factor that customs personnel can introduce, and the manual operations most vulnerable to corruption should be automated first. It should also be kept in mind that automation can become an effective way to combat corruption only when it is coupled with other measures mentioned in the Declaration.

However, automated systems used in customs control are vulnerable to both external attacks and manipulations from inside the customs organisation. This means that there will be new challenges in ensuring cybersecurity and protecting automated customs administration systems. [See: Zubarev S.M., 2020].

[8] This innovation has caused debate in the business community because there is a different customs authority where the declarant will have to submit the required documents on paper.

[9] In addition to automation, the Declaration also identifies the other main weapons for combating corruption: transparency; reform and modernization; audit and investigations; code of conduct; interaction with the private sector, etc.

6. Electronic Customs: Does Classic "Hands-on" Customs Control Have a Future?

The formation of a unified system of electronic customs does not mean that the Russian Federation is trying to completely replace "hands-on" or direct customs control. Various specific features of customs control and its important function in law enforcement make it inevitable that some direct customs control will remain (direct control is explicitly prescribed by federal law in particular cases).

The only thing that will change is the ratio between the competences of electronic customs and direct customs control. As digitalization of customs procedures and other customs operations proceeds, the scope of electronic customs will expand and the use of direct customs control operations will shrink.

Only three of the seventeen customs procedures specified by the EAEU Customs Code had been digitalized by the beginning of 2020. However, these three customs procedures are extremely comprehensive, as they constitute 98% of all declarations: 63% of them are imports for domestic consumption; 33.3% are for exports; 1.7% are for customs free zones. That means that the remaining customs procedures make up no more than 2% of all customs declarations submitted. These are not being shifted to electronic customs but are processed by traditional forms of direct customs control. The business community has shown interest in taking digitalization of customs further and has already requested expedited digitalization of customs processing procedures (processing within customs facilities, processing outside customs facilities, and processing for domestic consumption).

Direct customs control is currently applied to any customs procedures not yet digitalized as well as to a number of other areas: direct control where it is prescribed by law, customs control of goods and vehicles after goods have been released, etc.

Labour productivity is increased by electronic customs, and automation threatens to make many customs officials redundant. Will this cause wholesale reduction in the number of customs officials, including those with abundant practical experience? The heads of the customs service have stated in their speeches that the employees replaced through automation will be redirected to those areas of customs which are short of personnel, specifically: port customs, staffing and arrangement of new customs border stations, increased customs control over the constantly growing passenger flow

at airports, and possibly transfer of veterinary and phytosanitary control to the customs authorities in certain areas (primarily in the Russian Far East)[10].

7. Technologies for Electronic Customs

Electronic customs refers to a specialized body in customs operations for declaring goods through an electronic format, and it requires the use of modern, technologically advanced approaches. Let us describe the most important of them.

7.1. Risk-based approaches

Risk management processes in the Russian customs service are based on a subject-oriented risk management system in which foreign economic actors are classified as presenting low, medium or high risk depending on how likely they are to violate customs regulations, and this results in applying more differentiated and effective control measures to them[11].

This subject-oriented risk management system directs the attention of customs control to the consignments most likely to be out of compliance. The customs authorities can then allocate their personnel and technical resources more efficiently during customs control. In addition, the risk management system gives organisations with a good history of compliance the advantage of deferring customs control until after their goods have been released, which may considerably reduce their transport and overhead costs.

A subject-oriented customs risk management system would be as follows:

customs control of low-risk organisations ("green zone") is mainly carried out after the goods have been released;

for medium-risk organizations ("yellow zone") control is exercised mostly through verification of documentation (control measures may take place both before and after releasing the goods);

for organizations with a high level of risk ("red zone"), control by means of both document checks and hands-on inspection is completed before the goods are released.

[10] This would reproduce exactly what happened in China. The personnel freed up after the opening of electronic customs were transferred to phytosanitary and veterinary control assumed by the Chinese customs authorities.

[11] Available at: http://customs.ru/uchastnikam-ved/kategorirovanie-uchastnikov-ved/o-realizaczii-v-fts-rossii-sub-ektno-orientirovannoj-modeli-sistemy-upravleniya-riskami (accessed: 01.06.2020)

For organizations qualifying for the "green zone", control is designed to ensure compliance with prohibitions and restrictions. Other forms of control are carried out infrequently, and the information and documents required for these other forms of control are provided to the customs authorities after the release of goods.

For the "yellow zone", the same compliance control measures as in the "green zone" are applied, and other forms of control are still used relatively infrequently. Documentary control is carried out both before and after the goods are released. However, the main focus of documentary checks is on the stage after the goods have been released.

The "red zone" organizations are subject to all forms of customs control as well as to an expanded range of control measures. All customs control is carried out before the release of goods.

The risk levels are assessed automatically (without involving customs officials) depending principally upon the industrial or commercial category of an organisation[12]. Once the organisation's category has been established, information is analysed to determine the risk level, and subsequent customs control is adapted to handle various enterprises, such as car manufacturers, importers of fish and meat products, or exporters of domestic products.

The procedure for classifying an organization as a low-risk declarant relies on its declaration. The organisation sends an application to the FCS accompanied by documents which the FCS employs to reach a decision derived from its established criteria. If necessary, the FCS requests additional documents and information and finally decides whether to designate the applicant a low-risk organisation or not. The decision is issued in the form of an FCS decree.

There are general criteria for assigning foreign economic actors to different risk levels as well as more specific criteria for organisations in a particular industry, such as:

amount of authorised capital;
value of net assets;
main type of economic activity;
staff size;
applicable tax category;
volumes of foreign economic activity;

[12] For more details, see the orders of the FCS, e.g., No. 1740, 27 August 2015, No. 706, 8 April 2016, No. 731, 11 April 2016, No. 732. 11 April 2016, No. 733, 11 April 2016, etc.

commitment to paying customs duties, fines, and also taxes levied by tax authorities;

liability for any violations, etc.

Most of the organisations designated low-risk have been assigned that category by automated risk-categorization procedures set forth by FCS Order No. 2256 dated 1 December 2016. The established procedure analyses the organisation's activities over the previous two calendar years. The appendix to the Order identifies more than thirty evaluation criteria, such as: turnover of goods with offshore zones, changes in key indicators on customs declarations, results of customs control measures, liabilities, categorization by the Federal Tax Authority, compliance with foreign exchange regulations, degree of commercial focus on export, and others.

The customs authorities regularly update risk categories using software and the database of the Unified Automated Information System, which is shared with the FTS and the Central Bank of the Russian Federation. The procedure for risk categorization is first to calculate the score for each of the criteria and then to use those scores to make a final assessment of the organisation's activities ending in assignment of a low, medium or high level of risk.

The high-risk category applies not only to organisations whose overall scores meet the criteria for high risk, but also to organisations that match any one of the following pre-emptory criteria[13]:

the organisation is listed as an entity for which customs inspection is difficult;

the organisation is about to be liquidated or to terminate its activity;

has failed to fulfil its obligation to pay customs duties, penalties, or interest;

has failed to pay an administrative fine;

has a final conviction in court under Art. 194 of the Criminal Code of the Russian Federation[14];

has a high risk level for tax evasion according to the Federal Tax Authority's evaluation.

Organizations are considered medium-risk ("yellow zone") if they cannot be definitely categorized as either low-risk ("green zone") or high-risk ("red zone").

[13] If the organization meets any one of the preemptory criteria, it will be listed as a high-risk organization, regardless of the total evaluation score it actually received.

[14] Art. 194 of the Criminal Code of the Russian Federation "Evasion of customs payments levied on organizations or individuals".

About 10,000 entities were listed as low-risk at the end of 2019. These organisations participating in foreign economic activities accounted for 79% of all customs payments paid. The risk level for 10,500 other organizations was estimated as high, while over 95,000 organizations were designated medium risk[15] [Tregubov A.N., 2020]; [Arabyan M.S., Gilmanova K.M., 2019].

7.2. Personal account of a foreign economic actor

The option for a "Personal account of a foreign economic actor" was added to the website of the FCS at the end of 2015. The legal definition of these personal accounts is contained in Article 284 of Federal Law No. 289-FZ dated 3 August 3, 2018 "On customs regulation in the Russian Federation and on amending certain legislative acts of the Russian Federation". A personal account is an information resource belonging to the FCS and located on the internet and which may be used for exchange of electronic documents and information in digital form between the customs authorities and interested parties. The FCS issued instructions on how a personal account for the exchange of electronic documents and information is to be used (FCS Order No. 901 dated 3 June 2019). In that same order, the FCS regulated access to personal accounts by their users.

Until recently, organisations participating in foreign economic activities had to send someone to the customs authorities and spend substantial amounts of time conversing with customs officials. By using the new personal account online options, they can now carry out many requisites for customs clearance and customs control more quickly and easily. The personal account was designed for personalized information exchange between organisations and the customs authorities and provides information services for creating and storing electronic documents (declarations, notifications, reports, inventories, etc.) and for submitting them to the customs authorities, etc.

Users must register to create a personal account in one of the following ways:

with a digital signature[16] (registration is automatic, and the login name becomes the individual insurance account number[17]);

[15] More information on these classifications is available at: http://customs.ru/uchastnikam-ved/kategorirovanie-uchastnikov-ved/o-realizaczii-v-fts-rossii-sub-ektno-orientirovannoj-modeli-sistemy-upravleniya-riskami (accessed: 01.06.2020)

[16] Many functions of the personal account require a digital signature to protect the information entered from unauthorized access by third parties.

[17] Unique number of the individual personal account of the insured person in the mandatory pension insurance system (SNILS).

without a digital signature (the user creates a login name);

by using an existing online account created for one of the other Russian state services.

After the account is authorized, various functions are automatically available. Organisations using a digital signature have the option to maintain personal accounts and electronic archives, submit various types of customs reporting or to obtain permits, classifications of goods, and access to various "white lists". Individuals with personal accounts upon request may choose the options to submit a passenger declaration and to calculate the customs payment due.

The numerous personal account services can be divided into groups by their function:

informing about goods before they arrive at a customs facility:

providing preliminary information for expediting operations on water and air shipments; preliminary information on road and rail shipments; customs operations for goods transported via ATA Carnets, etc.;

customs declaration and customs operations necessary for the release of goods: declaration of goods; use of the electronic archive[18]; statistical declaration; use of a personal account; determining arrears of customs payments and other fees; requesting the status of a declaration of goods; providing collateral, bank guarantees, etc.;

information on foreign economic activities: permits; general information on declarations of goods[19]; risk level classifications; currency exchange control, etc.;

classification of goods*:* decisions on classifications of goods; classification of goods transported as components; information on preferences; information on preliminary decisions, etc.;

inspections and violations: administrative offenses; customs checks; customs inspections, customs appraisals, etc.;

customs activities: reporting (authorized economic operators, owners of a duty-free shop, importers of tobacco products, owners of customs warehouses, etc.); obtaining permission for temporary storage; registry maintenance, etc.;

[18] The digital archive is designed to store the user's digital documents within the customs authorities' information system. The uploaded documents can be used for other services during different declaration processes.

[19] This information service visually represents all declarations issued, no matter how the declarations have been submitted.

specialized personal accounts: for banks, customs carriers, customs representatives, etc.;

information services for individuals:

confirmation that an individual has opened a unified personal account (see 7.3 below); filing customs declaration as a passenger; receipts for payment of customs, etc.

The personal account opens up new opportunities for organizations to reach foreign markets. They can fill out electronic goods declarations independently and submit them to the customs authority without involving a customs official or acquiring specialized software. All the documents and information necessary for customs purposes can be provided without appearing in person at a customs office. Information about cash balances on personal accounts, decisions of the customs authority on registering a declaration or releasing goods, etc. are all available automatically.

7.3. Unified personal account of organisations participating in foreign economic activities.

Another new technical capability recently added to customs is the unified personal account, which was introduced toward the end of 2016. This system of centralized accounting for customs and other payments administered by the customs authorities had at first been available only to the largest tax-paying organisations; the others were saddled with making separate payments to each of the customs divisions they interacted with. But now, all organisations may use a unified personal account to direct the use of their payments to cover declarations wherever they were submitted. Once money has been received in a unified personal account, it can be used for transactions at any customs authority of the Russian Federation.

The new technology has several advantages. First, it is now possible to carry out customs operations for all the customs authorities at once. Personal accounts for each of the various customs authorities are no longer required as they were before. This supports large-scale implementation the policy for transitioning to remote payment of customs duties, taxes and fees.

Second, it greatly augments control over cash flow and expenditures. Any organisation can now monitor its expenses in its personal account on the website of the FCS. There is no longer any need to regularly track expenses and settle accounts with the various customs authorities.

Third, the system of unified personal accounts executes monetary transactions instantly (in no more than 6 seconds) and thus offers faster throughputs at customs, which in turn cuts transport, overhead and other costs for organisations participating in foreign economies. In addition, the uniform bank details for all types of customs payments minimize the likelihood of errors when transferring money.

A regulatory framework for the application of the new unified personal account function is now being drafted [Arabyan M.S., Gilmanova K.M., 2019]; [Abramova G.A., Voronina E.A., Goroshkov A.A., 2019].

Conclusion. Electronic Customs: What's Next?

The process of building an electronic customs system in Russia is clearly irreversible. The question of what will come after e-customs has already come up. The answer is indicated in the Strategy for the Russian Customs Development through 2030. The FCS has decided to introduce artificial intelligence technologies into the customs administration processes[20].

An intelligent checkpoint model for complete automation of customs processes is now in development. This model entails an information system which is unified for all regulatory authorities and into which all the existing technical tools for customs control will be integrated. This will facilitate and expedite the administration process and bring it to an entirely new level. The FCS plan a transition to completely paperless control and will introduce new software that can carry out customs control without any human factor involved.

References

Abramova G.A., Voronina E.A., Goroshkov A.A. (2019) The Customs Code of the EAEU and new rules for collecting customs payments. *Tamozhennoe delo*, no 3, pp. 3–7 (in Russian)

Aleshkova I.A., Molokaeva O.H. (2019) Dangers of digital development of law: obvious, hidden, imaginary. *Konstitucionnoe i municipalnoe pravo*, no 8, pp. 41–45 (in Russian)

Arabyan M.S., Gilmanova K.M. (2019) Digitalization as a priority tool of customs administration on the example of the EAEU. *Tamozhennoe delo*, no 4, pp. 17–21 (in Russian)

[20] FCS is going to make use of artificial intelligence. Available at: https://rg.ru/2019/10/24/fts-vozmet-na-sluzhbu-iskusstvennyj-intellekt.html (accessed: 01.06.2020)

Belickaya A.V., Belyh V.S., Belyaeva O.A. et al (2019). *Legal regulation of economic relations in modern conditions of digital economy development*. Moscow: Yusticinform, 376 p. (in Russian)

Koval V.D. (2018) The concept of corruption in Russian legislation and its main impact on the functioning of the customs system. *Administrativnoe pravo i process*, no 8, pp. 62–65 (in Russian)

Popondopulo V.F. (2019) Legal forms of digital relations. *Yurist*, no 6, pp. 29–36 (in Russian)

Romanovskaya O.V., Romanovskij G.B. (2019) Digital technologies and deconcentration of state power. *Konstitucionnoe i municipalnoe pravo*, no 8, pp. 36–40 (in Russian)

Saurin A.A. (2019) Digitalization as a factor of transformation of law. *Konstitucionnoe i municipalnoe pravo*, no 8, pp. 26–31 (in Russian)

Sharandina N.L. (2019) The digital economy and the formation of tax culture: legal aspect. *Finansovoe pravo*, no 10, pp. 25–32 (in Russian)

Tanimov O.V. (2020) Transformation of legal relations in context of digitalization. *Aktualnye problemy rossijskogo prava*, no 2, pp. 11–18 (in Russian)

Tanimov O.V. (2019) The impact of digital technologies on emergence of new structural elements of the legal system. *Rossijskaya yustitciya*, no 7, pp. 2–5 (in Russian)

Tregubov A.N. (2020) Improving customs control in the digital economy. *Tamozhennoe delo*, no 1, pp. 17–19 (in Russian)

Truncevskij Yu.V. (2019) E-corruption or E-anticorruption: the impact of global digitalization. *Mezhdunarodnoe publichnoe i chastnoe parvo*, no 4, pp. 42–48 (in Russian)

Zubarev S.M. (2020) Legal risks of digitalization of public administration. *Aktualnye problemy rossijskogo prava*, no 6, pp. 23–32 (in Russian)

Zubarev S.M., Sabaeva S.V. (2020) Legal regulation of digital technologies of state control: experience of the subjects of the Russian Federation. *Rossijskaya yustitciya*, no 7, pp. 17–21 (in Russian)

Confidentiality of Communications: What it Covers according to the Russian Judicial Practice

Nikita Danilov

Senior Lecturer, Law Faculty, National Research University Higher School of Economics, Candidate of Juridical Sciences. Address: 20 Myasnitsky Str., Moscow 101000, Russian Federation. E-mail: ndanilov@hse.ru

Abstract

Analysis of confidentiality of communications in Russian judicial practice.

Keywords

citizens, correspondence, service, rights and freedoms, offence, liability, the Constitutional Court, the Supreme Court.

For citation: Danilov N.A. (2020) Confidentiality of Communications: What it Covers according to the Russian Judicial Practice // *Legal Issues in the Digital Era,* no 2, pp. 163–172.

DOI: 10.17323/2713-2749.2020.2.163.172

At the legislative level, the concept of confidentiality of communications and what it covers are defined in the Constitution of the Russian Federation and the Federal Law "On communications".

According to Article 23 of the Constitution of the Russian Federation, everyone has the right to the inviolability of private life, personal and family confidentiality and to protection of their honor and good name. Everyone has the right to confidentiality of correspondence, telephone conversations, postal, telegraph and other communications. Restriction of this right is permissible only on the basis of a court order.

Paragraph 1 of Article 63 of the Federal Law "On communications" also provides that the confidentiality of correspondence, telephone conversations, mail, telegraph and other messages transmitted over telecommunication and postal networks is guaranteed within the territory of the Russian Federation.

A literal interpretation of these provisions would conclude that the lawmakers initially regarded the content of communications as confidential. This is certainly very sensitive information, as people obviously do not want the content of their telephone conversations, short text messages or emails to be made public, or the content of communications to be accessed by third parties. Violation of the confidentiality of correspondence is a significant infringement of the rights and freedoms of citizens.

However, Russian judicial practice has applied a broader interpretation of the concept and coverage of confidentiality of communications.

According to the ruling of the Constitutional Court of the Russian Federation dated 2 October 2003 No. 345-O "Concerning declining to consider the inquiry of the Soviet district court of Lipetsk concerning confirmation of the constitutionality of paragraph four of Article 32 of the Federal Law dated 16 February 1995 'On communications'", the right of each person to confidentiality of phone calls in its constitutional sense implies a set of actions for the protection of information received via a communication channel, regardless of the time of receipt, or the extent and content of the information recorded at separate stages of its implementation. For this reason, any information transmitted, stored and established by telephone equipment, including data on incoming and outgoing signals of connection between telephone devices of specific users of communications is considered information that is subject to the confidentiality of telephone conversations protected by the Constitution of the Russian Federation and laws in force within the Russian Federation. In order to access this information, bodies engaged in operational search activities must obtain a court order. Otherwise, this would fail to comply with the requirement in Article 23(2) of the Constitution of the Russian Federation concerning the permissibility of restricting the right to confidentiality of telephone conversations only on the basis of a court order.

This decision of the Constitutional Court of the Russian Federation was largely dispositive in the development of subsequent judicial practice. It was consequential not so much in that it attributed confidentiality of communications to data about the incoming and outgoing signals of telephone connections, which are in fact details about calls (information on the date and time of calls made, data identifying call recipients and callers, and the duration of connections), but rather because the decision applied confidentiality of communications to any information transmitted, stored and provided using telephone equipment. This interpretation subsequently led courts of

general jurisdiction and arbitration courts to apply confidentiality of communications to any information, even of a technical kind, that is used in a communication network when making telephone calls or when subscribers use telecommunication services and data transmission services. This includes, for example, the IMSI number, IMEI, and other information.

That interpretation hinders the development of modern telecommunication services. For example, information about changes in an IMSI number (the unique identification code of a SIM card) can be used as part of information exchange between telecom operators and banks in order to counter fraud. There are instances in which hackers have used fraudulent powers of attorney to create duplicate SIM cards that are "linked" to bank accounts. Then the attackers used the duplicates to illegally debit money from the bank account of a bona fide person. Furthermore, telecom operators track information about the IMSI numbers used by the subscribers on their network. If this number changes, it is a signal potentially flagging an illegal modification of a SIM card, and this information can be transmitted by the operator to a bank for additional authorization when performing a banking operation. However, due to the classification of IMSI numbers as confidential communication which can only be disclosed on the basis of a court order, these verification practices fall into a "gray" legal zone.

This position of the Constitutional Court of the Russian Federation was reflected in some of its subsequent decisions, for example, in the ruling dated 21 October 2008 No. 528-O-O "On declining to accept the plea of Alexander Mullin concerning violation of his constitutional rights under the provisions of Article 9 of the Federal Law 'On information, information technologies and information protection' and Article 53 of the Federal Law 'On communications'".

The position of the Supreme Court of the Russian Federation also merits study. As noted in the review of judicial practice by the Supreme Court of the Russian Federation entitled "Review of judicial practice in criminal cases of crimes related to illicit trafficking in narcotic drugs, psychotropic, potent and toxic substances" (approved by the Presidium of the Supreme Court of the Russian Federation on 27 June 2012), information that is protected by the Constitution of the Russian Federation and laws in force within the Russian Federation is considered to be any information transmitted, stored and provided using telephone equipment, including data on incoming and outgoing connection signals of the telephone apparatuses of specific users of communications. In order to access this information, the authorities en-

gaged in search operations must obtain a court order. Otherwise, a search would fail to comply with the requirement of Article 23(2) of the Constitution of the Russian Federation that restricting the right to confidentiality of telephone conversations is permissible only on the basis of a court order. Hence, it is necessary to obtain a court decision to locate a telephone apparatus relative to a base station, as well as to identify subscriber devices of persons of interest in a search because obtaining that information is an invasion of privacy and entails restriction of the constitutional rights of citizens to the confidentiality of telephone conversations.

Therefore, this decision of the Supreme Court of the Russian Federation applies not only to the confidentiality of communications but also of information about the location of a subscriber's device.

Certainly, information about the location of a subscriber's device is quite important and sensitive information from the point of view of citizens' rights. It is unlikely that we want third parties to know about our location at a certain time and place. However, geolocation data can be processed anonymously in a data array. For example, at 13:00 in the vicinity of 7 Tverskaya Street there were 700 young people aged 18 to 35 years. This information is of commercial value because it could perhaps be used to make decisions about opening retail stores. That kind of information is completely depersonalized in that it does not directly or indirectly identify persons and does not indicate the location of a particular person. But there is a risk that regarding access to such information as restricted will interfere with providing services through Big Data analytics.

These decisions of the Constitutional Court and the Supreme Court of the Russian Federation have also influenced the practice of arbitration courts and courts of general jurisdiction.

For example, the decision of the Moscow Arbitration Court (decision dated 8 June 2015 in case No. A40-76979/2015) found the MTS (Mobile TeleSystems) service guilty of committing an administrative offense, liability for which is provided by paragraph 3 of Article 14.1 of the Administrative Code and punishable by an administrative fine in the amount of 30,000 rubles.

The materials in the case indicate that on 9 December 2010 a contract for the provision of communication services was concluded between a person identified by the initial 'S' and the telecom operator MTS OJSC (open joint stock company). In accordance with this agreement, MTS was assigned a subscriber number for the purpose of providing mobile radiotelephone services to subscriber S.

A credit card agreement and a debit card agreement were signed between subscriber S. and Tinkoff Credit Systems Bank CJSC (closed joint stock company). Subscriber S. provided the subscriber number (with first four digits 7915) as the main contact number for informational and financial interactions with the bank in the course of providing remote services under the specified agreements.

On the basis of clause 4.2 of the terms applicable to comprehensive banking services at Tinkoff Credit Systems Bank, the court established that the bank under the Universal Agreement for remote services provides information to its client by sending that information via the client's contact details as stated on the application form.

Subscriber S. received a message from Tinkoff Credit Systems Bank to the effect that sending passwords to the subscriber number beginning with 7915 was blocked due to replacement of the SIM card. In response to a request that subscriber S. sent by e-mail to Tinkoff Credit Systems Bank, the bank's customer service department explained that the block was imposed for security reasons and also indicated that the bank had tried to verify the link of the IMSI to the mobile phone number. When the bank sends messages to a subscriber, the IMSI is linked to the mobile phone number contact. If the SIM card is replaced (without changing the phone number), the IMSI changes. As a result, the bank's system will not automatically reestablish the link, and the subscriber must reset the IMSI binding in order to have the services to work as expected.

As the court noted in its decision, in accordance with the international standardization recommended by ITU-T E. 212, an international mobile subscriber identification number (IMSI or International Mobile Subscriber Identity) is a sequence of decimal digits, not to exceed 15 digits, that identifies a single subscriber. The IMSI is contained in the operator's database, stored on the subscriber's SIM card and, for the purpose of identifying the subscriber, is transmitted over the telecommunication network from the subscriber station to the receiving equipment of the operator when the subscriber is initialized in the network.

Subscriber S. did not provide information about the IMSI value of his SIM card to the bank, and the contract for the provision of communication services between MTS and subscriber S. does not specify the value of this identifier.

In response to the request, a representative of Tinkoff Credit Systems Bank confirmed that in the course of providing services to customers, the

bank uses verification of the link between the IMSI number located in the SIM card memory and the customer's subscriber number in order to identify a customer. The bank further explained that the IMSI is provided to the bank by the mobile telecommunications operator after the ID is transmitted by the mobile communication device during registration in the network.

In the explanation provided to Roskomnadzor, MTS denied that it had provided information about the IMSI value of the SIM card of subscriber S. to Tinkoff Credit Systems Bank.

According to Roskomnadzor, these actions by MTS constituted an administrative offense, liability for which is established in paragraph 3 of Article 14.1 of the Administrative Code of the Russian Federation (which covers conduct of business activities in violation of the conditions applicable to a special permit or license).

In accordance with Article 23.1 of the Administrative Code of the Russian Federation, Roskomnadzor filed a statement in arbitration court to the effect that MTS should be held liable for an administrative offense under paragraph 3 of Article 14.1 of the Administrative Code. The company was in fact held liable.

MTS appealed the decision, but the court of appeals upheld the legality of the administrative liability.

The court noted in its decision that, on the basis of paragraph 1 of Article 63 of the Federal Law "On communications", the confidentiality of correspondence, telephone conversations, mail, telegraph and other messages transmitted over telecommunication networks and postal networks is guaranteed within the Russian Federation. Restriction of that right to confidentiality is permissible only as stipulated by federal laws.

In accordance with the national standard of the Russian Federation GOST R 53801-2010 "Federal communications: Terms and definitions", a telecommunication message is any information transmitted by means of telecommunications.

Hence, the court found that an IMSI belongs to the category of messages transmitted over telecommunication networks, and as such it is subject to the requirements of the legislation of the Russian Federation which ensure confidentiality of communications. Paragraph 2 of Article 63 of the Federal law "On communications" stipulates that the operator must ensure the confidentiality of communications when providing services.

As follows from the materials of another case (decision of the Ninth Arbitration Court of Appeals dated 28.03.2014 N 09AP-1573/2014 in case N

A40-145794/13), the unique IMEI number which identifies an apparatus also constitutes information that is subject to confidentiality of communications.

MTS sued in arbitration court to have a decision of the Bank of Russia's financial markets service declared illegal and to rescind liability of MTS for an administrative violation under paragraph 9 of Article 15.9 of the Administrative Code of the Russian Federation, which stipulates a fine of 500,000 rubles as penalty.

The case establishes that, in the course of conducting a desk audit to investigate possible misuse of insider information and market manipulation, the Federal Service for Financial Markets (FSFM) asked MTS to provide the following information:

All information listed in paragraph 1 of Article 53 of the Federal law "On communications" concerning all users of communication services who were allocated a subscriber number beginning with +7(985)386.... The information was to include the period of use of this number by each of the users of communication services and the IMEI of the terminal equipment used in each period. Copies of documents confirming the information provided, including contracts, agreements, and customer profiles as well as changes and additions to these documents were also to be provided;

Information about whether communication services were provided to the subscriber number +7(985)386... in the period from 1 January 2012 until the date of receipt of the order;

Information about other subscriber numbers used during that period by the service user who was assigned the subscriber number +7(985)386... under contracts concluded between the subscriber and MTS, specifying the subscriber numbers, dates on which contracts were concluded or terminated, and the IMEI of terminal equipment used by the subscriber;

Details of the subscriber's invoices for the period in electronic form using the MS Excel format on optical media.

MTS provided the information and documents requested by order of the Federal Service for Financial Markets with the exception of the identification numbers of subscriber devices (IMEI) and information about the details of subscriber accounts for the period in MS Excel on optical media.

The FSFM charged MTS with an administrative offence on grounds of refusal to provide information.

Subsequently, the Bank of Russia's financial markets service under the Central Bank of the Russian Federation issued a decision to the effect that,

under paragraph 9 of Article 19.5 of the Administrative Code of the Russian Federation, MTS was subject to administrative liability in the form of a fine of 500,000 rubles.

In finding MTS liable under paragraph 9 of Article 19.5 of the Administrative Code of the Russian Federation, the Bank of Russia reasoned that MTS had violated Article 16(1) of the insider trading law and article 11(1) of the law concerning protection of investors' rights.

According to legislation on countering insider information (in the version that was in effect at that time), legal entities are required to submit documents, explanations, and information in written and oral form, including commercial, official, and banking information subject to confidentiality.

MTS alluded to these circumstances as the basis for its appeal to the court concerning the above requirements.

The court sided with MTS.

As the court noted in its decision, the details of the subscriber's account contain information about the mobile communication services provided, indicating the date and time of all connections, their duration and subscriber numbers.

Hence, the subscriber account details represent data on incoming and outgoing connection signals of the telephone sets of specific communication users.

Information contained in the subscriber's account details, including data on incoming and outgoing connection signals of telephone apparatuses of specific communication users, is stored and set by the communication operator using only telephone equipment.

In addition, the identification number of the subscriber's IMEI device is not required by the terms of the mobile service agreement, and therefore it cannot be established based on the provisions of contracts concluded with subscribers.

When concluding mobile communication service contracts with subscribers, the operator provides them with subscriber identification modules (SIM cards) where the subscriber number is recorded, but the operator does not provide the telephone apparatus. Subscriber devices are purchased by the subscriber independently in a retail network, which sells them without requiring an identity document, and therefore the IMEI code of the subscriber device is not directly linked to either the telecom operator or to the subscriber himself.

At the same time, the subscriber has the right to use any subscriber devices, and the telecom operator is not obliged to maintain a database containing information about these devices.

Information about the identification numbers of subscriber IMEI devices is "registered" (set) by the communication equipment only during telephone connections; that is, it is contained only in the connection protocols (details) of specific subscribers whose SIM cards were used in a particular telephone device.

Given the above, as noted in the court decision, it was justifiable to find with the court of first instance that information about the IMEI identification numbers of subscriber devices also represents information transmitted, stored and installed using telephone equipment, and it therefore falls under the confidentiality of telephone conversations.

In accordance with Article 63 of the Federal Law "On communications", the confidentiality of correspondence, telephone conversations, mail, telegraph and other messages transmitted over telecommunication and postal networks is guaranteed within the Russian Federation.

Restriction of the right to confidentiality of correspondence, telephone conversations, mail, telegraph and other messages transmitted over telecommunication and postal networks is permitted only as stipulated by federal laws. Telecom operators are required to ensure the confidentiality of communications.

This right is guaranteed by the aforementioned Article 23 of the Constitution of the Russian Federation.

In light of the above and the previously mentioned legal position of the Constitutional Court of the Russian Federation, set out in the definitions dated 2 October 2003 N 345-O and 21 October 2008 N 528-O-O, information subject to the confidentiality of telephone conversations includes any information transmitted, stored and installed using telephone equipment, including data on incoming and outgoing connection signals of telephone devices of specific communication users; and to access this information it is necessary to obtain a court order.

The court of appeals, in accordance with the rules pertaining to the nature of the information (data) requested by the administrative authority, held that the billing details of a specific subscriber and information about the identification numbers of subscriber devices (IMEI) are subject to confidentiality of communications, inasmuch as those details consist not only of the information contained in the telephone connection (conversations), but also data on the connections between individual subscribers (date, time, duration), and any other information transmitted, stored, and installed with communications equipment.

The information withheld by MTS was subject to the confidentiality of communications and therefore should not have been provided upon request to the administrative body.

In this case, the court of first instance rightly alluded to the response of the Ministry of Communications and the letter of Roskomnadzor, which explained that the account details specific to a caller and data about the identification numbers of their subscriber devices (IMEI, IMSI) are protected by the Constitution of the Russian Federation as confidential interactions by telephone.

In view of the above circumstances, the court rightly upheld the conclusion of the court of first instance that the refusal of MTS to provide such information to the FSFM does not constitute sufficient proof of an offense as specified by paragraph 9 of Article 19,5 of the Administrative Code. That conclusion was the basis for a declaring that the decision to subject MTS to administrative liability is unlawful and void.

The judicial practices outlined above show that the concept of confidentiality of communications is interpreted very broadly by the courts. In addition to the content of interactions, confidentiality of communications extends to geolocation, call details, and technical information transmitted over communication networks (IMSI, IMEI). The classification of technical information as a confidential communication is questionable because processing that information does not affect the rights and freedoms of citizens, and it does not violate the right to privacy in any way.

Digitalizing Kazakhstan's Courts: Keeping Up with the Times

Nail Akhmetzakirov

Head, Department of Ensuring Activity of Courts under the Supreme Court of Kazakhstan. Address: 39 Dinmuhameda Kunaeva Str., Nur-Sultan 020000, Kazakhstan. E-mail: 707-0007@sud.kz

Keywords

information, citizens, judiciary, proceedings, documents, electronic form.

For citation: Akhmetzakirov N. (2020) Digitalizing Kazakhstan's Courts: Keeping Up with the Times // *Legal Issues in the Digital Era,* no 2, pp. 173–177.

DOI: 10.17323/2713-2749.2020.2.173.177

The global digitalization trend has embraced all spheres of life, including the justice system, and Kazakhstan is no exception.

Back at the Sixth Judiciary Convention in 2013, the first president of Kazakhstan, Elbasy Nursultan Nazarbayev, ordered the broad introduction of new information technologies in courts. This was reflected in many strategic documents, including the 100 Concrete Steps National Plan and the state's Digital Kazakhstan program.

The experience of using new technologies in the Republic's courts earned positive reviews both within the country and abroad. Thanks to the digitalization of its courts, Doing Business ranked Kazakhstan 4th among 190 countries for contract enforcement and 2nd for judicial quality.

This result has been achieved through the systematic development of a number of information systems and services over the past five years. These include the Törelik system, the Internet portal of the judicial authorities, the Court Office service, electronic mailing systems and others. These have simplified the justice system significantly, making it mobile, transparent and easy to understand. Electronic justice saves citizens both money and time. Each of these steps deserves individual mention.

The unified platform of the judicial authorities (sud.gov.kz) was established in 2014. This site makes it possible to view information about the activities of the Supreme Court and all of the country's 390 courts. The site currently receives 25,000 views daily from more than 5,000 unique users.

In addition to its informational character, the content of this Internet resource also has practical applications. Any visitor can use such online services as Court Office, Court Summons, Reviewing Court Documents, Viewing Court Summons Documents, and justice-related FAQs.

The **Audio/Video Recording** (AVF) of court proceedings or electronic transcripts have now completely replaced paper records. Currently, 92,5% of all court cases are recorded using AVR. The service prompts not only the parties, but also the judges themselves to exercise greater discipline. The introduction of AVR has significantly reduced the number of appeals against judges' rulings.

Törelik (Arbitration) – the unified information system of the judiciary. This system makes possible the quick receipt of high-quality judicial information about judicial acts and the resolutions of complaints and requests submitted to the court. The service solved an extremely important problem: participants in the process can now constantly monitor whether registration, the acceptance of motions and the granting of deadline extensions for the consideration of cases are proceeding in a timely manner. The system identifies all deadline violations, making court employees more disciplined and eliminating the red tape connected with the use of paper documents. The Törelik system can generate statistical and analytical reports and simplifies paperwork and judicial procedure.

A special module of the Törelik system helps judges prepare judicial acts by "highlighting" all legislative discrepancies. As part of the project, the courts receive materials concerning misdemeanors and sanctions issued by the criminal authorities in electronic form only. This greatly expedites the handling of criminal cases and provides a unified record of criminal offenses and their perpetrators, as well as the decisions made regarding those cases during pre-trial investigations.

Electronic writ proceedings in civil cases. This project is noteworthy for having introduced simplified (written) proceedings in electronic format in 2018.

Automatic Case Assignment (ARD). This new system has greatly automated a very important service for judges. When assigning a judge to a case, it now takes into account each judge's specialization, workload, reas-

signment to another court, functioning as an investigative judge in criminal cases or on-duty judge in administrative cases, scheduled vacation time and work-related travel, and sick-leave. This updated ARD eliminates the subjective factor in case assignments, thereby reducing the opportunity for corrupt practices.

Court Office (SK) has been in operation since 2014. This unified electronic "window" that provides access to all court services, has changed the way citizens interact with the courts. Users using any type of gadget can submit more than 100 types of electronic communications to the court without leaving their homes. The SK makes it possible for users to see when their communication was registered as well as its movement (status) within the court system, and to receive a judicial act and an AVF of the proceedings. It greatly reduces the cost of paperwork and postal services, and is fast and secure.

The more than 300,000 people who now use the service have sent approximately 7 million communications to the courts. Whereas 3% of such communications were submitted to the courts through the e-government portal in 2013, approximately 75% were sent using Court Office in the first half of 2020.

The **Mobile Court Office** enables people to participate remotely in a court session, even when they are abroad. To do so, they need only connect to the service via a tablet or smartphone and receive ID confirmation from the court. During the first eight months of 2020, more than 300,000 such remote court proceedings have been held.

The service has been updated to enable users working from a gadget to use a QR code to authorize their log in and sign documents.

Every person in the country who uses this system will receive **SMS notifications** (through e-mail and the Court Office) indicating the date and location of their particular court proceedings. More than 3.5 million such notifications have been sent during the first eight months of this year. This gives people more time to prepare for the court process.

The **Situation Center** (SC) began operations in the Supreme Court in 2017. This is a centralized system for monitoring court activity. It serves as a clearinghouse of all information on judicial proceedings in the Republic, making it possible to quickly identify and correct any operational errors in the courts. The SK monitors the courts' activities according to 750 main indicators, including court proceedings, clerical correspondence, information security and AVF use.

A service for **Reviewing court documents using a QR code** has been developed and will be implemented soon. It will allow users to review and download documents by submitting a QR code.

The **Court Map** function allows users to locate court contacts, lawyers, mediators and notary publics in specific regions.

Digital Agent is a mobile application that allows users to rate the convenience, service, court procedures and work of court staff, leave complaints and suggestions, and contact court administrators online to obtain a quick resolution to any issues that arise.

Smart Court Bot is an application for the Telegram instant messaging service. It enables users to find the Telegram bots of every court, submit a question to a technical support operator and obtain other court services.

Obtaining Apostille for Official Court Documents. This state service is provided through the e-government portal (www.egov.kz).

Smart Cell is one of the pilot projects of the Seven Stones of Justice program announced by Supreme Court Chairman Z. Asanov in 2018 towards the goal of modernizing the judicial system and improving the administration of justice. The project aims to ensure that the court's IT services are satisfactory by accomplishing the following tasks:

ensuring unfettered and convenient access to the administration of justice;

automating court proceedings and making them cost-effective;

beginning working with big data, using all the possibilities of judicial practice worldwide.

The **Strategy for Digitalizing the Judicial System of the Republic by 2022** that the Supreme Court adopted in 2019 streamlines this process and "breathes" even more dynamism into it.

Improved laws. The civil procedure code of the Republic of Kazakhstan has been supplemented with a chapter on the distinctive features of electronic court proceedings. An electronic format for criminal proceedings has been introduced, as have a number of innovations in remote participation in civil proceedings and the use of gadgets and other technical means.

In Kazakhstan, IT services streamline court proceedings significantly. More than 90% of civil claims are filed electronically. The quality of criminal proceedings improves by integrating the information systems of courts (Törelik) with those of law enforcement bodies (The Unified Register of Pre-trial Investigations). The criminal prosecution authorities send courts materials on misdemeanors and sanctions in electronic form. This greatly expedites their review and makes it possible to maintain a unified record

of criminal offenses and their perpetrators, as well as the decisions made regarding those cases during pre-trial investigations.

Rules-based justice is an important factor in making Kazakhstan more attractive to investors. To achieve it, the Supreme Court and the Atameken National Chamber of Businesspeople are developing an IT program for judicial analysis and forecasting the outcome of court cases. It will help people better understand their legal situation.

Digitalizing the courts provides the following advantages to all participants in the process:

First, it makes it possible to control the entire process of civil proceedings — from the filing of a court petition to the final resolution of the case.

Second, it provides maximum transparency of judicial processes.

Third, it cuts costs.

It should be noted that the high level of digitalization of the judicial system has made it possible to transfer all courts to remote hearings promptly during the COVID-19 emergency, and in response to the CEPEJ guidelines (Strasbourg) of June 10, 2020 on the possible need to halt in-person court proceedings as a public health and safety measure. From a technical standpoint, our courts were ready for this. Online court proceedings differ from in-person sessions in the way they are conducted — that is, via a gadget. Online processes are also recorded in the electronic transcript of the proceedings.

With the support of the government, the number of mobile video conferencing servers was increased from 67 to 152. The bandwidth of communication channels and electronic storage reserves were also increased. Citizens were informed through the media and social networks that they should have sufficient Internet speed and mobile videoconferencing skills to participate in court sessions. Our courts have been able to carry out 100% of their functions in electronic format.

Up to 95% of all documents submitted to the courts now come in electronic form through the Court Office. The daily number of court proceedings held remotely has risen from 150 per day before the current crisis to 4,500 now, a 30-fold increase. As many as 99.5% of all judicial processes now take place online, and the parties themselves speak out about their online participation in the processes.

Plans call for equipping civil and criminal courtrooms with electronic equipment as well. The digitalization of the administration of justice continues.

Legal Issues in the **DIGITAL AGE**

ISSUED QUARTERLY

"Legal Issues in the Digital Age" Journal is an academic quarterly e-publication which provides a comprehensive analysis of law in the digital world. The Journal is international in scope, and its primary objective is to address the legal issues of the continually evolving nature of digital technological advances and the necessarily immediate responses to such developments.

The Digital Age represents an era of Information Technology and Information Communication Technology which is creating a reliable infrastructure to the society, taking the nations towards higher level through, efficient production and communication using digital data. But the digital world exposes loopholes in the current law and calls for legal solutions.

"Legal Issues in the Digital Age" Journal is dedicated to providing a platform for the development of novel and analytical thinking among, academics and legal practitioners. The Journal encourages the discussions on the topics of interdisciplinary nature, and it includes the intersection of law, technology, industry and policies involved in the field around the world.

"Legal Issues in the Digital Age" is a highly professional, double-blind refereed journal and an authoritative source of information in the field of IT, ICT, Cyber related policy and law.

Authors are invited to submit papers covering their state-of-the-art research addressing regulation issues in the digital environment. The editors encourage theoretical and comparative approaches, as well as accounts from the legal perspectives of different countries.

Legal Issues in the **DIGITAL AGE**

Authors guidelines

The submitted articles should be original, not published before in other printed editions. The articles should be topical, contain novelty, have conclusions on research and follow the guidelines given below. If an article has an inappropriate layout, it is returned to the article for fine-tuning. Articles are submitted Word-processed to the address: lawjournal@hse.ru

Article Length
Articles should be between 60,000 and 80,000 characters. The size of reviews and the reviews of foreign legislation should not exceed 20,000 characters.

The text should be in Times New Roman 14 pt, 11 pt for footnotes, 1.5 spaced; numbering of footnotes is consecutive.

Article Title
The title should be concise and informative.

Author Details
The details about the authors include:

- Full name of each author
- Complete name of the organization — affiliation of each author and the complete postal address
- Position, rank, academic degree of each author
- E-mail address of each author

Abstract
The abstract of the size from 150 to 200 words is to be consistent (follow the logic to describe the results of the research), reflect the key features of the article (subject matter, aim, methods and conclusions).

The information contained in the title should not be duplicated in the abstract. Historical references unless they represent the body of the paper as well as the description of the works published before and the facts of common knowledge are not included into the abstract.

Keywords
Please provide keywords from 6 to 10 units. The keywords or phrases are separated with semicolons.

References
The references are arranged as follows: [Smith J., 2015: 65]. See for details http://law-journal.hse.ru.

A reference list should be attached to the article.

Footnotes
The footnotes include legal and jurisprudencial acts and are to be given paginaly.

The articles are peer-reviewed. The authors may study the content of the reviews. If the review is negative, the author is provided with a motivated rejection.

Выпускающий редактор *В.С. Беззубцев*
Художник *А.М. Павлов*
Компьютерная верстка *Н.Е. Пузанова*

Подписано в печать 30.10.2020. Формат 70×100/16
Усл. печ. л. 11,25.