Legal Issues in the **DIGITAL AGE**

Вопросы права в цифровую эпоху

3/2020

ISSUED QUARTERLY

Articles

Comment

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

The Phenomenon of the Algorithm and Its Impact on the EU Legal System: an Attempt at a Multidisciplinary Approach

Stefano Dorigo

Associate Professor, University of Florence. Address: 4 Piazza di San Marco, Florence 50121, Italy. E-mail: stefano.dorigo@unifi.it.

Ettore M. Lombardi

Professor, University of Florence. Address: 4 Piazza di San Marco, Florence 50121, Italy. E-mail: ettoremaria.lombardi@unifi.it.

Erik Longo

Associate Professor, University of Florence. Address: 4 Piazza di San Marco, Florence 50121, Italy. E-mail: erik.longo@unifi.it

Stefano Pietropaoli

Professor, University of Salerno. Address: 132 Via Giovanni Paolo II, Fisciano 84084, Italy. E-mail: spietropaoli@unisa.it

Abstract

We are experiencing a digital revolution that is changing the very nature of law. Digital code becomes a form of regulation through which private actors link their values to technological artifacts that prove capable of conditioning their operations both on a material and moral level. But technological artifacts appear to be non-neutral means, reflecting choices of different nature, among which those of a political nature stand out. The more the regulatory provisions are implemented through the use of technologies, the more the codes acquire the status of a regulatory technique, which can be used both to define and incorporate regulatory and contractual provisions into codes both to implement them. The impact of the algorithm is of crystal clear relevance not only in regulation but also in the other side of the coin: surveillance. Each new option brought by the development of technology brings new possibilities and changes the way humans relate to each other. All these beautiful technological devices that few of us are willing to abandon produce a positive enhancement of the human and new kind of addiction, but also a new slavery". The algorithmic revolution spills over to society and public systems designed to ensure its well-being. So, fiscal consequences of the algorithmic revolution risk, if not governed, to call into question the very foundation of the social pact, to which the fiscal duty is connected as a manifestation of solidarity within an organized community, not only within the borders of the individual State but also in a wider sphere. Legal

scholars can face the newest challenges of the present without fear and without nostalgia. But to this purpose he must remove all obstacles to the necessary dialogue between jurists of different backgrounds, between jurists and non-jurists, between jurists and society.

Keywords

Artificial Intelligence, Algorithms, Constitutional law, Philosophy of law, Private Law, Robotics, Tax law

For citation: Dorigo S., Lombardi E., Longo E., Pietropaoli S. (2020) The Phenomenon of the Algorithm and its Impact on the EU Legal Systerm: an Attempt at a Multidisciplinary Approach // *Legal Issues in the Digital Age*, no 3, pp. 3–34.

DOI: 10.17323/2713-2749.2020.3.3.34

1. What is law? Three layers of the legal dimension

Law is a technology. Law is *techne*. It is the technology of social coexistence. To achieve this result, it uses very powerful technological machinery: the legal system, made up mainly — or exclusively for some [Kelsen H., 1967] — of norms.

The legal norm is a technical rule. If you want to work within the system, you must know how it works: you must acquire highly specialized technical knowledge. Law is the knowledge of doing or making things with norms [Austin J., 1962]. Surely, jurists change the legal world with normative propositions: we create institutions, modify personal status, and operate on society with these kinds of tools.

However, is law just this? Is it just norms? Is it just technology? Is it just a set of rules concerning a social body? Of course, not. Law is not merely the set of regulatory provisions that govern social organizations. Otherwise, we could talk about something like Neanderthal law and maybe even penguin law or ant law", and so on. We have to go beyond that.

Law has not always existed: it is a human creation, and it is not the first creation conceived by *homo sapiens*. Law is a specific kind of knowledge that was born in Ancient Rome a few centuries before Christ [Schiavone A., 2005]. Today, we still study Roman law not only because it allows us to learn two or three Latin phrases to impress our clients but also because the history of our research field was born there, in Rome: it was in Rome that a class of scholars started to dedicate themselves for the first time to *jus*, an autonomous area of knowledge, detached from religion, ethics and politics. It was in Ancient Rome that law became a science",

where the term science stands not for natural science or hard science or empirical science but for *scientia*, which in Latin means knowledge *per se* (just as *episteme* in Ancient Greek).

Thus, law is both technology and science. However, that is still not enough. Law is also a form of art". Why is Michelangelo's *David* so famous? Surely, because it is beautiful. However, more than that, it is the symbol of a young man with just a stone in his hand fighting against tremendous forces. And the young man — clearly a symbolic representation of Renaissance Florence — wins. It is the symbolic dimension of the work that really makes it stand out.

Law requires technical ability — *techne* — and overall vision — *episteme*. It uses tools and means to achieve high ends. It is rational, yet it cannot be purely rational because of the symbolic dimension at its foundation. It is ritual, yet it must also be myth [Stolfi E., 2020]. And law is also art", because it is artificial": it is a creation of the human intellect. It is not natural, i.e., there is no law without humans.

2. Law and ICTs. From sacred orality to blind computability

Law — technology, science and art together — provides mankind with a means of coexistence. In this perspective, there must be communication between humans. This is why law and communication technologies have always been bound together. For this reason, it would be useful to reinterpret the history of law in the light of the four great revolutions of information and communication technologies in an inevitably concise overview.

Let us start with language or, better, words. Law consists of words, and it is words that must be communicated. Law is *jus dicere*: jurisdiction. The very concept of normativity rests on this vision directed at other human beings and at the future. Nevertheless, in comparison to other forms of language, legal language has something magic about it. This is why primitive law was managed by priests: priests jealous of their own wisdom, which was exclusively oral wisdom.

As a reaction against such elitist knowledge, people demanded to know what rules were used to resolve legal disputes. They wanted to understand how these clerics made their decisions. It was a matter of power, of course. So, it happened that oral law was put for the first time in writing, as evidenced by the Law of the Twelve Tables or the *Jus Flavianum* [Zocco-Rosa A., 1914]. After law became written law, anyone who was capable of reading could access this knowledge, control it, and try to change it. The new law was without doubt more democratic than primitive law. It represented a revolution in law, related to the new use of the

technological instrument of writing: *jus* was separated from *fas*, the most sacred sphere. This marked the birth of law as a science studied by legal scholars.

This law naturally paid very close attention not only to words but also to the oral dimension. Nevertheless, for over a thousand years, the Roman paradigm continued to exert a fundamental influence in the West, precisely because it had succeeded — through writing — in taking away the power held by pontiffs and opening access to the management of legal problems, investing a new class of jurists.

Printing techniques were known already a thousand years before Christ. Still, the third revolution we are interested in took place in the mid-15th century when Johannes Gutenberg introduced the first movable type printing system in Europe. The technology of printing played a key role in the scientific revolution as well as in the birth of the modern state and modern law systems. Printing technologies made it possible to spread learning to the masses. However, they also served as a very useful tool for creating a monopoly on normative production in the modern state (especially, but not exclusively, in civil law countries).

Law was changing. This period marked the beginning of a process that led after the French Revolution to the emergence of the code as the main instrument of expression of the lawmaker's will [Grossi P., 2010]. In the nineteenth century, law became code, although this development had already been foreseen by Thomas Hobbes in 1651. Napoleonic legislation was the symbol of this change: all law was incorporated into codes, and there is no law outside the code. This approach obviously excluded all non-state sources, such as natural law, customs, and so on, from the legal landscape. Law became a complete and self-sufficient system. This legal theory or, more precisely, legal ideology was established two centuries ago and still plays an important role today.

We have finally arrived at the fourth revolution — the digital revolution — which we are experiencing today (perhaps without being fully aware of it). It would be a mistake to consider the ICT revolution only as the development of new instruments for law. Far from simply providing tools for law, the great ICT transformations changed its very nature.

The digital revolution raises the question: is law computable [Deakin S.F., Markou C., 2020]? In other words, the central problem today is to understand whether everything we call law can be formalized and reduced to a system of machine-readable signs [Brownsword R., 2020]. A problem of this kind would have amused people until the middle of the last century. Today, it no longer makes us laugh. Indeed, we have to take it very seriously.

Attempts that seemed to be ramblings a few decades ago must now be considered carefully and perhaps even with concern. We could try to lock ourselves

up in the ivory tower of twentieth-century scholars faithful to Roman law codes and say that law has nothing to do with such things. Nevertheless, we must face reality. And reality shows that this kind of approach is increasingly employed and already affecting the way law works. Software systems based on machine learning techniques have been used for years by the biggest law firms in the United States and Asia. So, we are faced with a real problem. Closing our eyes and behaving like ostriches will not bring us very far.

3. Tech for law and law for tech. Old rights changing, new rights emerging

The first way we can look at the connection between law and digital technologies moves from technology to law. In essence, we can examine the tools that technology has provided to law in recent years. This is what is commonly called lawtech.

Lawtech is the term we use to describe technologies that aim to support, supplement or replace traditional methods for delivering legal services or that improve the way the judicial system operates. Lawtech covers a wide range of tools and processes, including legal research, document automation, smart contracts, drafting automation, electronic dispute resolution, e-discovery and many other processes in law firms [Ashley K.D., 2019]. Such systems are already available. They can draft documents, perform legal research, disclose documents in litigation, provide legal guidance, and resolve disputes online.

All these tools are used by lawyers to perform their professional activities. Nevertheless, there is, of course, another issue that also matters to those who are not lawyers or judges: what tools can we use today to enforce our old rights? One example is the adoption of an electronic voting system. Obviously, it must be provided with all sorts of possible guarantees defending the constitutional values that are at stake. However, there are also more trivial examples such as the use of electronic mail or other electronically certified mail systems, electronic signatures, biometric keys and many other instruments with which we can enter into safe and reliable contact with the public administration to ask questions, make requests and protect our rights.

However, this perspective, too, goes from technology to law by providing tools for law. Let us try to reverse this perspective and look from law to technology. Let us consider how law is trying to address new problems in an increasingly digital society.

Someone has said that technology is an enabler of rights rather than a right in itself. Nevertheless, it is not clear whether this statement can be successfully de-

fended today. The two examples that come to mind are the right to Internet access and the right to Internet neutrality. Nevertheless, even without thinking about new rights, we can say that the digital revolution is radically changing the way old rights work, because there is no area of our social life — and therefore of the legal system — that is not affected by technological innovations. It suffices to think of the protection of personal data, which is increasingly overlapping with our identity: we are becoming what Google tells us about us, even if we do not like it at all. Or take the related issue of the freedom of expression, which must be balanced with the right to privacy. Or the freedom of association on the Internet, the exercise of consumer rights in e-commerce, the rights of workers (with the problem of surveillance at the workplace), the right to education (even in the form of remote education that has appeared in recent months), and so on.

New technologies are generating new rights and changing the way old rights are exercised. At the same time, they are creating new criminal activities and changing the way traditional crimes are carried out. Just a few examples: if you write on Facebook that I am a complete idiot, this is defamation; if you find the password to my e-mail account and peek into my correspondence, this is a violation of privacy as well as abusive access to a computer system; if you flood me with phone calls, instant messages, and emails, this is stalking; if you find some embarrassing photos on a portable storage device and want to send them to my wife, this is extortion; and, if you try to sell me the Trevi Fountain with an eBay ad, well, this is fraud. In all these cases, traditional crimes are performed using new technologies. Moreover, new crimes are appearing, too [Pagallo U., 2013].

The most common term for crimes committed exclusively through digital technologies is cybercrimes". Sadly, we are becoming familiar with such terms as phishing", revenge porn", ransomware", and maas". At the same time, we are becoming increasingly aware of the importance of cybersecurity.

Obviously, the first thing that comes to mind when we talk about illegal activities committed through information technologies are crimes against the person or against things and property. Then we think of state law. However, there is another issue of fundamental importance here: computer crimes are, by their very nature, transnational. Expressions and concepts such as *locus commissi delicti* have to be reviewed and completely changed, if necessary. There is another crucial aspect: cyber-attacks can also have relevance under international law. Contemporary international law is not only faced with the major problem of the military use of high-tech instruments such as drones. The very concept of war is changing. One mistake we often make is to consider cyberwarfare as a virtual war, as if it were a PlayStation or Xbox game. However, this is wrong. Cyberwarfare is real war — a war in the true sense of the word — because it can cause exactly the same damage

as traditional weapons. An example would be the cybernetic attack on the Iranian nuclear base in Natanz a few years ago.

4. Norm and technology are strongly interrelated concepts

In view of the complex scenario depicted so far, we can easily understand how human behaviour is increasingly influenced by a complex of factors of a digital nature on which artificial intelligence (AI) is based. As a result, AI is beginning to play a similar role to traditional codes of written rules designed to regulate the actions of a particular group.

Thus, the digital code is becoming a form of regulation that is making private actors link their values to technological artefacts that prove capable of conditioning their actions at a material and moral level. Consequently, norms in the sense we are giving them here must be considered as regulatory tools that make use of algorithms to regulate, whether directly or indirectly, the behaviour of the subjects they refer to.

Norms and technologies therefore form a complex relationship, interacting through a system of dependencies and interdependencies that contribute to the regulation of individual behaviour to a greater or lesser extent.

With the advent of modern information and communication technologies, the relationship between law and technologies has changed radically, as evidenced by the growing use of technologies as a complement to (and support for) law; this can be understood, according to some authors [De Filippi P., Hassan S., 2016: 3 ff.], by distinguishing four recent phases that explain the relationship between norms and technologies. The first stage, which is currently very advanced already, uses digitized information, replacing paper and ink by complex data available on computers and giving users a huge corpus of jurisprudential cases, laws and regulations that were initially available for a fee through large databases yet have been gradually placed in open access [Berring R.C., 1986]. The second stage involves the automation of decision-making processes: most of the research carried out by legal information technologies focuses on translating regulatory provisions into computer code. Both policy makers and judges use IT applications to derive regulatory provisions and jurisprudential guidelines and to analyse and compare them in order to structure arguments that are adequate for the purpose and improve the decision-making process [Waterman D., Paul R., Peterson R., 1986: 212 ff.]. However, this objective can only be achieved with difficulty, not least because of the ambiguity that can characterize legal language and of the need for rules to be flexible and linked to factuality [Grossi P., 2014]. Despite these difficulties, government institutions and the global business community are trying to create

automatic and semi-automatic decision-making processes (e.g., specific IT applications for taxation) on the basis of the experience of different sectors such as healthcare and fiscal and financial regulation. The third stage has witnessed the transformation of legal rules into algorithms, on the one hand, and the emergence of regulation through algorithms, on the other.

With the widespread diffusion of the Internet, we are witnessing the *de facto* emergence of new forms of regulation that increasingly rely on soft law (i.e., technical rules) for disciplining human behaviour with an ever-greater number of interactions being governed by computer programs and with technological support providing significant assistance not only for taking decisions but also for the direct implementation of rules. In this context, algorithms can assist in identifying what is or is not admissible in regulating legal relationships, thereby making the rules of application much more efficient [Reidenberg J.R., 1998; 553]. During the fourth stage, which has just begun, one is developing a new approach to regulation (the so-called codification of the standard"), which involves a growing use of computer codes not only for implementing but also for elaborating legal rules.

5. The impact of technological artefacts on policy makers' strategies

As an indispensable tool in all areas of human existence, information technologies are playing a central role in contemporary life that has been marked in recent years by the growing influence of certain basic phenomena such as machines with increased autonomy and the capacity for self-learning. The latter stand out through their complexity and, above all, their ability to elaborate, predict and plan the human decision-making process, which supports the idea of the gradually growing role of AI in human existence [Christian B., Griffiths T., 2016].

It is therefore not surprising to observe that the development of these types of machines raises some difficult questions about the way in which human beings can adopt a predictive attitude and how this can influence, in a more or less reliable way, the prediction of the future.

The fact is that technological tools had existed as a means of implementing regulatory data long before the advent of modern information technologies.

Thus, far from being neutral means, technological artefacts are profoundly subject to the influence of laws adopted by policy makers, which indicate the type of actions to be prohibited or condoned [Mowshowitz A., 1984].

If political choices are, either intentionally or unintentionally, incorporated into the way technology is structured and if these different configurations have a

significant social impact insofar as they support certain political groups or facilitate certain actions or behaviour towards others [Winner L., 1980: 234 ff.], then we may speak of four forces that exist and combine, to a greater or lesser extent, to shape individual actions in ways that are often beyond the control of the individual: the law, social norms, the market and the composition of spaces [Lessig L., 1999].

The law creates artificial constraints that limit the actions of individuals by legal rules (for example, prohibiting theft and punishing those who violate this rule), social norms regulate cultural behaviour through peer pressure (for example, it is not acceptable to speak aloud during a professional meeting), the market encourages or discourages certain behaviour by resorting to the mechanism of supply and demand (for example, by predicting prices for certain goods or services), while the composition of spaces — i.e., the way in which the surrounding world is structured both naturally and artificially — imposes a series of limitations that affect the type of actions that an individual can undertake (for example, biology, technology or geography) [Malone G., 2008: 139]; [Yeung K., 2010]; [Semeraro M., 2012: 808]; [Sirena P., 2014: 3 ff.]; [Enriques L., 2009: 1147] (including an-depth discussion of the impact of regulation on the financial market); [Andenas M., Deipenbrock G., 2016].

The unprecedented diffusion of information technologies and the globalized network have contributed to the creation of a new environment for human beings and their behaviour, whose rules are implemented in algorithms. Just as any other technological artefact, this algorithm reflects different kinds of choices, especially in the political domain [Christian B., Griffiths T., 2016].

The algorithm can, therefore, form the basis of a new construct capable of conditioning individual human actions through the use of technological tools. What impact, then, can the algorithm have on the traditional regulatory scheme, whose primary referents are the regulator and the law?

Although technological infrastructures can be structured to promote or prevent certain types of behaviour, the desired effect cannot always be guaranteed, as technological tools are used for different purposes that may depend on specific contingencies.

The implications deriving from the use of particular technologies, therefore, cannot be fully grasped without viewing them in the social and historical context where the technologies are meant to operate. In fact, more than its structure, it is the way in which a technology is meant to operate according to the choices made by a particular group of individuals that determines its influence on the social and political spheres.

Regardless of whether or not this effect is intentional, the digital world opens the doors to new forms of regulation that are entrusted to private actors who seek to im-

pose their values by embedding them in a given technological tool, which, depending on the concrete use to which it is put, can influence the way a certain number of individuals behave [Jeorges B., 1999: 428]. In a nutshell, it is possible to describe the relationship between regulators, norms and algorithms in terms of conflicting energies: whereas regulators try to control socio-economic dynamics with their rules, algorithms can create regulations that have their own legitimacies if they have been previously legitimized by the public sphere from which they take their binding force.

6. The two-way relationship binding rules and algorithms: towards the need for flexibility and prediction

The framework outlined so far shows that there is a two-way functional exchange between norms and algorithms. Thus, while the use of algorithms aims to reinforce the application of normative data, the latter can also serve as a tool for strengthening the correct and adequate use of algorithms to avoid their violation or alteration. The fact remains that the transposition of legal rules into technical rules, which requires the elaboration of an algorithm as a means of defining the application of normative data, is not an easy operation insofar as, unlike legal rules that are developed using a language that is intrinsically ambiguous, technical rules must be transposed into codes and are therefore based on algorithms and mathematical models. It is the peculiar ambiguity of the legal system, which is necessary to ensure an adequate and potentially flexible application of the rule on a casuistic basis, that allows algorithm programmers to incorporate their own understanding of normative data into the technical artefact they are developing — the algorithm [on the specific problem of the configurability of the new type of algorithmic responsibility, see [Ruffolo U., 2017: 148]. Thus, although it is true that, in the digital world, the algorithm is increasingly assuming some of the functions traditionally ascribed to legal operators (in particular, judges), it is also true that, in recent years, law has increasingly begun to take on the features of the computer code [Lessig L., 2000: 1]. (The recommendations on the use and impact of artificial intelligence are particularly relevant at the EU level. They have been developed by the European Commission and disseminated through the adoption of the European Ethical Charter for the Use of Artificial Intelligence in Judicial Systems and Related Areas on December 4, 2018, and of the European Communication Building Trust in Human-Centric Artificial Intelligence on April 8, 2019.)

The characteristics of the norm thus constructed should essentially translate into a high level of malleability and adaptability, allowing individuals to experiment with a wide range of versions and adaptations of the same rule, and into an *ex ante* implementation of technical rules with the respective legal implications, which could also derive from a predictive key.

While codes and algorithms have begun to be used on a major scale in recent years, we are also witnessing the gradual delegation to technologies of fundamental activities embodied in the interpretation and application of regulatory provisions or, at least, of attempts to do so, which, assuming different degrees of complexity and articulation, allow the achievement of increasingly valuable, appreciable and technically sophisticated results.

However, it is not always easy to transpose wet code into dry code: while the former makes use of intrinsically malleable language and can be applied, on a casuistic basis, to an indefinite number of hypotheses that may not have been foreseen in detail from the start (abstract and general rules), the latter employs a precise and formalized language with well-defined categories and a methodological choice that must be established *ex ante*.

For this reason, it can be argued that the norm is progressively transforming itself into a code: the more provisions are implemented through the use of technologies, the more codes acquire the status of regulatory techniques that can be used both to define regulatory and contractual provisions and to incorporate them into codes.

The elaboration in codified form of legislative and contractual provisions ultimately entails a further consequence — namely, that rules are traditionally conceived in sufficiently broad, abstract and general terms so as to be applied to a variety of different situations and to have a binding effect both at the time of promulgation and in new and unforeseen situations that are factually different from those contemplated in the original norm but show similar traits at the practical and ideological level. For this reason, the standard must be read and reconstructed in its scope by the interpreter before being applied.

For a long time, norms were drafted by human beings and intended to be applied to and by other human beings. As a result, they needed human judgement to give them meaning that would take into account the intentions of the legislator and therefore consider the context and the contingencies that existed at the time the norm was drawn up [for a further discussion of the interpretation of rules, see, among others [Mengoni L., 1996: 103–114]; [Alpa G., 2017: 35].

Because of this ambiguity and flexibility, regulatory and contractual provisions cannot be transposed into code and automatically implemented unless they are anchored to a formal language whose high degree of technicality can only be processed and grasped by a machine. However, this would entail the simultaneous rejection of genericity and abstraction for the sake of an ever more precise formulation that could be interpreted more objectively than before.

The result of this process would be the greater ease in transforming provisions into codes that, thanks to the corresponding algorithms, entail automatic applica-

bility facilitated by the use of technological tools. However, the trend towards an increasingly formalized language that allows the code to be rigid and penetrating in its application mechanisms contradicts the traditional concept of a norm perceived as flexible and adequately ambiguous.

The judge, however, cannot limit his/her functions to simply declaring the norm and intervening constructively only in the event of its indeterminacy, insofar as codes that are based on a detailed regulation of the activity of interpretation must be drafted in such a way as to allow the legal operator to clarify the will of the legislator. Only in this way can judicial discretion expressed in interpretative activity be preserved even in times of codification.

If, then, the computer code, like any other technological tool, can reflect political interests and if its way of being structured can have significant implications for the work of many individuals, the call for greater flexibility must be heeded. Since codes cannot be complete or regulate all cases faced by judges, they must refer to further sources of law and allow for the relativization of their use. Only in this way can the authentically human function of legal operator recover its real scope through the importance assigned to details. While the latter are often ignored by the objectivized operation of the computer code, they can acquire enormous importance in a specific case and bring out its most characteristic and specialized traits, both at the national and at the European levels.

7. Algorithmic surveillance

The impact of the algorithm is of utmost relevance not only in regulation but also in the concomitant process of surveillance. Indeed, a number of questions may arise about the impact of algorithmic decision-making on the idea and practice of liberty [Brownsword R., 2019]. One of the biggest concerns today relates to the power of national and big tech companies to make surveys with the help of big data analytics and other powerful means of automatic computation [Pasquale F., 2015]; [Zuboff S., 2019]. This is why the power of technology must be subject to rules no less than any other licit or illicit power.

The massive use of algorithms has improved people's lives. Each new technological development creates new opportunities and changes the way humans relate to each other [Rifkin J., 2014]. Today, we know that these improvements have a price". All these beautiful technological devices that few of us are willing to abandon expose us to the reasonable certainty of being potentially monitored at any time: they produce not only a positive enhancement of the human and a new kind of addiction but also a new slavery", as writes in his recent book Remo Bodei [Bodei R., 2019].

We take for granted that the benefits — security, efficiency, protection, rewards, and convenience — compensate for the fact that our personal data is recorded, stored, recovered, crossed, traded and exchanged through surveillance systems. Since ordinary people have no reason to question surveillance (the nothing to hide misconception) [Schneier B., 2015: 446], the order built by the system is strengthened, allowing people to be normalized (as Foucault would have said) by the system [Lyon D., 2003].

Because of the massive use of technology, we are now subject to a new form of surveillance that has a more profound impact on the freedom of individuals, being intrusive and invasive in private life [Lyon D., 2001]. Explicit and non-explicit forms of surveillance affect virtually all forms of human interaction. In addition, surveillance has become ubiquitous and continuous, and we can no longer evade it.

Over the past twenty years, surveillance, counter-terrorism, pandemic, and us, four elements that formerly had nothing in common, have become more closely connected than we could have ever imagined. Tools formerly employed only for targeted surveillance are now in common use. Applied only selectively before, they can now be used by anyone and at any moment, even with no particular purpose.

During the COVID-19 pandemic, Chinese and Korean authorities have used — in addition to more familiar authoritarian techniques of control — data from the world's most sophisticated mass surveillance systems to track infected people. This has not always had positive outcomes and, in any event, taken place at the expense of citizens' rights [Joe C., 2020; Mozur P., 2018]. Other governments have implemented extraordinary measures limiting the exercise of fundamental rights and civil liberties in order to stop the spread of the disease: among the other measures, surveillance has played a major role in compelling people to stay at home or limit their social activities.

The pandemic has also increased the relevance of the power of algorithms over us. In a world where connections have replaced social relations [Simoncini A., 2020], our smart devices have become not only tools of communication but also indispensable means for studying, working, training, and entertaining, as well as for being watched.

In our soft and liquid society [Bauman Z., 2006], forms of control and surveillance have multiplied [Hijmans H., 2016]. However, differently than in the past, they are no longer the exclusive prerogative of institutional powers, as Jeremy Bentham [1995] has shown. Today, they profoundly depend on the participation of those being surveilled: not only being watched but also watching has become a way of life [Lyon D., 2018].

If we apply the Marxist interpretation of capitalism to this industry, we can understand how and why simple forms of surveillance have turned into mass sur-

veillance [Gambetta D., 2018] thanks to the parallel tendency of the Internet to create societal benefits while making the protection of some fundamental values ineffective [ECHR, 2015]. We have gone far beyond the mere exploitation of our data, as Shoshana Zuboff explains: You are not the product; you are the abandoned carcass. The 'product' derives from the surplus that is ripped from your life [Zuboff S., 2019].

As the EU Court of Justice has pointed out, mass surveillance can be implemented by both governments and private companies, and it is likely to produce in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance"[1]. In both cases, we see surveillance that is intrusive of people's lives and entails the loss of control of individuals over their personal data.

Mass surveillance, which takes the form of seeing and being in the digital milieu, is inseparable from the so-called data exhaust pouring from millions of machines every moment of every day and the greedy global effort to create value from them [Lyon D., 2018: 170]. People strive to be connected, amused, entertained, supplied, updated, reassured and informed by the power of digital life. Gathering data from people and groups is made possible by numerous means today, including photography, video, genetic footprints, fingerprints, and face recognition. Furthermore, databases can be interconnected through cloud storage, and data can be extracted and immediately aggregated from multiple sources. However, as we engage in online life, we not only perceive being subtly watched by an external power but also employ surveillance tools from within in many contexts and for many purposes [Accoto C., 2019]. Surveillance is indeed welcomed as a means to attain greater security, convenience, and efficiency [Cohen J., 2016] and only seldom queried or resisted as being inappropriate or excessive [Lyon D., 2018: 151].

The result of these changes is that today all of us are more dependent on surveillance mechanisms than in the past. However, the result of this unprecedented revolution is different from anything we have seen before, as we are now not only passive subjects of surveillance but also active masters of it. Indeed, when we integrate everyday life with surveillance technologies, we expose ourselves to them and, more profoundly, participate in them to make them possible, legitimate and institutional. It has been said that surveillance is the fertilizer behind smart devices and the Internet of Things.

Furthermore, surveillance is convenient both for the controller and the controlled, since it gives the latter a sense of security and protection (surveillance is intrinsically ambiguous [Lyon, 2003: 11]). Our societies are increasingly based on

[1] Joined cases C-293/12 and C-594/12, *Digital Rights Ireland* (C-293/12) and *Seitlinger* (C-594/12), EU:C:2014:238, par. 37.

security anxiousness [Greenwald G., 2014] that is generated by the odd perception of menace to our security and the corresponding demand for abnormal protection [Lyon D., 2003: 11].

The effects of these systems and processes should be understood from an empirical point of view but also with regard to the profound social, economic, political and anthropological changes that they entail. While surveillance remains an aspect of social control that is always present in human relationships, mass surveillance points to the emergence of a different conception of life and society.

This may well be the real point of departure of the idea that code as the architecture of the Internet is capable of constraining the actions of individuals via technological means [Lessig L., 2006].

The implications for liberty should not be underestimated, insofar as private freedoms and democratic participation can be moulded in accordance with what business and government know about individuals [Benkler Y., 2011].

However, the emerging era of big data does not only entail the progressive loss of control over personal information but also shows the incapacity of governments to deliver protection [Hijmans, 2016].

The logic of exchanging privacy for convenience and efficiency amplifies the weakness of the notice and consent paradigm upon which the legality of data treatment rests [Yeung K., Lodge M., 2019]. In this situation, it is practically impossible for individuals to provide meaningful and voluntary consent to the activities entailed in algorithms (for a discussion of the uncertainties related to privacy in the context of big data, see [Acquisti A., Brandimarte L., Loewenstein G., 2015: 509–514]).

8. If it is no longer possible to evade surveillance, can we protect ourselves from it?

The legitimacy and accountability of this kind of surveillance is at stake due to the secrecy and the cooperation of the private sector in government surveillance, as a result of which surveillance activities, whether targeted or massive, are threatening constitutional guarantees.

To be legitimate and guarantee data protection and other constitutional freedoms, surveillance tools and algorithms should be designed and used with a view to their purpose (as set out in Article 9 of the GDPR), proportionality and effects for individuals (one of the most important rights is the empowerment of individuals", which must be assured by improving the ability of individuals to control their data as set out in Article 16 of TFEU [Hijmans H., 2016]). While this is easy to

codify, it is difficult to implement in practice for many reasons that mostly involve technological issues.

Examples of how the development of surveillance systems can infringe on freedom and democracy are abundant. The most striking cases today relate to the use of face recognition software — probably, the most controversial mass surveillance tool used today.

One of the most recent examples of the dangers of this technology concerns the small company Clearview that has written a code for face recognition better than any application available so far. It is so powerful that over 600 US law enforcement agencies have bought Clearview in recent years [Hill K., 2020].

Clearview has done something extremely invasive on today's Internet to beat its competitors. It has massively harnessed photos uploaded on Facebook, Instagram, and Twitter and videos on YouTube to create an immense archive at the disposal of its powerful algorithm. The same reporter of *The New York Times* that covered this story discovered some unknown photos of herself. Not surprisingly, it was Clearview's algorithm to trace such pictures on the web by matching them with her name. The algorithm seems to survey data silently, waiting for the moment when stored and indexed information becomes useful for face recognition. Considering the kind of data accumulated, we can conjecture that this is the biggest database ever built [O'Flaherty K., 2020]. Clearview has sold its face recognition service to the FBI and hundreds of local police offices, which are using it for solving extremely difficult cases [Schuba T., 2020]. Currently, Clearview is targeted by a lawsuit alleging violations of privacy law in Illinois[2]. Meanwhile, the US Senate has introduced several bills regulating the use of such technologies in law enforcement activities[3].

This example shows how forms of targeted surveillance that were developed for monitoring and apprehending terrorists could become systems of mass surveillance if used on a massive scale. The Clearview case sheds light on the loss of control over personal information in an algorithmic society in which public institutions do not consider the dangers of outsourcing services to systems that collect, capture or otherwise obtain personal data without informing the subjects of these activities. In addition, it is evident that any face recognition system must also include a mechanism for assessing the risks produced by the deployment of this technology in society and the secondary use of data for other purposes. The analysis of the impact of face recognition systems must therefore compare the current situation (for example, supervision and recognition by human agents) with a

[2] Hall v. Clearview AI, Inc. et al (Case No. 20-cv-00846).

[3] S.2878 and S.3284 — 116th Congress (2019–2020).

scenario based on the implementation of automatic recognition with the help of data uploaded on publicly accessible social platforms (for a discussion of the legal issues created by face recognition, see the recent report [FRA, 2019b]).

Particularly worrisome is the use of face recognition tools in school for security purposes [Weinstein N., 1980: 806–820]. At the moment, the introduction of such technologies is forbidden by national data protection authorities (Sweden and France) and administrative judges (France). As far as we can see, the real issue at stake in such cases is the use and storage of data — namely, the extent to which school and other authorities keep data about students and the level of security that they apply in managing them.

In view of this situation, many scholars have argued, following David Lyon, that the advent of the superpanopticon", whose main characteristic is total and uninterrupted surveillance by states [Lyon D., 2003], has taken place over the last twenty years. This may seem to imply that more power over citizens has been concentrated in the hands of states, yet a closer look shows that this conclusion is wrong for many reasons [Tincani P., 2015: 72–87]. The superpanopticon increases the *de facto* power of legitimate dominion only in the event when the latter has a monopoly on the (legitimate) means of power and control. In contrast, technological transformation has increased private powers, giving them a tremendous ability to control and monitor people in addition to states [Lyon, 2018]. Moreover, the power of surveillance and the concentration of the data gathered by both public and private mechanisms is focused on a small number of actors, public and private, based mainly in one jurisdiction and leading to a rapid erosion of state sovereignty and democracy [Pinto R., 2019].

The supervised society — a society in which surveillance can be infinitely extended until it observes the entire population — is achievable only if surveillance is automated, which requires the availability of powerful technological means.

9. The protection of fundamental rights

Let us examine the specific new technologies (in particular, technologies for mass surveillance) that are currently presenting the biggest challenges to freedom and democracy.

New technologies with algorithmic power are being continuously developed and rapidly deployed despite inadequate transparency, high uncertainty, and little knowledge of the exact data processing techniques (for a description of the problem, see [Yeung K., 2018: 505–523]). Today, this process is accelerating to such an extent that some people are speaking of a Cambrian explosion of technologies with potentially harmful implications [Kurzweil R., 2004: 381–416]; [Pratt G., 2015: 51–60].

In the context of algorithmic governance, we are continuously being faced with algorithmic unknowns", especially in the case of machine learning [Andrews, 2019a: 210–211]. The problem of machine learning algorithms becoming too complicated for humans to understand is a major concern in view of the widespread necessity of building administrative capacity in this field [Andrews L., 2019b: 296–310].

The problem of the unknown or black box effect is surely one of the most important issues today, particularly due to the harmful or discriminatory effects of some algorithms.

From a constitutional point of view, this situation has come into conflict with basic data protection principles set down in the GDPR [De Gregorio G., 2018: 65]. These principles aim at structuring and limiting the processing of personal data and making it transparent for data subjects[4]. In addition, personal data should be processed only for specified and explicit purposes, as the Clearview case shows. Data processed through machine-learning AI is based on large data volumes that are used for training and testing and that have been collected for other purposes and may be not suitable for new functions. Thus, AI comes into conflict with the basic conception of the current data protection law because in many cases even the programmers — particularly in the case of unsupervised learning — are no longer able to comprehend how AI obtains its results [Marsch N., 2020: 33–52]. While the GDPR counteracts the imbalance created by the platform economy by giving individuals powerful rights in the new arena where private powers are dominant, simply attributing new rights does not solve the asymmetry of power.

This perspective leads to a further concern. Algorithms collect and process vast quantities of personal and biometric data, making individuals highly visible to the public eye [Van Dijck J., 2014: 197–208]. These processes not only make individuals susceptible to private monitoring and profiling but also put privacy and democratic values at risk, since they increase the online transparency of citizens and reduce the sphere of their autonomy [Richards N., 2015: 168]. This new transparency reverses, for example, the presumption of innocence and generally diminishes the zone of individual freedom, as scholars have pointed out [Reidenberg J., 2014: 583].

The right to individual self-development can only be exercised by people who have control of their own lives (self-determination). Constitutionally speaking, this presupposes the protection of informational self-determination", as the capacity of the individual to determine the disclosure and use of his personal data"[5].

[4] Cf. Articles 5 and 6 of the GDPR.

[5] German (Federal) Constitutional Court 1 BvR 209, 269, 362, 420, 440, 484/83 'Census Judgment' (15 December 1983), par. 155.

Rather than being an end in itself, this right is a means of protecting other fundamental rights –especially democracy and the freedom of expression[6].

The last key element in this domain concerns the likely discriminatory effects produced by the automation of decision-making due to its inexplicability and unpredictability [Bygrave L., 2014: 220]. This applies particularly to the aspects of discrimination and persuasion, since individuals might not know that they are being discriminated against or persuaded or even that this can happen at all[7]. In this context, it is important to note the possible negative implications for fundamental rights (the right to non-discrimination, economic and social rights, the equality between men and women, the access to a fair trial and effective remedies, and the right to private and family life, as well as the protection of personal data) produced by machine-learning algorithms fed with low-quality data [FRA, 2019a].

10. A representative example of the impact of digitalization on the regulative and supervisory dimension: algorithmic revolution and tax law

At this point of our analysis, it is of paramount importance to consider an even more practical aspect of the thesis so far elaborated. As one easily sees, the dematerialization of the usual activities of digital multinationals thanks to algorithms makes it difficult to identify the territory in which these multinationals act and obtain their income. Therefore, the two fundamental concepts of international taxation — source and residence — are put into question [Pistone P., 2016: 395 ff.].

The fact that digital business is based on dematerialized goods and services abolishes physical presence in a specific jurisdiction through such material structures as offices, factories, and warehouses. Digital business is free to move across states without particular difficulty, since it is not linked to any territory by forms of stable and tangible presence that would not be easily moveable by their very nature [Brauner Y., 2018: 462 ff.]; [Cipollina S., 2014: 21 ff.]. At the same time, even the source of income becomes malleable, since transactions are dematerialized, often conducted in a non-place (such as the cloud), and are not linked to the production and delivery of a good that can be placed in a certain physical space: they depend on the location of the user with his device, an uncertain and changeable element by its very nature. The identification of the state with the right to tax relevant income is, therefore, called into question [De Wilde M., 2015: 796 ff.]. Moreover, in

[6] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Feb 27, 2008, 120 Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 274 (F.R.G.).

[7] In the European context, this was the case of the judgment made by the court in *Google Spain and Google v CNIL*.

the context of the digital economy, there is uncertainty in the determination of taxable income, since most of the time the user does not pay a sum of money but accesses services free of charge by providing his/her personal data; it is therefore difficult to determine the economic value of a transaction for a company. One of the main characteristics of the digital economy often emphasized by the OECD is the economic exploitation of hard-to-value intangibles: *hard-to-value intangibles […] means intangibles that the current arm's-length-based transfer pricing regime is unable to regulate* [Brauner Y., 2014: 98 ff.].

The fiscal consequences of the use of algorithms can also be seen in the field of intelligent machines employed in industrial production. Due to its relation to physical goods sold against payments on traditional markets, there are no problems related to the residence of the company or to the identification of its source of income. However, in some situations, companies can gain a competitive advantage over others by investing in automation and thus achieving higher production levels at lower cost. This entails the replacement of human labour (including, to a certain extent, intellectual labour) by machines with a consequent loss of revenue for the state, since workers who lose their jobs to robots stop receiving wages and are therefore no longer subject to income tax. This creates problems for public coffers, all the more so as they have to finance social support measures for different categories of workers expelled from the production system. It should be said that some analysts have called for public intervention to protect weaker categories of workers. They propose, among other things, creating a national dividend by making each technological enterprise confer part of its actions to a public trust so that every member of the community becomes a *de facto* shareholder. Rather than discouraging the development of robotics by introducing a tax, the national dividend would allow all members of a given society to have a decent standard of living even if all human workers were replaced by robots [Varoufakis Y., 2017].

As in all revolutions, new and unexpected situations arise rapidly (and violently — understood not in a physical sense but with reference to the incisiveness of the change that they impose on previous situations) and, as such, are not covered by the legal regulations in force, albeit the latter are designed and implemented for very different situations. At the same time, there emerges a category of subjects (whether digital multinationals or manufacturing companies capable of automating their production processes) that are able to take advantage of such situations, drawing fiscal benefits that may be lawful, as they are generated in strict compliance with the rules in force, yet act to the detriment of both competitors and the community and ultimately put the social pact to a very severe test. Finally, as a consequence of the two elements just mentioned, there appear clear ruptures in the economic and social order with the drain of public resources and the simultaneous emergence of social tensions fuelled both by small local businesses, pressed

by digitization, and by the mass of workers for whom the social protection of the state becomes increasingly insufficient (in particular, due to the loss of revenue mentioned above).

In short, the fiscal component of the algorithmic revolution first impacts the economy and then (just as all revolutions) spills over to society and public systems designed to ensure its prosperity.

One must therefore ask whether tax law, with its current principles and rules, is able to cope with this emergency by mitigating social risks through a fair redistribution of wealth among the affiliates or whether, on the contrary, it is not up to the task, as many of its basic concepts and institutions need to be rethought in view of lessons deriving from other branches of law (international and EU law as well as constitutional law), since what is at stake is not just tax revenues but the entire system of individual and collective rights, as well as the rules of the economy based on a level playing field and the social function of enterprises.

It seems that the most alarming consequence of the algorithmic revolution, seen through the prism of tax law, is not so much that some operators can generate unimaginable profits that can make them compete even with sovereign states but, rather, the fact that these profits are not, in the majority of cases, submitted to a fair level of taxation in the state (or states) where they are generated and where the need for a more intense participation in public expenditure is therefore greater. We are thus faced with a situation in which a more favourable tax position is at odds both with the inalienable solidaristic aspect of tax duty [Sacchetto C., Pezzini B., 2005][8] and with the social mission of enterprises that is now strongly emerging in doctrinal reflection and practice. This means that market advantage with the concomitant increase in available profits is not — as it should be — a presupposition for solidarity with the territorial and social communities that made it possible but, in a paradoxical reversal of the situation, is the result and consequence of the failure to fulfil one's duty to contribute to the public expenditures of the state in which the value was created and, in a distinct yet related manner, to direct the selfish aims of the enterprise towards objectives of social utility (or at least towards not harming the local community).

[8] The vast scope of the doctrinal debate on the function of taxation and its link, through the ability to pay, with the principles of substantial equality and solidarity prevents us from giving an adequate account here. We should simply say that scholarly studies on this subject often emphasize the connection between the contribution to public expenditures and the need to take into account the role of the taxpayer within the social organization [Gallo F., 1998]. It follows that taxation is an instrument through which the individual participates in the social organization both as a person who benefits from goods and services made available by the state and as a contributor to the relevant expenses. Thus, if there is taxation, then there is a social structure within which the taxpayer moves.

One therefore understands that, unless the fiscal consequences of the algorithmic revolution are regulated, they can call into question the very foundation of the social pact, to which the fiscal duty is connected as a manifestation of solidarity within an organised community, not only within the borders of an individual state but also in a wider sphere (as the experience of the European Union shows).

11. The possible reactions of the tax system: interventionism or laissez faire?

The question arises whether tax law can be made to play a positive role in the management and regulation of the situations described above [Lesage D., Vermeiren M., 2011: 43 ff.]. Opinions diverge on this matter. On the one hand, there exist advocates of a more incisive role of tax law in the sense that new forms of taxation should be imposed on new activities to allow states with ordinary tax regimes to recover revenues for their own welfare needs. On the other hand, there are those who value the role of the market, which is capable, or so they argue, of striking a balance between antagonistic conditions on its own. It has been held that automation and AI are not necessarily synonymous with technological unemployment and its negative effects and that technological change can, in fact, create new types of jobs [Falcão T., 2018: 127–131]. Indeed, the introduction of a levy with a balancing function could have the opposite effect, inducing the most advanced operators to abandon the state and depriving it of the advantages of their presence (in terms of investments and infrastructures).

The first direction, which we could call sovereign", promotes the strong role of state and the redistributive effect that taxes generate; the second ("liberalist or market") approach opposes all regulation in the name of the trust in progress and the ability of the market to find a vaccine against the inequalities that new phenomena initially produce. Both approaches seem weak, as they are based on controversial assumptions. Indeed, the sovereign approach fails to resolve the problem of capital flight in the new economy as a result of the unilateral, and therefore uncoordinated, introduction of restrictive fiscal measures. Similarly, liberalist theories adopt an abstract philosophical vision that is increasingly refuted at the practical level on account of the persistent inequalities that favour only a few large operators to the detriment of most others.

A third way can be proposed. It seeks to combine economic freedom and the protection of the tax revenues of states by enhancing, as a balancing element, individual and social rights in a supranational perspective. A multilateral approach is therefore needed, making it possible to regulate the activities of algorithmic companies while avoiding the negative consequences of unilateral measures [Garcia Antòn R., 2016: 148 ff.]; [Pistone P., 2014: 3 ff.]. Multilateralism calls for synthesis

that would, on the one hand, ensure that national systems are incapable of exerting unfair competition by failing to comply with supranational guidelines and, on the other, reduce the gap with traditional companies. An example would be negotiating multilateral international instruments aimed at making states introduce uniform taxation systems for high-tech corporate income [Avi-Yonah R., 2015: 33 ff.] a guaranteed minimum level of taxation would protect the revenues of the most advanced states (and therefore the stability of national welfare systems), while the uniformity of rules, at least in the tax domain, would discourage multinationals from moving their businesses elsewhere in search of better conditions.

Without a doubt, such proposed tax measures are not new. Global tax governance has been discussed for some time now now [Rosenblum D., Noked N., Helal M., 2014: 183 ff.]; [Stewart M., 2012: 152 ff.] and largely been accepted in principle. Some authors have observed that the traditional defensive model, which lies at the root of the concept of unilateral taxation, is giving way to a supranational approach based on international cooperation between states, even though this path is full of difficulties [Cipollina S., 2015: 356 ff.]. Such an approach has to be a substantial multilateral intervention, i.e., it should deal with the fundamental elements of taxation linked to the profits of the algorithmic economy. In short, the aim should be to sign an international agreement for introducing a global system of taxation introducing a minimum tax rate for income deriving from activities related to this economy that would be applied in every country. Two remarks should be made in this respect.

First of all, the OECD has been working for some time already on a common proposal to introduce a form of minimum tax in the digital economy [Englisch J., Becker J., 2019]: according to this project, the source state, in the event that the state of residence of the company does not, for some reason, levy taxes on the income it produces, would be entitled to intervene by levying a tax to attain the specified minimum level. The work of Pillar II of the BEPS project (also known as the global anti-base erosion or GLOBE proposal), which aims at introducing a minimum level of taxation on the profits of multinational enterprises [Pistone P., Nogueira J., Andrade B., Turina A., 2020], is proceeding slowly, yet the approach seems to be acceptable and could therefore be extended to the robotization of industry. One could specify, for example, that exceeding a certain level of automated production (measured by the degree of replacement of human workers by robots) should in any case lead to a greater imposition in the state where this phenomenon occurs or, failing that, in the states of the outlet markets for finished products.

The proposal of introducing a minimum level of taxation to be applied alternately in states that show the political will to impose the new rule would have the effect of underlining the solidarity function of taxation as an instrument of par-

ticipating in public expenditures for the benefit of all affiliates, including the less prosperous. It would not, in short, be a sanction against entrepreneurial phenomena that are lawful and positive. The tax would, instead, serve to redistribute wealth not only within a single system (which is the function of taxation in state systems) but also in a supranational context. Here, the now irreversible interrelation between states, regional authorities and the international community requires the pursuit of broader redistributive tax justice that would fill the gaps not only between classes but also between different states [Essers P., 2014: 54 ff]; [Hongler P., 2019].

This perspective has very broad implications that can only be hinted at here. The current emergency caused by the coronavirus demonstrates the interdependence, for better or for worse, of states that are part of the globalised world; the decisive importance of technological evolution; and thus the need for fiscal justice to apply to those economic operators that are most advantaged by progress in order to provide states and international bodies (in particular, the EU) with the resources to intervene in urgent cases to protect the most vulnerable parts of the population.

There are many difficulties involved in achieving such an arrangement. The greatest problem is that decision-making power remains in the hands of states, which are driven to take unilateral and therefore uncoordinated measures. The latter not only risk being ineffective but can also trigger conflicts of a wider scope, as demonstrated by the reaction of the United States to the introduction of a digital tax by the French Parliament. This rigidity should not weaken efforts, however. The doctrine must propose solutions that may not be realizable today on account of historical and political contingencies. In this context (and in the context of the broad debate that has developed in recent years at a philosophical rather than a juridical level [Koche R., 2019: 41 ff.]), the re-evaluation of the solidaristic function of taxation beyond the borders of any individual legal system appears to be a fundamental key to interpreting the new phenomena [Koche R., 2019]. It would help to justify both the greater burden imposed on companies operating in high-tech sectors and the need for the results of this imposition to be shared in a supranational perspective.

12. Algorithms, computability and the future of law

As much as the other themes considered earlier, decisions are a key theme with which contemporary law must deal. We take decisions all the time, and we do so more and more often, relying on the support provided by new technologies at several different levels. In politics, the very role of parliament is being replaced by forms of digital democracy that completely overturn the modern concept of democracy. Obviously, many ethical questions are involved: new technologies are changing ethical problems, on the one hand, and we are beginning to see the problem of entrusting certain automatic decisions to machines, on the other. The world

economy is increasingly controlled by algorithms, and global stock exchanges are operating at the speed of light. There are digital platforms based on machine learning systems that can propose an ideal partner by examining affinities, desires, and many other parameters that we are not even able to control. Every time we buy a book or anything else online, profiling systems suggest other goods to buy. If you liked this one, then you might also like another. In short, we increasingly make decisions at the suggestion of machines.

Are these decisions carefully considered, however? Clearly, the main problem for us here is that of the legally relevant decision. For a jurist, the decision *par excellence* is the court judgment. We increasingly speak about technologies applied to the work of judges and courts [Sartor G., Branting K., 1998: 216]. Digital evidence is a highly debated topic today, all the more so as a whole range of instruments is applied to legal procedure. However, the problem that interests us here is more specific: the algorithmic decision [Barfield W., 2020].

The spectre of the robot-judge is haunting law today. An automatic judge is a nightmare for some. The prospect of machines working alongside humans generates the fear that the former may replace the latter [Pasquale F., 2020]. An automatic judge is frightening, because judging must also involve listening. The judgment is a place where general and abstract law comes to terms with the embodied reality of society. In judges, we also look for the humanity of this reality, which is always particular and concrete, while machines are seen as lacking all passions and emotions. However, even if this were true, our tradition also includes the ideal of an impassionate judge.

We firmly believe that algorithms are *not* good or bad, right or wrong: it is the *application* of algorithms that is good or bad, right or wrong. Law cannot pass by the opportunities that such an instrument offers, yet it should not suffer its adverse effects, either. Law must govern technology [Wischmeyer T., Rademacher T., 2020], striking a balance between synthetic and human, impartiality and emotivity, the law of silicon and the law of flesh. Law must remain human, precisely because it is artificial in the sense indicated above.

Law is not only a set of public norms. The cognitive heritage of a legal system is not only formal, i.e., computable, but also heuristic, i.e., based on experience and practical observations. The result is that law does not offer any mathematically calculable solutions. Law is not fully computable.

It is obvious that law is undergoing a great evolution. One thousand years ago, custom was the quasi-exclusive source of law. Law was *jurisprudential*, i.e., made by experts. With the modern state, law has become (predominantly, if not exclusively) an expression of the will of the legislator. Today, we are faced with something

totally different once again. It is unlikely that law will be entirely produced by machines in the near future. It is too early for dystopian visions. The most likely scenario is that something hybrid will arise [Hildebrandt M., Gaakeer A., 2015].

Information technologies are inevitably presenting problems in every field of knowledge. We agree with those who say that our time will be remembered as a revolutionary era that upset previous social, economic, political, cultural and even mental models. Just as writing and printing before, digitization opens up hitherto unimaginable possibilities as well as posing problems that need to be addressed. The resulting social transformations are still in the making, of course. Nevertheless, this process has already led to disruptions that are visible to everyone. If legal science wants to maintain contact with society (and reality), it cannot disregard the new technologies.

Knowing the methods and techniques of information technology is a prerequisite for understanding the functioning of information society, including its legal aspects. This is a complicated task insofar as it requires jurists to tackle problems that go beyond traditional legal issues. It is also a challenge that compels jurists to engage on two fronts at once.

On the one hand, the question of how information technology can contribute to solving the practical and theoretical problems of legal science remains open. On the other, there exists the problem of constantly renewing classical legal disciplines in the face of the remarkable changes that the ICT revolution is producing in society [Galloway K. et al, 2019: 27–45].

The jurist should face the new challenges of today without fear and without nostalgia. To this end, he must consent to the necessary dialogue between jurists of different backgrounds, between jurists and non-jurists, and between jurists and society.

Let us therefore continue to teach about larceny while also helping students to understand how phishing is handled in criminal cases in our legal system. We must emphasize the unchanging value of the definition of usufruct in the *Corpus juris civilis* while also reflecting about the legal responsibilities of Internet service providers. We should not throw away the voluminous tomes of the *Pandectæ*, yet we should not keep them as a yoke on our shoulders, either. Let us climb upon them to look further into the distance.

References

Accoto C. (2019) *In Data Time and Tide.* Milano: BUP, 156 p.

Acquisti A., Brandimarte L., Loewenstein G. (2015) Privacy and human behavior in the age of information. *Science*, no 347, pp. 509–514.

Alpa G. (2017) *Giuristi e interpretazione. Il ruolo del diritto nella società post-moderna*. Genoa: Marietti, 340 p.

Andenas M., Deipenbrock G. (2016) More Risks than Achievements? In: *Regulating and Supervising European Financial Markets*. Cham: Springer, 437 p.

Andrews L. (2019a) Algorithms, regulation, and governance readiness. In: Yeung K., Lodge M. (eds.) *Algorithmic Regulation.* Oxford: Oxford University Press, 304 p.

Andrews L. (2019b). Public administration, public leadership and construction of public value in the age of algorithm and big data. *Public Administration*, no 2, pp. 296–310.

Ashley K. (2019) *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age*. Cambridge: Cambridge University Press, 446 p.

Austin J. (1962) *How to Do Things with Words: The William James Lectures Delivered in Harvard University in 1955*. Oxford: Clarendon Press, 167 p.

Avi-Yonah R. (2015) A Perspective of Supra-Nationality in Tax Law. In: Brauner Y., Pistone P. (eds.). *BRICS and the Emergence of International Tax Coordination*. Amsterdam: University Press, pp. 33 ff.

Barfield W., Pagallo U. (2018) *Research Handbook on the Law of Artificial Intelligence*. Cheltenham: Edward Elgar, 736 p.

Barfield W. (2020) *The Cambridge Handbook of the Law of Algorithms.* Cambridge: University Press, 809 p.

Bauman Z. (2006) *Liquid Modernity*. Malden (MA.): Polity Press, 228 p.

Benkler Y. (2011) Networks of Power, Degrees of Freedom. *International Journal of Communication*, no 5, p. 39.

Bentham J. (1995) *The Panopticom Writings*. London: Verso, 82 p.

Berring R. (1986) Full-text Databases and Legal Research: Backing into the Future. *High Technology Law Journal*, no 1, pp. 27 ff.

Bodei R. (2019) *Dominio e sottomissione. Schiavi, animali, macchine, Intelligenza Artificiale*. Bologna: Mulino, 407 p.

Brauner Y. (2014) What the BEPS. *Florida Tax Review*, 2014, pp. 98 ff.

Brauner Y. (2018) Taxing digital economy post-BEPS seriously. *Intertax*, pp. 462 ff.

Brownsword R. (2019) *Law, Technology and Society: Reimagining the Regulatory Environment*. N.Y.: Routledge, 361 p.

Brownsword R. (2020) *Law 3.0: Rules, Regulation and Technology*. N.Y.: Routledge, 136 p.

Bygrave L. (2014) *Data Privacy Law: An International Perspective*. Oxford: University Press, 233 p.

Christian B., Griffiths T. (2016) *Algorithms to Live By*. Croydon: HarperCollins, 368 p.

Cipollina S. (2014) I redditi 'nomadi' delle società multinazionali nell'economia globalizzata. *Rivista di diritto finanziario e scienza delle finanze*, no 1, pp. 21 ff.

Cipollina S. (2015) Profili evolutivi della CFC Legislation: dalle origini all'economia digitale. *Rivista di diritto finanziario e scienza delle finanze*, no 1, pp. 356 ff.

Cohen J. (2016) Between truth and power. In: Hildebrand M., van der Berg B. (eds.). *Information, Freedom and Property*. N.Y.: Routledge.

Corrales M., Fenwick M., Forgó N. (2018) *Robotics, AI and the Future of Law*. Singapore: Springer, 237 p.

Deakin S., Markou C. (2020) *Is Law Computable? Critical Perspectives on Law and Artificial Intelligence*. Oxford: Hart, 30 p.

De Filippi P., Hassan S. (2016) Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code. *First Monday*, no 12, pp. 3 ff.

De Gregorio G. (2018) From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society. *Eur. J. Legal Stud.*, no 11, p. 65.

De Wilde M. (2015) Tax Jurisdiction in a Digitalizing Economy: Why 'Online Profits' Are So Hard to Pin Down. *Intertax*, pp. 796 ff.

Dietsch P., Rixen T. (2014) Redistribution, Globalisation, and Multi-Level Governance. Available at: https://ssrn.com/abstract=2502523 (accessed: 22.01.2020)

Doucek P., Pavlicek A., Luc L. (2017) Internet of Things or Surveillance of Things? In: Research and Practical Issues of Enterprise Information Systems. Shanghai: Springer, pp. 45–55.

English J., Becker J. (2019) International Effective Minimum Taxation — The GLOBE Proposal. Available at: https://ssrn.com/abstract=3370532 (accessed: 22.01.2020)

Enriques L. (2009) Regulators' Response to the Current Crisis and Upcoming Reregulation of Financial Markets: One Reluctant Regulator's View. *University of Pennsylvania Journal of International Law*, no 4, pp. 1147 ff.

Essers P. (2014) International Tax Justice between Machiavelli and Habermas. *Bulletin for International Taxation*, pp. 54 ff.

Falcão T. (2018) Should My Dishwasher Pay a Robot Tax? *Tax Notes International*, pp. 1273 ff.

Gallo F. (1998) Ratio e struttura dell'IRAP. *Rassegna tributaria*, pp. 636 ff.

Galloway K. et al (2019) The legal academy's engagements with LawTech: technology narratives and archetypes as drivers of change. *Law, Technology and Humans,* no 1, pp. 27–45.

Gambetta D. (2018) *Datacrazia: politica, cultura algoritmica e conflitti al tempo dei big data*. Ladispoli: D editore.

Garcia Antòn R. (2016) The 21stCentury Multilateralism in International Taxation: The Emperor's New Clothes? *World Tax Journal*, pp. 148 ff.

Greenwald G. (2014) *No Place to Hide: Edward Snowden, NSA, and US Surveillance State*. New York: Macmillan, 260 p.

Grossi P. (2010) *A History of European Law*. Chichester: Wiley-Blackwell, 224 p.

Grossi P. (2014) Sulla odierna fattualità del diritto. *Giustiziacivile.com*, no 1, pp. 11–25.

Hijmans H. (2016) The European Union as Guardian of Internet Privacy: The Story of Art 16. Cham: Springer, 604 p.

Hildebrandt M., Gaakeer A. (2015) *Human Law and Computer Law: Comparative Perspectives*. Berlin: Springer, 604 p.

Hill K. (2020) The secretive company that might end privacy as we know it. Available at: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-face-recognition.html. (accessed: 28.10.2020)

Hongler P. (2019) *Justice in International Tax Law*. Amsterdam: Benjamin, 608 p.

Joe C. (2020) China has launched an app so people can check their risk of catching the coronavirus. Available at: https://www.technologyreview.com/f/615175/china-has-launched-an-app-so-people-can-check-their-risk-of-catching-the-coronavirus/ (accessed: 28.10.2020)

Joerges B. (1999) Do Politics Have Artefacts? *Social Studies of Science*, no 3, p. 428.

Kelsen H. (1967) *Pure Theory of Law.* Berkeley: University of California Press, 356 p.

Koche R. (2019) Fiscalità e globalizzazione: pensare il diritto tributario in un quadro filosofico-giuridico transnazionale? *L'altro diritto rivista*, no 1, pp. 41 ff.

Kurzweil R. (2004) The law of accelerating returns. In: Teuscher C. (ed.) *Alan Turing: Life and Legacy of a Great Thinker*. Berlin-Heidelberg: Springer, pp. 381–416.

Lesage D., Vermeiren M. (2011) Neo-liberalism at a Time of Crisis: The Case of Taxation. *European Review*, issue 1, pp. 43 ff.

Lessig L. (1999) *Code and Other Laws of Cyberspace.* N.Y.: Basic Books, p. 123.

Lessig L. (2000) Code is Law. *Harvard Magazine*, p. 1.

Lessig L. (2006) *Code. Version 2.0*. N.Y.: Basic Books, 416 p.

Lyon D. (2001) *Surveillance Society: Monitoring Everyday Life.* Philadelphia: Open University Press, 189 p.

Lyon D. (2003) *Surveillance after September 11*. New York: Polity, 208 p.

Lyon D. (2018) *Culture of Surveillance: Watching as a Way of Life*. Cambridge: Wiley, 172 p.

Malone G. (2008) From the Positive to the Regulatory State: Causes and Consequences of Changes in the Mode of Governance. *Journal of Public Policy*, issue 2, p. 139.

Marsch N. (2020) Artificial Intelligence and the Fundamental Right to Data Protection: Opening the Door for Technological Innovation and Innovative Protection. In: Wischmeyer T., Rademacher T. (eds.) *Regulating Artificial Intelligence*. Cham: Springer, pp. 33–52.

Mengoni L. (1996) *Ermeneutica e dogmatica giuridica*. Milano: Giuffré, pp. 103–114.

Mozur P. (2018) Genocide Incited on Facebook, With Posts from Myanmar's Military. Available at: https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html (accessed: 23.11.2019)

O'Flaherty K. (2020) Clearview AI's database has amassed 3 billion photos. If you want yours deleted, you have to opt out. Available at: https://www.forbes.com/sites/kateoflahertyuk/2020/01/26/clearview-ais-database-has-amassed-3-billion-photos-this-is-how-if-you-want-yours-deleted-you-have-to-opt-out (accessed: 28.10.2020)

Pagallo U. (2013) *The Laws of Robots: Crimes, Contracts, and Torts*. Dordrecht: Springer, 200 p.

Pasquale F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press, 320 p.

Pasquale F. (2020) *New Laws of Robotics: Defending Human Expertise in the Age of AI*. Cambridge: Harvard University Press, 352 p.

Pinto R. (2019) Digital Sovereignty or Digital Colonialism? Available at: https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism/ (accessed: 16.09. 2020)

Pistone P. (2014) Coordinating Action of Regional and Global Players during the Shift from Bilateralism to Multilateralism in International Tax Law. *World Tax Journal*, no 4, pp. 3 ff.

Pistone P. (2016) La pianificazione fiscale aggressiva e le categorie concettuali del diritto tributario globale. *Rivista Trimestrale di Diritto Tributario*, p. 395 ff.

Pistone P., Nogieira J., Andrade B., Turina A. (2020) The OECD Public Consultation Document 'Global Anti-Base Erosion (GloBE) Proposal' — Pillar Two. *Bulletin for International Taxation*.

Pratt G. (2015) Is a Cambrian explosion coming for robotics? *Journal of Economic Perspectives*, no 3, pp. 51-60.

Reidenberg J. (1998) Lex Informatica: The Formulation of Information Policy Rules through Technology. *Texas Law Review*, no 3, p. 553.

Reidenberg J. (2014) Data surveillance state in the United States and Europe. *Wake Forest Law Review*, vol. 49, p. 583.

Richards N. (2015) *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*. New York: Oxford University Press, 170 p.

Rifkin J. (2014) *The Zero Marginal Cost Society: Internet of Things, Collaborative Commons, and Eclipse of Capitalism*. New York: St. Martin's Press, 280 p.

Rosenblum D., Noked N., Helal M. (2014) The Unruly World of Tax: A Proposal for an International Tax Cooperation Forum. *Rivista trimestrale di diritto tributario*, pp. 183 ff.

Ruffolo U. (2017) *Intelligenza artificiale e responsabilità*. Milano: Giuffré, 148 p.

Sacchetto C., Pezzini B. (eds.) (2005) *Il dovere di solidarietà*. Milano: BUP, 217 p.

Sartor G., Branting K. (1998) *Judicial Applications of Artificial Intelligence.* Dordrecht: Springer, 222 p.

Schiavone A. (2005) *Ius: L'invenzione del diritto in Occidente*. Turin: Einaudi, 529 p.

Schneier B. (2015) *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. N.Y.: Norton, 448 p.

Schuba T. (2020) CPD using controversial face recognition program that scans billions of photos from Facebook, other sites. Available at: https://chicago.suntimes.com/crime/2020/1/29/21080729/clearview-ai-face-recognition-chicago-police-cpd. (accessed: 16.08.2020)

Semeraro M. (2012) «Regolazione» del «mercato»: relazioni semantiche e scelte di sistema (spunti dalla casistica). *Rass. dir. civ.*, pp. 808 ff.

Simoncini A. (2020) Il diritto alla tecnologia e le nuove diseguaglianze. In: Marini F., Scaccia G. (eds.) *Emergenza Covid-19 e ordinamento costituzionale*. Turin: Giappichelli, 320 p.

Sirena P. (2014) L'europeizzazione degli ordinamenti giuridici e la nuova struttura del diritto privato. *Osserv. del dir. civ. e comm.*, pp. 3 ff.

Stewart M. (2012) Transnational Tax Information Exchange Networks: Steps towards a Globalized, Legitimate Tax Administration. *World Tax Journal*, pp. 152 ff.

Stolfi E. (2020) *La cultura giuridica dell'antica Grecia: Legge, politica, giustizia*, Rome: Carocci, 284 p.

Tincani P. (2015) Controllo e sorveglianza. In: Brighi R., Zullo S. (eds.) *Filosofia del diritto e nuove tecnologie*. Rome: Aracne, pp. 72–87.

Turner J. (2019) *Robot Rules: Regulating Artificial Intelligence*. Cham: Palgrave Macmillan, 400 p.

Van Dijck J. (2014) Datafication, dataism and dataveillance: big data between scientific paradigm and ideology. *Surveillance Society*, no 2, pp. 197–208.

Varoufakis Y. (2017) Taxing robots won't work. Available at: www.weforum.org. (accessed: 12.06.2019)

Waterman D., Paul R., Peterson R. (1986) Expert Systems for Legal Decision-Making. *Expert Systems*, no 3, pp. 212 ff.

Weinstein N. (1980) Unrealistic optimism about future life events. *Journal of Personality and Social Psychology*, no 5, pp. 806–820.

Winner L. (1980) Do artefacts have politics? *Daedalus*, pp. 121 ff.

Wischmeyer T., Rademacher T. (eds.) (2020) *Regulating Artificial Intelligence.* Cham: Springer, 391 p.

Yeung K. (2018) Algorithmic regulation: a critical interrogation. *Regulation Governance*, no 4, pp. 505–523.

Yeung K. (2010) The Regulatory State. In: *Oxford Handbook of Regulation*. R. Baldwin, M. Cave, M. Lodge (eds.). Oxford: Oxford Handbooks, 211 p.

Yeung K., Lodge M. (eds.) (2019*) The Algorithmic Regulation.* Oxford: OUP, 304 p.

Zocco-Rosa A. (1914) *La figura di Appio Claudio nella storia dell'"Jus Flavianum"*. Catania: Instituto di storia del diritto romano.

Zuboff S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. N.Y.: Public Affairs, 717 p.

2020 Post-Crisis Development and 2021 Trends in Russia and Europe: Fintech and Digital Assets Regulation

Maria Agranovskaya

Attorney at Law, Managing Partner, GRAD Legal & Financial Advisory Services. Address: 33/2, bld. 1, Baumanskaya Str., Moscow 105005, Russian Federation. E-mail: office@agranovskaya.com

David Kitsmarishvili

Attorney at Law, GRAD Legal & Financial Advisory Services. Address: 33/2, bld. 1, Baumanskaya Str., Moscow 105005, Russian Federation. E-mail: kic-david@mail.ru

Abstract

The article examines 2020 post-crisis results and 2021 trends in FinTech regulation development. FinTech companies are entering the financial market in collaboration — or competition — with classic players. These new alliances are transforming the market. Speed and cost savings have been decisive, and DeFi applications, new digital banks and the digitization of assets are rapidly evolving. Innovation needs regulatory updates to be legitimate. The most revolutionary developments have appeared in smaller European countries, which the leaders are forced to follow. Law harmonization has become a natural step forward for Europe to regulate blockchain businesses and to agree on terminology and risk prevention measures for innovation support. Talks on MiCA regulations have begun. On account of anti-laundering and terrorism prevention rules for businesses, confidentiality has virtually ceased to exist in the blockchain space, which had previously been anonymous. The commercial turnover of big data and the use of artificial intelligence in financial services have led to problems in customer protection and privacy. Technology standards are also a key area of regulation. New types of stablecoins are playing important role in technology-based markets (from Tether to the Binance USD). Libra as a potential supranational currency is awaiting regulation in Switzerland yet meeting with resistance internationally. Finally, central banks in Sweden, China, Russia and other countries are introducing digital currencies. Changes have been accelerating on account of the crisis and pandemic, as potential solutions are appearing in the regulated classic financial market. Authors address the pros and cons of technology regulation and make a comparative analysis of the leading trends.

Keywords

FinTech; financial sector regulation; banking license; blockchain; crypto; digital assets; stablecoins; DeFi; neobanks; central bank digital currencies.

Acknowledgements: The authors are grateful to our former colleague Olga Antonova for her help and valuable comments on several parts of the article.

For citation: Agranovskaya M., Kitsmarishvili D. (2020) 2020 Post-Crisis Development and 2021 trends in Russia and Europe: Fintech and Digital Assets Regulation // *Legal Issues in the Digital Age,* no 3, pp. 35–58.

DOI: 10.17323/2713-2749.2020.3.35.58

Introduction

Despite its recent appearance, FinTech has already become a major industry that combines rapidly developing technologies (digital solutions, blockchain, artificial intelligence (AI) and machine learning, Internet of things (IoT), big data, etc.) with financial products and services. This has led to the emergence of new terms and concepts such as DeFi (decentralized finance).

The experience of the 2008 crisis is important to analyse the current 2020 situation and crisis outcomes. It helps to understand present-day issues and predict future trends. The year 2008 apparently gave rise to new FinTech projects and initiatives for the innovation and renewal of banking, insurance, payment systems, lending and other financial areas [Arner D. et al, 2020: 4].

The period 2020–2021 will be even more significant in our opinion. The world has changed, and technology solutions have become vital for financial players to survive and remain competitive.

Today, most countries are keen to regulate FinTech and support innovation. The adoption of new regulations has accelerated on account of the social and economic impacts of the financial crisis [e.g., Fenwick M., Uytsel S., Ying B. et al, 2020: 31]. The challenges of the future post-crisis FinTech industry will require even greater reorganization and re-evaluation of standard approaches on the part of regulators and legislators, as well as far-going international law harmonization and collaboration at different levels (between governments, regulators and cross-border associations such as R3 for legal initiative proposals)[1].

The pandemic outburst has proven the importance of new mechanisms for technology implementation and of common international standards and rules of the game that have yet to be elaborated. In this article, we focus on several FinTech areas that could be the drivers of the post-crisis revival and on recent trends in regulation updates and related problems as well as analysing some approaches taken in Russia and other countries, including EU member states.

[1] R3 is the Association of Business Recovery Professionals. Available at: https://www.r3.org.uk/ (accessed: 25.11.2020)

A retrospective review of previous post-crisis measures is useful for understanding the efficiency of the new measures to be taken. A cross-jurisdictional comparative analysis should help to uncover the best solutions in specific FinTech areas and mechanisms for the general development of the economy such as sandboxes and experimental legal regimes [Allen H., 2020: 30]. Such work may assist in the unification and harmonization of international approaches and the identification of best practices and common standards for financial technology regulation that can open a new era in FinTech [Arner D. et al, 2016: 44]. While Professor Arner and his colleagues believed that the time has not yet come to move to internationally standardized regulatory approaches in FinTech, governments can no longer put off this issue today.

Russia has declared the national importance of FinTech and the digitization of the economy. The National Digital Economy Programme reflects this development priority[2]. Nevertheless, the nascent crisis has already had a serious impact on these plans. The state budget for new technology projects is being cut, and resources are being redistributed to healthcare and the support of the most affected businesses[3]. Nevertheless, there remains an acute need for upgrading the legal framework; this work is continuing and will be even more important for economic recovery — in this regard, we support the view expressed in Pulse of FinTech by KPMG [Pollari I., Ruddenklau A. et al, 2020: 8]. Compared to Russia, such European countries as Switzerland, Liechtenstein, Malta, have proven more efficient in FinTech regulation.

The regulatory and supervisory authorities in the aforementioned jurisdictions have adopted regulations providing special legal regimes and sandboxes for FinTech firms and even new FinTech licenses for legal operation. The issue of FinTech licenses and the inevitable competition between classic financial (credit) institutions and new FinTech firms will be discussed in more detail below.

Despite the current crisis, the year 2021 looks promising in the domain of understanding and regulating products and services based on distributed ledger technologies (DLT) and integrating other technological solutions into FinTech regulation.

1. Major Trends

The following trends should appear in 2021:

Globalization & harmonization — the development of crypto-related regulations and laws will continue, and the number of progress-oriented countries will

[2] The National Digital Economy Programme of the Russian Federation was adopted on July 4, 2019. The Programme includes the current normative regulation of the digital industry. Available at: URL: https://digital.gov.ru/ru/activity/directions/858/ (accessed: 25.11.2020)

[3] For more details, see, for example, Government Order no. 1006-p of April 13, 2020. Available at: URL: http://publication.pravo.gov.ru/Document/View/0001202004140032 (accessed: 25.11.2020)

grow. This will most likely lead to the need for the harmonized regulation of the FinTech area, especially in such economic and political unions as the European Union (EU) and the Eurasian Economic Union (EAEU). On September 24, 2020, the European Commission (EC) adopted a new Digital Finance Package that will transform the European economy in the decades to come. The package aims to improve the competitiveness of the continent's FinTech sector and technologies, while mitigating risks and ensuring financial stability.

The new regulatory framework includes a novel regulation — Markets in Crypto Assets (MiCA)[4]. This regulation should ensure the support of innovative projects, a unified regulatory approach to different kinds of virtual assets, the regulation of specific activities within the EU, and the delineation from the regulation of securities and financial markets and electronic payments. General customer and investor protection rules should still apply.

At the same time, some proposals have been discussed in the global context. For example, the International Monetary Fund (IMF) has published several policy papers. IMF specialists agree that technology is changing the landscape of the financial sector, increasing access to financial services... and these changes have been in motion for several years, affecting nearly all countries in the world"[5].

Nevertheless, the development of global policies on FinTech-related issues will not be driven by the IMF. The key role shall continue to be played by standard-setting bodies such as the Group of Seven (G7), the Group of Twenty (G20) and the Financial Stability Board (FSB). The FSB defines FinTech as technologically enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services[6]. In addition, the recommendations of FSB specialists state that different crypto assets definitely have the potential to enhance the efficiency of the provision of financial services, but may also generate risks to financial stability, particularly if they are adopted at a significant scale… while such financial stability risks are currently limited by the relatively small scale of these arrangements, this could change in the future"[7]. Generally, their recommendations call for regulation, supervision and oversight that would be proportional to the potential risks. These risks may relate to chal-

[4] Regulation of the European Parliament and of the Council on Markets in Cryptoassets (MiCA) Proposal. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A52020PC0593 (accessed: 26.11.2020)

[5] Sahay R., Beaton K. et al (2020) The Promise of FinTech: Financial Inclusion in the Post-COVID-19 Era. IMF Departmental Paper No. 20/09, p. 11.

[6] Available at: https://www.fsb.org/work-of-the-fsb/policy-development/additional-policy-areas/monitoring-of-fintech/ (accessed: 26.11.2020)

[7] FSB. Final Report and High-Level Recommendations 2020 P.1. Available at: https://www.fsb.org/wp-content/uploads/P131020-3.pdf (accessed: 27.11.2020)

lenges to financial stability; consumer and investor protection; data privacy and protection; financial integrity, including compliance with rules governing anti-money laundering and countering the financing of terrorism and proliferation (AML/CFT); tax evasion; fair competition and antitrust policy; market integrity; sound and efficient governance; cyber security and other operational risks; as well as the safety, efficiency and integrity of financial market infrastructures (FMIs) (e.g., payment systems); and resolution and recovery considerations[8].

The FSB has agreed to the following actions as key building blocks of the roadmap to enhance cross-border payments commissioned by the G20:

First of all, the completion of international standard-setting work by December 2021. These standards should become guiding principles for further cooperation.

Second, the establishment or adjustment of cooperation arrangements among authorities by December 2021 (and subsequently as needed based on market evolution).

Third, at the national level, the establishment and/or adjustment of regulatory, supervisory and oversight frameworks consistent with FSB recommendations and international standards and guidance by July 2022.

Finally, the review of implementation and the assessment of the need to refine or adapt international standards by July 2023[9].

The Financial Action Task Force (FATF) has expanded the aforementioned FSB findings in the FATF report to the G20 on stablecoins. The FATF has found that crypto assets (in particular, stablecoins) share many of the same potential money laundering and terrorist financing risks as some virtual assets in virtue of their potential for anonymity, global reach and layering of illicit funds[10].

1.1. Development of Regional Regulations

Local regulations have become a leverage and investment-promotion instrument for some countries, e.g., in the domain of blockchain. Smaller European countries have been more active and successful in improving their legal frameworks to support innovation. The introduction of new legislation for supporting innovations that trigger economic development and attract investments has become popular worldwide. Some offshore jurisdictions (such as the Cayman Is-

[8] Ibid. P. 7.

[9] Available at: https://www.fsb.org/work-of-the-fsb/policy-development/additional-policy-areas/monitoring-of-fintech/ (accessed: 26.11.2020)

[10] FATF (2020), Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins. P.32. Available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf (accessed: 26.11.2020)

lands, BVI, Bermuda, etc.) and post-Soviet countries have begun to regulate crypto and digital assets [Ward M. et al 2020: 39][11].

Technology development — the interest of different governments in FinTech is driven by the growing potential of technologies.

Technological giants such as Alibaba, Alphabet, Apple and Tencent focus on FinTech projects, especially in developing markets — whether directly or by forging investments. Not only Big Tech companies but even FinTech startups invest in other emerging firms in order to augment their capabilities, get access to talent more quickly, and grow. This area is interesting for governments, as it includes the development of artificial intelligence (AI) that can be used by government bodies in different sectors, including the financial domain.

In Russia, for example, the use of robots and AI in financial services (legitimate sources of information, its status, cybersecurity, know your customer/anti-money laundering (KYC/AML), algorithmic trade, the use of bots, sources of information for AI, etc.) has become the subject of regulators' attention following Presidential Decree no. 490 On the Development of Artificial Intelligence in the Russian Federation of October 10, 2019 (the AI Decree together with the National Strategy of AI Development for the Period until 2030)[12]. A new experimental regime was launched in Moscow in 2020 as the specific legal regime for AI-related projects. In this area, not much has been done in the domain of regulation so far, yet the latter has been clearly declared the top priority.

In addition to innovation potential, such aspects of progress as the human factor, privacy and the elaboration of standards for drones and robots should not be overlooked. Here we should note the legislative initiatives of some leading market players (Media Communication Alliance, FinTech Association), including a Data Ethics Code, which should serve as the regulatory foundation for big data. A draft version of the Unified Information Code is still being reviewed. It should systemize legislative acts in the areas of telecom and information and integrate different acts on information, information technology, data protection and other issues. An important new document has finally been enacted: Federal Law № 258-FZ On Experimental Legal Regimes in the Digital Innovation Field in the Russian Federation of August 31, 2020 ("ELR Law") that will come into force on January 28, 2021.

Digital technology projects in the financial industry should be managed by the Central Bank and may become the subject of a separate regulatory regime. This is a long-awaited act. Sandboxes and experimental regimes — banks in different jurisdictions (including Russia) are highly active in new technology implementa-

[11] Russia, Belarus, the Ukraine and some other post-Soviet countries are currently working on the development of FinTech regulations (e.g., the Russian Central Bank and the National Bank of Ukraine are currently developing sovereign e-currencies).

[12] Available at: URL: http://www.kremlin.ru/acts/bank/44731 (accessed: 27.11.2020)

tion and the establishment of accelerators (e.g., Sberbank, Tinkoff, VTB). As the regulator, the Central Bank of Russia (CBR) may be rather conservative, yet it is proactive as the promoter of new technologies.

The CBR launched a sandbox in April 2018 for piloting and modelling processes for new financial services and technologies in the event that regulations need amendment[13]. In general, such sandboxes facilitate conducting risk analysis, justifying the expediency of new projects, elaborating the required regulations (if needed), and supervising projects. To address this, the special CBR Expert Market Participants Council (including technology and financial market associations) and the Interdepartmental Expert Council (government bodies) have been established. An applicant can be any entity proposing an innovative financial project. The CBR analyses the need for implementation via its council (with additional questions and technological tests). Priority is given to digital technologies. The DLT itself and the crowdfunding platforms controlled by the CBR are welcomed by the regulator, while foreign cryptocurrency and tokens issued abroad are not. The new federal law shall be another incentive for further development.

The Swiss FINMA and Singapore MAS precedents of creating new legitimate grounds and attracting investments by reviewing projects on a case-by-case basis could be much more successful for Russia than lengthy vertically governed legislative processes and their subsequent implementation, especially in view of rapidly changing technologies. The CBR is not highly active in Russia compared to regulators in Switzerland, Liechtenstein, Singapore, Malta and other countries.

Taxation of crypto assets — besides the development of AI and experimental regimes for FinTech companies, states are also interested in controlling and taxing crypto assets and crypto-related activities such as mining, payment systems, etc.

The Russian Ministry of Finance has proposed draft amendments of the Federal Tax Code for the declaration of crypto assets, yet they are far from ideal, and the understanding of the technological aspects of digital assets remains low at the level of implementing officials. Certain innovation-related tax benefits are also being discussed.

FinTech & blockchain licenses– some countries have implemented digital banking and FinTech licenses to stimulate competition and deliver services to under-served/un-served segments of the population and to support innovation. New FinTech firms and digital neobanks may now be regulated by more appropriate legislation without the burdensome rules for traditional banks. For more information on FinTech licenses, see Neobanks. New FinTech and Blockchain-Related Licenses below.

Decentralized financing (DeFi) — new decentralized applications in place of traditional financial service providers are rapidly occupying a substantial market

[13] Available at: http://old.cbr.ru/eng/fintech/regulatory-sandbox/ (accessed: 27.11.2020)

niche. The new technologies help to reduce transaction costs, facilitate the integration of decentralized platforms with each other, produce distributed trust with no single failure point, and reduce costs by the elimination of mediators. The new business models are highly competitive. Decentralized financial services may become even more decentralized, innovative, interoperable, borderless, and transparent [Chen Y., Bellavitis C., 2019: 27]; [Zetzsche D. et al 2020: 56]. Centralized DeFi players are more reliable in comparison to decentralized ones, and so the combination of efforts with regulated players allows the segment to access institutional players and become accepted. DeFi is attracting the attention of central banks and the leaders of classic finance industry. DeFi approaches are also taken into account by regulators for the sovereign issue of digital currencies that have become a hot trend in 2020.

The first steps have already been taken. On October 9, 2020, the Bank of International Settlements (BIS) together with seven central banks of different countries published the first central bank digital currency (CBDC) report laying out the key requirements[14].

The BIS Report outlines the foundation principles and core features of a CBDC. About 10% of leading central banks are ready to introduce their own digital hard currencies to replace cash.

Although many legal issues must still be cleared, the idea is already being put into practice in pilot programs in such states as Sweden and China, while Russia's Central Bank has published a report and announced public consultations[15].

Institutional players and regulated crypto services — alliances and partnerships will accelerate between Big Tech players and FinTech-oriented firms, traditional corporations and startups and even between the FinTech firms themselves; moreover, these partnerships will be highly regulated and customer-oriented. The unpacking of financial products will lose popularity as consumers increasingly seek a solution to complex and fragmented digital issues, preferring a trusted platform over an unknown application. PayPal is partnering with PAXOS to allow its clients to buy crypto (yet not to sell or trade it). Binance is issuing BUSD with NYDFS and PAXOS — its first regulated stablecoin[16].

Collaboration or competition: classic financial institutions and FinTech firms — FinTech firms and challenger banks will continue to expand the range of their service offerings beyond their initial niche area. The focus on open data

[14] The BIS Report was drafted together with the European Central Bank, the central banks of Canada, Japan, Sweden, Switzerland, and the United Kingdom, and the US Federal Reserve. For more details, see the official BIS webpage. Available at: https://www.bis.org/press/p201009.htm. (accessed: 28.11.2020)

[15] Available at: http://cbr.ru/analytics/d_ok/dig_ruble/ (accessed: 28.11.2020)

[16] Available at: https://www.paxos.com/busd/ (accessed: 28.11.2020)

opportunities will move beyond banking into other aspects of the financial service industry as well as solving common difficulties in other sectors such as power, telecommunications, etc. Deals based on FinTech will predictably be seen in jurisdictions outside of traditional markets, such as Southeast Asia, Latin America and Africa.

Confidentiality or transparency, preventing money laundering and terrorism financing vs. protecting privacy — anonymity in finances is almost non-existent, including the crypto space when it comes in touch with classic finance.

In the following sections, we will discuss in greater detail the impact of FinTech on payments, the traditional banking system, and the regulation of the financial sector as well.

1.2. Neobanks. New FinTech and Blockchain-Related Licenses

Payments are essential for the proper functioning of the economy. McKinsey estimates that global payment revenues totalled $1.9 trillion in 2018 and continued to grow in 2019 [Bruno P. et al, 2019: 2]. While banks have traditionally dominated the payments market, they are currently facing intense competition from FinTech firms, on the one hand, and sovereign states, on the other [Panzarino H. et al, 2020: 10]. In the United States, for example, technology giants such as Google, Facebook, and Microsoft have already entered the payments market. In China, mobile payments for consumption alone account for about 16% of the GDP[17]. In addition, regulations such as the Revised Directive on Payment Services (PSD 2)[18] in Europe or the Services Regulations 2017[19] in the UK have spurred FinTech to enter the sphere of payment services.

Sovereign states are also contemplating introducing digital currencies of their own. In the US, a digital dollar has been introduced three times in different bills [Hockett R., 2020: 7]. Previous bills of March 2020 suggested distributing immediate *digital cash relief* for recovery from COVID-19, but this was not approved. Instead, the aforementioned acts have proposed that digital dollar wallets should become available by the start of 2021. The bill calls for a universal basic income of

[17] BIS Annual Economic Report (2019) Big tech in finance: opportunities and risks". P. 58. Available at: https://www.bis.org/publ/arpdf/ar2019e3.pdf (accessed: 01.12.2020)

[18] The PSD 2 requires banks to provide customers' account information, upon their consent, to third-party payment providers in a standardized form. For more details, see the European Commission webpage: https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en (accessed: 01.12.2020)

[19] By adopting the Services Regulations 2017, the UK implemented the Second Electronic Money Directive and the PSD 2. Available at: http://www.legislation.gov.uk/uksi/2017/752/contents/made. (accessed: 01.12.2020)

$2,000 per month for all US citizens during the crisis and, after that, $1,000 per month for a year.

This should be financed by the issue of $2 trillion in dollar coins"[20]. Some other countries (BRICS member states, Venezuela, etc.) have also considered introducing national digital currencies [Kakushadze Z., Liew J., 2018: 4–5]. The Russian Parliament is also discussing the amendment of legislation on cryptocurrencies. On July 31, 2020, the Russian President signed a law on digital financial assets and digital currency, including amendments to certain acts (DFA Law).

Russian financial regulators have been hard at work reviewing a newly revised version of the DFA Law that would not criminalize Bitcoin or other cryptocurrencies. However, it is safe to say that the regulations on cryptocurrencies were imposed. These regulations will be discussed in more detail below.

After the financial crisis of 2008, banks were also forced to comply with Basel III[21], the Dodd-Frank Act[22], and other similar requirements, which led to increasing costs. In response to the aforementioned competition, banks are proposing different online services to their customers and trying to reduce high operational expenses for employee salaries, the lease of office space, etc. Another issue is that classic credit institutions cannot compete with startups. Slow regulatory changes and huge institutional players with internal procedures and rules are unable to regulate a promptly changing area with a lot of relatively small players. This has been an obstacle to the development and investment funding of technology and FinTech startups.

From an industry and regulatory perspective alike, one needs to take a new approach towards FinTech regulation. From this point of view, the examples of Switzerland, the UK, Liechtenstein, Gibraltar, and Malta are particularly interesting.

Singapore, known as the Asian Switzerland", is another world leader that has done a lot for harmonizing its financial regulations with Western Europe. However, a detailed analysis of its legal novelties shall be the subject of an another article (upcoming).

Gibraltar was the first jurisdiction to implement special FinTech regulatory legislation. By passing the Financial Services (Distributed Ledger Technology or DLT) Regulations 2017[23] that entered into force on January 1, 2018, the Gibraltar

[20] Available at: https://tlaib.house.gov/sites/tlaib.house.gov/files/ABCAct.pdf.(accessed: 01.12.2020). The bill was introduced on April 16, 2020.

[21] Basel III is a global regulatory framework on bank capital adequacy, liquidity risks, and stress testing. Available at: https://www.bis.org/bcbs/basel3.htm. (accessed: 01.12.2020)

[22] The Dodd-Frank Act is an integrated bill that put strict regulations on the US financial industry and created programs to stop mortgage companies and lenders from taking advantage of consumers.

[23] Available at: http://www.gfsc.gi/uploads/DLT%20regulations%20121017%20(2).pdf. (accessed: 01.12.2020)

Financial Services Commission (GFSC) became the standard-setting body licensing any person (legal entity), in or from Gibraltar, that uses DLT for storing or transmitting value belonging to others.

Liechtenstein was also among the world's first jurisdictions to pass a specialized Blockchain Act"[24]. The Blockchain Act applies to all trustworthy technologies service providers (instead of blockchain or distributed ledger technology", the term trustworthy technology or TT is used). From January 1, 2020, the following professional service providers in Liechtenstein must register with the Financial Market Authority of Liechtenstein (FMA):

Token issuers — entities publicly offering tokens[25] on behalf of third parties (e.g., a trading venue carrying out an ICO). Furthermore, persons making a private placement must also register if the value of the tokens sold in one year exceeds or shall exceed CHF 5 million.

Token generators — entities generating original tokens on behalf of third parties.

TT Key Depositaries and TT Token Depositaries — entities that safeguard tokens or private keys for third parties, e.g., in a safe or a collective wallet. This also includes the execution of transactions for third parties. These services are typically provided by crypto exchanges (such as Bittrex) and wallet providers.

Generally speaking, the law clearly specifies all the service providers that should be registered (licensed) by the Liechtenstein FMA. In addition to the aforementioned providers, they include TT Protectors and Physical Validators, TT Exchange Service Providers, TT Verifying Authorities, as well as TT Price and Identity Service Providers[26]. The Blockchain Act aims to improve investor protection, combat money laundering and establish legal certainty in regulating blockchain projects.

The Maltese legal framework governing the FinTech industry includes three main laws: the Innovative Technology Arrangements and Services Act (ITAS), the Malta Digital Innovation Authority Act (MDIA), and the Virtual Financial Assets Act (VFAA), supplemented by guidance of the Malta Financial Services Authority.

Licensing issues are regulated by the VFAA. One of the salient features determining the applicability of the VFAA is the type of asset with which the operator deals. Through the application of the Financial Instrument Test, a DLT asset (i.e.,

[24] Originally, the Token and TT-Service Provider Act (the so-called Blockchain Act") was adopted by the Liechtenstein Parliament on October 3, 2019, and entered into force on January 1, 2020. Available at: https://www.regierung.li/media/medienarchiv/950_6_04_11_2019_TVTG_english.pdf?t=1 (accessed: 01.12.2020)

[25] In the Blockchain Act (art. 2), a token stands for a piece of information on a TT System (i.e., blockchain) and for a kind of container for representing a right.

[26] For more details, see Liechtenstein's FMA. Available at: https://www.fma-li.li/en/fintech-and-tvtg.html (accessed: 02.12.2020)

a cryptocurrency) is classified as a virtual token, a financial instrument, e-money or a virtual financial asset in accordance with the VFAA. It should be said that EU directives and regulations on markets of financial instruments, e-money, and payment services, as well as anti-money laundering laws, are additionally applicable. The same holds for Gibraltar, as we mentioned earlier. The provision of the following services in or from within Malta in relation to a DLT asset which has been determined to be a virtual financial asset in terms of VFAA, requires a license:

Reception & transmission of orders: the reception from an entity of an order to buy, sell or subscribe to virtual financial assets and the transmission of that order to a third party for execution.

Execution of orders on behalf of other persons: concluding agreements on buying, selling or subscribing to one or more virtual financial assets on behalf of another entity.

Custody or nominee services: acting as a custodian or nominee holder of a virtual financial asset and/or private cryptographic key or holding a virtual financial asset and/or private cryptographic key as a nominee, where the entity acting as the nominee is doing so on behalf of another entity.

Portfolio management: managing assets (one or more virtual financial assets or arrangements) belonging to another entity with the discretion to invest any of these assets in one or more virtual financial assets.

Dealing on one's own account: trading against proprietary capital resulting in the conclusion of transactions involving one or more virtual financial assets.

Investment advice: giving, proposing or agreeing to give personal recommendations with regard to one or more transactions relating to one or more virtual financial assets to entities in their capacity as investors or potential investors or as an agent for an investor or potential investor.

Placement of virtual financial assets: marketing newly issued virtual financial assets or virtual financial assets which are already issued yet not admitted to trading on a DLT exchange to specific entities without making an offer to the public or to existing holders of the issuer's virtual financial assets.

Operations of a VFA exchange: virtual financial assets may be exchanged, which requires specific regulations.

In order to provide the above services, one needs to obtain a license. There are four types of FinTech licenses. *VFAA Class 1:* license holders are authorized to receive and transmit orders and/or provide investment advice in relation to one or more virtual financial assets and/or place virtual financial assets. Class 1 license holders are not authorized to hold or control clients' money or assets. *VFAA Class 2:* license holders are authorized to provide all VFA services and to hold or control clients' money yet not to operate as a VFA exchange or deal on their own. *VFAA Class 3:* license holders are authorized to provide all VFA services and to hold or control clients' money yet not to operate as a VFA exchange. *VFAA Class 4:*

license holders are authorized to operate as a VFA exchange, to hold or control clients' money, virtual financial assets and private cryptographic keys, and to provide custodian or nominee services solely in relation to the operation and activities of such a VFA exchange.

The Virtual Financial Assets Act sets down the application procedure and the requirements that the service providers must meet in order to receive a license, including, but not limited to, organizational requirements, financial requirements, operational requirements, and requirements relating to anti-money laundering (AML), combating the financing of terrorism (CFT), and cybersecurity[27].

The VFAA license only covers services relating to virtual financial assets. If an asset is classified as a financial instrument, then any services provided in relation thereto (including placement) would require prior authorization under the traditional financial services legislation.

The Swiss legal framework governing the activities of traditional banking (financial) services and FinTech firms consists of federal acts, implementing executive orders and a number of circulars, as well as guidance of the Financial Market Supervisory Authority (FINMA). In addition, a new FinTech license has been introduced by the recent amendments to the Banking Act 2019[28]. FinTech-related companies came into conflict with the Banking Act, as the acceptance of deposits from the public requires a banking license. As the Banking Act sets down stringent conditions for granting licenses, the banking license serves as a considerable barrier for FinTech companies that want to enter the market.

The current Swiss FinTech model provides opportunities for all market participants, whether established financial service providers or startup companies. FINMA takes an intrinsically neutral stance towards new business models and technologies and considers innovation as an important factor for the competitiveness of the Swiss financial market. At the same time, the Swiss standard-setter pays close attention to prudential and conduct supervision[29]. FINMA only supervises institutions it has authorized to engage in financial market activity. This supervisory function is prudential with respect to banks, insurance companies and other financial service providers: these institutions must always have adequate capital buffers and liquidity and should have their risk exposure under control.

Switzerland's model is based on the following core elements: a FinTech license allows non-bank companies to accept deposits from the public without conduct-

[27] Available at: https://www.mfsa.mt/fintech/virtual-financial-assets/#legislativeRegulatoryFramework. (accessed: 02.12.2020)

[28] Available at: https://www.admin.ch/opc/de/classified-compilation/19340083/index.html. (accessed: 02.12.2020)

[29] FINMA Annual Report 2019. Available at: https://www.finma.ch/en/search/ (accessed: 02.12.2020)

ing any lending operations with maturity transformation or interest payments (Art. 1b of the Banking Act 2019); the conditions to be fulfilled for obtaining a FinTech license are less stringent than for traditional banks: deposits may not exceed the value of CHF 100 million and may not be reinvested; the minimum capital shall always be three percent of the total amount of deposits held yet not less than CHF 300,000; a legal entity pursuant to Art. 1b of the Banking Act 2019 is subject to supervision by FINMA.

The aforementioned requirements allow FinTech firms to appear and compete with classic banks. As of October 26, 2020, there exists a registered entity licensed by FINMA pursuant to Art. 1b of the Banking Act 2019[30]: Yapeal AG, a neobank registered in Zurich[31]. Yapeal will offer accounts with Swiss IBAN without being tied to an offline bank payment system. Having both FINMA banking and securities dealer licenses, Sygnum and SEBA[32] banks also provide examples of how traditional and innovative banking services can be combined. These crypto banks enable professional individuals and companies as well as institutional clients to invest, safekeep, trade, and borrow against digital and traditional assets, all in one space. For Swiss blockchain companies, these banks provide accounts and custody for fiat and digital assets. In addition, they intend to issue their own digital currencies (Sygnum, for example).

The Russian FinTech market has been growing significantly over the past two years in terms of both the number of transactions and the volume of investments. The market has several particularities: Russia is a leading global supplier of IT specialists, and some areas such as P2P lending, crowd investments and cryptocurrencies have yet to be regulated. According to some FinTech companies, the key challenges facing the Russian market include the low interest of external investors, the low spending power of citizens, geopolitical risk and the inflexibility of the taxation system.

In 2018, as we mentioned above, the Russian Central Bank created a regulatory sandbox to encourage the development of new financial services and technologies such as a system of fast payments, a unified system of biometric identification, and a financial supermarket.

Accelerators such as the FRII accelerator and the HSE incubator regularly support the development of FinTech startups. FinTech partnership programs designed to help early-stage startups to meet market needs were set up back in 2018 by Sberbank, Raiffeisenbank, Tinkoff and Alfa Bank. Several banks also acquired startups in the field of loyalty and payments, including Alfa Bank (Cardsmobile)

[30] The list of persons licensed by FINMA. Available at:: https://www.finma.ch/en/search/. (accessed: 03.12.2020)

[31] Available at:: https://yapeal.ch/#intro. (accessed: 03.12.2020)

[32] Available at:: https://www.seba.swiss/ (accessed: 03.12.2020)

and Tinkoff (Cloudpayments). The UK FinTech unicorn Revolut also entered Russia in 2018 via a licensing deal with Qiwi Bank. Russia's Central Bank has launched a FinTech association and a sandbox designed to support further development.

The FinoPolis FinTech forum is also strengthening the ecosystem. Cryptocurrencies and tokens are legal yet discouraged means of payment while ICOs and crowdfunding have gained popularity as alternative sources of capital. Accelerators and incubators such as Russia FinTech Lab, Huobi, Digital Horizon and Digital October are active in the country, as are over 70 VC firms, which invested a total of over 212 million euros in 2017.

2. Blockchain Assets: New Forms

The past years have witnessed the emergence and development of the main approaches to the classification and legal qualification of digital and blockchain-based assets. Grounded in classical legal theory, new relations and forms of asset transfer have led to changes in the terminological framework. Indeed, this was the most difficult aspect of all. What is cryptocurrency? How shall it be accounted for? As money, goods, derivatives or a programme code protected by intellectual property provisions?

The clear definition and classification of blockchain-based assets is an essential condition for their proper regulation by the legal system; this is particularly important in the context of the highly regulated financial sector and DLT-based crowdfunding. The initial understanding of the term and its applications has changed not only in theoretical works but also in the practice of regulatory and supervisory bodies in different jurisdictions. We should note that the terms smart properties and smart contracts were already used by [Szabo N., 1994], which described peer-to-peer finance operations where all participants are equal (also casting the foundations for DeFi as we know it today) and specified that software should fully embed the contractual terms relating to property in the property itself. In 1998, the concept was further developed in B-money by Wei Dain, who wrote about an independent protocol whose execution would be triggered by a public cryptographic key[33].

Without a doubt, the first cryptocurrency that most people heard about was Bitcoin. Bitcoin is basically the modern version of the smart contract (just as Side Chains, NXT, Ethereum and some other cryptocurrencies) [Savelyev A. 2016: 7–10]. Bitcoins and smart contracts have certain similar features and operating principles. Apart from being a code that may be protected by intellectual property laws, Bitcoin is a separate value item *per se* that can be transferred freely, anonymously and without mediators. Some other new digital asset types not only

[33] Available at:: http://www.weidai.com/bmoney.txt. (accessed: 03.12.2020)

include unique codes but also play a role in the system, have additional functions and/or are derivatives from real assets. Many different types of new assets have appeared, and they continue to develop today.

Japan was among the first to acknowledge Bitcoin as legal tender by a special act in 2017. To keep up to date with recent progress and market changes, a new act entered into force this year as a revision of the Act on Settlement of Funds and the Financial Instruments and Exchange Act, and crypto-related regulations have been tightened. Apart from the new requirements on margin trading, crypto derivatives, risk transparency and hack prevention, the term *virtual currencies* has been replaced by *crypto assets"*.

Switzerland has been among the leaders in theory elaboration and regulatory development. The first ICO Guidance, issued in September 2017, acknowledged the impossibility of catch-all definitions. A separate warning noted that real cryptocurrencies should be stored on distributed networks and use blockchain technology"[34]. Extensive FINMA documents have been published, and the doctrine has been supported with high-quality materials, including articles by the MME Law Firm on the nature and legal essence of cryptocurrencies and tokenized assets.

The small territory of Gibraltar was the first to adopt advanced DLT-related regulations. In early 2014, a private cryptocurrency working group was launched to examine crypto matters; in early 2016, the Gibraltar government began to collaborate with it, and a discussion paper was issued[35]. Distributed ledger technology is defined in the Financial Services (Investment and Fiduciary Services) Act of 1989[36] as a database system in which (a) information is recorded and consensually shared and synchronized across a network of multiple nodes and (b) all copies of the database are regarded as equally authentic. 'Value' includes assets, holdings and other forms of ownership, rights or interests, with or without related information, such as agreements and transactions for the transfer of value or its payment, clearing or settlement." This approach was subsequently adopted by some others: defining not cryptocurrency but the technology and its manifestations and the ways how assets are used and issued. On October 12, 2017, the Financial Services (Distributed Ledger Technology Providers) Regulations 2017 were made public in accordance with the Financial Services (Investment and Fiduciary Services) Act. These regulations entered into force on January 1, 2018. Their most important effect was to convince organizations that it is good to be regulated. The rules have allowed persons who are willing to be regulated and who have stable grounds for

[34] FINMA Report 2017. Available at: https://www.finma.ch/en/news/2017/09/20170919-mm-coin-anbieter/ (accessed: 03.12.2020)

[35] Available at: http://www.fsc.gi/uploads/GoGPR12102017.pdf (accessed: 03.12.2020)

[36] Available at: http://www.gibraltarlaws.gov.gi/articles/1989-47o.pdf (accessed: 03.12.2020)

operation to get a special license. Crypto-related financial operations could now be licensed just as classic financial services. A local regulated crypto-exchange has been launched (Global Blockchain Exchange or GBX).

Malta and other countries have followed in the wake, developing their own internal legislations. It is important to emphasize that local crypto-related legislation does not apply to business development and active marketing in other countries: what is legal in one country may still be prohibited in another. This presents difficulties, in particular, for EU member states: to adopt new blockchain-related rules, they must ensure compliance with existing local laws as well as following EU directives and regulations on financial services (MIFID II), the issue of securities (Prospectus Directive), collective investment schemes (Alternative Investment Funds Directive) and other issues.

Liechtenstein's new set of rules and the comments of the Financial Markets Authority (FMA) emphasize that cryptocurrencies are private and purely virtual currencies that are usually implemented using a blockchain. Up to now, neither the production nor the use of virtual currencies as means of payment has been subject to any licensing requirements governed by specialized legislation. In individual cases, however, there may be a licensing requirement depending on the specific type of business model[37]. According to the Fact Sheet on Virtual Currencies, the latter may be commonly defined as the digital representation of a (quasi-monetary) value that is issued neither by a central bank nor by any other official authority. Obviously, they are not official currencies despite the existence of certain similarities. Risks embodied in such virtual assets are addressed by the corresponding Fact Sheet and the new legislation. Bitcoin is produced by end users themselves in a decentralized fashion using special software on a computer network. Individual Bitcoins are saved in a digital wallet and can be used as a means of payment… Every transaction carried out in Bitcoin is recorded in a centralized location on the internet (a blockchain) and is thus in principle traceable. As a rule, however, the end user remains anonymous. This extended definition reflects a change in the regulators' understanding as compared to the first official publications. Digital has replaced crypto".

The new CFA Law in Russia, entered into force on January 1, 2021, defines a digital currency as electronic data (a digital code or denomination) in an information system that are offered and/or accepted as a means of payment while not being a monetary unit of the Russian Federation, a monetary unit of a foreign country and/or an international monetary or accounting unit and/or serve as an investment, and there is no person obliged to any holder of such electronic data as such, except for the operator and/or nodes of the information system that are

[37] Available at: https://www.fma-li.li/en/financial-centre/fintech-in-liechtenstein/business-models.html (accessed: 03.12.2020)

responsible for assuring compliance with the information system rules on the issue of electronic data and performing actions for their entry into the information system or the amendment of entries"[38]. This definition is technically imperfect and uses the term information system that can generally refer to almost any database. Any bonus, electronic certificate or air miles may easily be qualified as digital currencies in the current version of the law. Previous court and supervisory practice has been very diverse and does not help to clarify the situation, either. Bitcoin and other cryptocurrencies are widely recognized as property, making it possible to protect owners' rights and use classic vindication, inheritance or transfer by contracts.

Most countries do not consider cryptocurrencies to be money", securities or commodities (with some exceptions). However, legal definitions of cryptocurrencies (as opposed to tokens, securities, money, electronic bonuses and their regimes) are often lacking. Given the transborder character of the technology, the harmonization of internationally recognized definitions and rules is essential for sector development. We are referring to upcoming major developments in this area. The most advanced example today is EU cooperation, yet it is not easy to agree upon a common set of rules for addressing such a disputable class of assets and their concomitant risks.

2.1. Tokens and Digital Assets

It would be important to address the key definitions and classification approaches to analysing regulation changes and key trends of the year 2020 that should continue in 2021. The pandemic has served as an accelerator of regulatory development in this area. Innovative digital models offering cost savings and mediator-free solutions are rapidly expanding on the financial market. This expansion requires supervisory bodies to pay attention to legitimate integration and collaboration with classic institutional players. The most advanced regulation of token classifications and of the rules relating to their issue and operations is found in Switzerland. Following the 2017 Guidance, FINMA published the ICO assets classification for added clarity in February 2018, stressing that there is no consistent doctrine or internationally recognized legal concept of cryptocurrency. FINMA categorises tokens into three main types (hybrid forms are also possible):

Payment tokens are synonymous with cryptocurrencies and have no further functions or links to other development projects. In some cases, tokens expand their functionality over time and become accepted means of payment;

Utility tokens are tokens that provide digital access to an application or service;

Asset tokens represent assets such as participation in real physical undertakings, companies or income streams or as entitlements to dividends or interest

[38] *Cf.* Clause 1, Subclause 3, of the DFA Act.

payments. In terms of economic function, asset tokens are analogous to equities, bonds and derivatives.

The classification of tokens and its legal consequences (including forms of transactions, taxation, etc.) depend on the economic function and purpose of tokens (i.e., blockchain-based units). Another important qualifying feature is tradability or transferability. A similar approach has been taken by most regulators, including FMA, FCA (UK) and others. The principal digital classifications of assets aimed to distinguish them from securities and electronic money, yet this may be no longer sufficient today.

For example, according to Swiss specialists, the absence of a precise classification leads to some degree of legal uncertainty in practice. Moreover, the qualification of tokens for decentralized, open-sourced and community-based projects, which do not need a centralized issuer, seems to be out of the scope of the FINMA model"[39]. They classify tokens on the basis of functionality, target use and the existence and type of counterparty as well as the presence of an underlying asset or value. This classification includes three kinds of tokens:

Native Utility Tokens are transferred on a decentralized ledger between users; they do not give rights to another person or provide for any right except for the right relating to the token itself (issuer or transferor).

Counterparty Token represent any relative right against a third party; such tokens give the right to receive services, assets, or corporate rights.

Ownership Tokens give technical ownership rights in assets. Their purpose is to transfer rights to assets associated with the token. They refer to IP rights and material objects; they award no claims or relative rights against a counterparty but only absolute rights (erga omnes) in the form of a right in rem of the associated assets.

In terms of obligations law, it was important to decide whether tokens result in any obligations on the part of the issuer (e.g., asset-backed tokens). This also determines whether a specific asset class is transferrable by a smart contract[40]. A code succession or algorithm may not be sufficient to comply with the existing formalities to render a transaction valid.

This is especially problematic for internationally executed contracts for digital assets transfer. In addition, not all objects may be digitalized and transferred in a purely electronic fashion, although almost everything today can have a digital Gemini or shadow in theory. It has been noted at the World Economic Forum that, by 2027, around 10% of the world's GDP will stem from blockchain-based contracts[41].

---

[39] Available at: https://www.mme.ch/de/magazin/bcp_framework_for_assessment_of_crypto_tokens/ (accessed: 04.12.2020)

[40] *Cf.* FINMA Report 2018, p. 30. Available at:: https://finma.ch/de/dokumente/ (accessed: 04.12.2020)

[41] Available at: https://www.weforum.org/reports/how-to-end-a-decade-of-lost-productivity-growth (accessed: 04.12.2020)

Another issue that may hinder the qualification and transfer of digital assets (for DeFi services, international ICOs or any other digital asset-related operation) is the absence of international and often even domestic standards and norms for the security level, software development quality, and use of cryptography (yet the latter may, in contrast, be highly regulated). This is important for the use of technologies by government bodies and the control of operations. Ethereum used to be the market leader, yet new technologies are currently supplanting it (e.g., Solidity, Fift (TON) and others)[42].

2.2. Stablecoins

The initial excitement about coins and tokens and the interest in digitizing assets was naturally fuelled by the seemingly easy access to substantial amounts of funds that could allegedly be raised out of existing regulations and control. Many entrepreneurs have tried to follow this path. Initially, this was mostly the domain of IT startups. Today, such industrial giants as Norilsk Nickel are considering asset digitization and regulated stablecoin issue. Stablecoins may be a solution to increasing liquidity or accessing new markets or groups of investors, which is becoming increasingly important nowadays.

For crypto markets, stablecoins are introducing stability and means of exchange that are reliable and accepted by all market participants.

The existence of real assets behind stablecoins is not always guaranteed, as this matter is not regulated. Nevertheless, the issue of such digital assets is one of the most actively developing trends today. The Tether cryptocurrency linked to the USD is well known and widely accepted.

In September 2020, a new asset was placed on the market by Binance, a leading regulated crypto-exchange, under the supervision of New York Department of Financial Services (NYDFS). This dollar-backed stablecoin is approved by the US regulator and issued by Binance's regulated partner PAXOS, as we mentioned above. The major public auditor Withum is supporting the currency. The issue size is $209 million, and the monthly trading volume exceeds $1 billion. This digital dollar is bought and sold 24/7, assuring rapid and inexpensive value transfers to any part of the world with guaranteed validation. Its fixed rate is 1:1. Such instruments are introducing new operating possibilities for the financial system and competing with banking services.

A different stablecoin was announced by Libra Association linked to Facebook. The disputes around this potential supra-national competitor to national currencies have been acute, and the issue's future is not fully clear yet. France and the US

[42] Available at: https://mining-cryptocurrency.ru/yazyki-programmirovaniya-dlya-blokchejna-i-smart-kontraktov/ (accessed: 04.12.2020)

are among the harshest critics of the project. The international resistance has been so serious that most institutional players (including Visa, Mastercard, and PayPal) have had to leave the association so as not to risk their licenses and positions. The Libra case has got a lot of political attention due to the enormous number of Facebook users. Switzerland has issued a detailed and well-grounded statement about Libra. In its press release of September 11, 2019[43], FINMA confirmed that the Libra Association had asked FINMA for an assessment of how it would classify the project in regulatory terms under Swiss supervisory law. FINMA wrote that a project of this kind would fall under financial market infrastructure regulations and only require a payment system license in accordance with the Financial Market Infrastructure Act (FinMIA)[44] in addition to meeting some extra requirements.

Regulatory requirements for payment systems in Switzerland are based on prevailing international standards, particularly the Principles for Financial Market Infrastructures (PFMI). Libra has filed for a license in Switzerland and established its headquarters in Geneva.

FINMA also stated in its press release that the international scope of the project required an internationally coordinated approach and that work on elaborating requirements (in particular, for combating money laundering) should be carried out internationally, too. FINMA stressed that the project's size and scale may result in additional requirements, including even a banking license. Capital allocation, reserves, risk management, liquidity and other requirements should be calculated for the Libra project based on its business plan and submitted to FINMA. Swiss blockchain experts have emphasized that existing AML, KYC and transparency requirements will be applied and that scrutiny will be particularly close given the importance of the project. In addition, FINMA has introduced a completely new stablecoin manual that applies to other players as well[45]. The manual was subsequently further extended by a Supplement to the ICO Guidelines[46].

In this domain, Russia has introduced the long-debated DFA Act, as we mentioned above. Its asset qualification is not exactly the same as described above: the Central Bank of Russia refuses to accept the use of any digital currency as a means of payment and stipulates that the Russian rouble remains the only means of this kind today [Yankovsky R.M., 2020: 3–4].

---

[43] Available at: https://finma.ch/en/news/2019/09/20190911-mm-stable-coins/ (accessed: 04.12.2020)

[44] Available at: https://www.admin.ch/opc/en/classified-compilation/20141779/index.html (accessed: 04.12.2020)

[45] Available at: https://www.mme.ch/de/magazin/finma_aeussert_sich_zu_libra/ (accessed: 04.12.2020)

[46] Available at: https://finma.ch/en/documentation/dossier/dossier-fintech/innovation-und-aufsicht-2019/ (accessed: 04.12.2020)

The CBR has recently launched the Digital Rouble project and published a report for public consultations. Bitcoins and other privately issued cryptocurrencies are not allowed to circulate freely. A draft version of the Digital Currencies Act along with amendments to the Criminal and Administrative Codes have been presented yet have not passed the first reading so far. The Ministry of Finance has also proposed amendments to the current legislation and the Russian Tax Code, yet this has not resulted in any further action so far. In contrast to digital currencies, DFAs are digital rights that include monetary claims, rights to issued securities, non-public joint stock company capital participation rights, and the right to claim the transfer of issued securities according to the DFA conflict resolution protocol as stipulated in the Act, providing that the issue, accounting, and turnover of such assets are possible only by their entry into an information system on the basis of a distributed ledger and other information systems[47]. The Central Bank will undoubtedly have to issue a series of documents to clarify the numerous questions resulting from such a definition. It is currently discussing a draft document about the right of qualified (accredited) investors to buy DFAs and about the limitations on Russian investors. The DFA Act has introduced new types of regulated players (DFA issuers and exchanges). Certain classic financial market license holders will also be allowed to act as such.

Other digital assets resembling utility tokens ("utility digital rights") are regulated by the Crowdfunding Law"[48]. They do not conform to the common European understanding of utility tokens referred to above. It should be said that Russia has chosen a regulatory approach that focuses on limiting rather than developing the market, while other countries are allowing innovative projects to enter the market on the condition of risk control, mitigation and transparency.

International harmonization is extremely important. New crypto-specific regulation called MiCA (Markets in Crypto Assets) is currently being elaborated. It will address most, if not all, crypto market regulations, except for money laundering that lies outside the MIFID II and Payments Directive. While it is difficult to believe that these rules will come into force within a year, all participants are aiming at the rapid adoption of the new standards.

Conclusion

The pandemic has served as an accelerator for regulation development in the FinTech area. Innovative digital models offering cost savings and mediator-free solutions are rapidly taking over the financial market. This expansion requires su-

[47] *Cf.* Clause 1, Subclause 2, of the DFA Act.

[48] Federal Law no. 259-FZ On investments using investment platforms and amendment of certain legal acts of the Russian Federation of August 2, 2019 // SPS Consultant Plus.

pervisory bodies to pay attention to legitimate integration and collaboration with classic institutional players. Following the introduction of new regulations, the level of trust in digital currencies and assets has risen, and new institutional players are entering the expanding crypto market. The new alliances of crypto and FinTech companies with classic market participants will allow this process to take place more efficiently.

References

Allen H. (2020) Experimental Strategies for Regulating FinTech. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3533240 (accessed: 25.11.2020)

Arner D. et al (2020) Digital Finance & the COVID-19 Crisis. University of Hong Kong. Faculty of Law. Research Paper No 2020/017. 24 p.

Arner D. et al (2016) The Evolution of FinTech: A New Post-Crisis Paradigm? University of New South Wales. Law Research Paper No. 2016-62. 45 p.

Bruno P. et al (2019) Global Payments Report 2019: Amid Sustained Growth, Accelerating Challenges Demand Bold Actions. 33 p. Available at: https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/tracking%20the%20sources%20of%20robust%20payments%20growth%20mckinsey%20global%20payments%20map/global-payments-report-2019-amid-sustained-growth-vf.ashx (accessed: 01.12.2020)

Chen Y., Bellavitis C. (2019) Decentralized Finance: Blockchain Technology and the Quest for an Open Financial System. 27 p. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3418557 (accessed: 28.11.2020)

Fenwick M., Uytsel S., Ying B. (eds.) (2020). *Regulating FinTech in Asia: Global Context, Local Perspectives*. Cham: Springer, 225 pp.

Hockett R. (2020) The Treasury Dollar: An Immediate Funding and Digital Banking Plan for Pandemic Relief and Beyond. Cornell Legal Studies Research Paper No. 20–30, pp. 1–8.

Kakushadze Z., Liew J. (2018) CryptoRuble: From Russia with Love. *World Economics*, issue 4, pp. 165–187.

Panzarino H., Hatami A. (2020) *Reinventing Banking and Finance: Frameworks to Navigate Global Fintech Innovation*. L.: Kogan and Page, 250 pp.

Pollari I., Ruddenklau A. et al (2020) Pulse of FinTech H2 2019. Available at: https://home.kpmg/xx/en/home/campaigns/2020/02/pulse-of-fintech-h2-19-top-10-predictions-for-2020.html (accessed: 25.11.2020)

Savelyev A. (2016) Contract Law 2.0: Smart contracts as the beginning of the end of classic contract law. HSE Working Papers WP BRP 71/LAW/2016, 24 p.

Szabo N. (1994) Smart Contracts. Available at: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (accessed: 03.12.2020)

Ward M. et al (2020) Blockchain and cryptocurrency regulation 2020. Available at:https://www.careyolsen.com/sites/default/files/CO_Blockchain-and-Cryptocurrency-Regulation-2020-2nd-Edition.pdf (accessed: 27.11.2020)

Zetzsche D., Arner D., Buckley R. (2020) Decentralized Finance. *Journal of Financial Regulation,* issue 2, pp. 172–203.

Yankovsky R.M. (2020) Cryptocurrency in Russian Law: surrogates, other assets and digital currency. *Legal Issues in the Digital Age,* no 1, pp. 3–31.

Crowd Arbitration: Blockchain Dispute Resolution

Aleksei Gudkov

Associate Professor, Department of Theory of Law and Interdisciplinary Studies, National Research University Higher School of Economics, PhD. Address: 20 Myasnitskaya Str., Moscow 101000, Russia. E-mail: ag2868@gmail.com

Abstract

Internet technology makes digital value transactions between anonymous individuals possible, but leaves unanswered the question of how to resolve disputes between unidentified parties. Blockchain dispute resolution platforms provide a response to this problem. In the social dispute resolution systems for blockchain currently in use, pseudo anonymous jurors can resolve disputes between pseudo anonymous parties. This paper presents Kleros as the most illustrative blockchain dispute resolution platform BDRP. To describe the features of the Kleros dispute resolution platform and the qualification of jurors, this research employs an online dispute resolution survey of both the jurors and stakeholders of the Kleros platform. This study raises important questions about key elements of procedural justice in resolution platforms for blockchain disputes. The research underlines the pros and cons of dispute resolution for crowdsourced blockchain and contributes to the further development of online dispute resolution systems. It tests the wisdom of the crowd as the core attribute of the resolution process in crowdsource disputes. Crowdsource mass dispute resolution, coupled with cooperative jurors and blockchain technology, could ensure greater effectiveness and fairness of the dispute resolution process, especially the adjudication of online small claims disputes.

Keywords

blockchain; dispute resolution; distributed arbitration; social justice; blockchain court; online justice; ODR, crowd arbitration.

For citation: Gudkov A.V. (2020) Crowd Arbitration: Blockchain Dispute Resolution // *Legal Issues in the Digital Age,* no 3, pp. 59–77.

DOI: 10.17323/2713-2749.2020.3.59.77

Introduction

Online technologies are part of everyday life. Online interactions, including online commerce, freelance activities, values exchange, transactions with cryptoassets, and the network infrastructure to support these activities are growing. The number of cross-border small trade transactions conducted online has sig-

nificantly increased as well. For example, the total number of cross-border buyers on AliExpress grew from 10 million in 2014 to 150 million in 2018[1]. Inevitably, this has triggered an increase in the number of disputes, including a clear upward trend in the number of small, cross-border disputes.

The development of blockchain technology has made it possible for anonymous persons to carry out decentralized payment settlements and has made it even more difficult to resolve disputes between persons acting online. There are social and legal ramifications, caused by market demands that change the approaches relating to the dispute resolution process. Online commerce requires that disputes be settled quickly, securely and fairly, and that they be enforceable despite problems with identification and distance. Technological progress provides an opportunity to improve the dispute resolution process. Blockchain technology is well-suited to these needs. Blockchain dispute resolution is a crowdsourced online dispute resolution system that uses blockchain technology to set up arbitration, organize dispute adjudication, and reward jurors.

This study examines the technological, social and legal solutions for dispute resolution, focusing on the adaptation of blockchain technology to the international justice system. It introduces the existing models of dispute resolution and primarily weighs the advantages and disadvantages of blockchain dispute resolution for online platforms. It also examines the application of blockchain technology in disputes between unidentified persons; the effects of the wisdom of the crowd when considering fairness; and the characteristics of procedural justice in blockchain dispute resolution.

This study is based on an online dispute resolution practice and data analysis, obtained from a survey (hereafter, the Survey) of the jurors and stakeholders of the Kleros blockchain dispute resolution platform. The Survey contains twenty questions to evaluate the skills and preferences of Kleros jurors and stakeholders. The study also assesses the characteristics of the adjudication process on blockchain platforms.

1. Dispute Resolution Models

There are three general models of dispute resolution: state court litigation; professional arbitration, including religious tribunals; and crowdsource dispute resolution, including blockchain dispute resolution. A modern technological solution also exists: automated conflict resolution systems such as an artificial intelligence judge. Every dispute resolution model has certain advantages and disadvantages.

[1] CIW. 2018. Alibaba's cross border e-commerce platform AliExpress reached 150 million buyers. Available at: https://www.chinainternetwatch.com/26756/aliexpress-social-ecommerce/ (accessed: 18.08.2019)

1.1. State Court

State courts take a professional approach to the dispute resolution process. The main advantage of the state court is that its judgments can be enforced by a coercive state power. However, because state courts have long, drawn out and costly procedures for dispute resolution, litigants in online trading disputes usually do not file lawsuits to a state court. Even specially created small claims state courts cannot fully meet the needs of disputing parties. For example, in Japan, a Small Claims trial takes approximately two months, from the filing of the case to the final judgment. The cost to file such a case is almost half of the value of an average e-commerce purchase [Habuka H., 2017: 79].

1.2. Professional Private Arbitration

For many centuries, professional arbitration has been the only option for dispute resolution. Its roots date back to early Greek, Roman and Jewish communities [Barrett J., 2004: 2–19]. The main advantages of arbitrators are speed and fairness: professional arbitrators resolve disputes faster than state courts do and the knowledge and reputation of individual arbitrators guarantee fairness.

The growth of online commerce caused an increase of small disputes between geographically distant parties. Small online disputes necessitate a rapid and cost-effective resolution process. As a result, online dispute resolution (hereinafter ODR") was developed.

1.3. Online Dispute Resolution

In response to market needs, some states help private arbitrators to organise online dispute resolution platforms. Online dispute resolution is a settlement carried out by combining the information processing powers of computers with the networked communication facilities of the Internet [Hörnle J., 2009: 75]. ODR is a form of dispute resolution in which reputable arbitrators adjudicate claims online. For example, the European Online Dispute Resolution platform, organized by the European Commission, provides access to dispute resolution tools. Private, authorized dispute resolution bodies offer out-of-court settlement procedures through this platform. The European Online Dispute Resolution platform resolved more than 36,000 cases in 2018[2].

[2] European Commission. 2018. Functioning of the European ODR Platform. Available at: https://ec.europa.eu/info/sites/info/files/2nd_report_on_the_functioning_of_the_odr_platform_3.pdf, (accessed: 03.08.2019)

1.4. Crowdsourced Dispute Resolution

Crowdsourced dispute resolution is an offline or online form of extrajudicial tribunal. Whereas offline mob justice can descend into criminal actions such as a lynching, the needs of the online market shift the focus to online dispute resolution. Crowdsource dispute resolution is a common solution for groups seeking to manage themselves by creating rules and establishing authorities and institutions to facilitate social regulation [Tyler T., 2000: 118–119].

In contrast to competent court judges and professional arbitrators, crowdsource arbitration consists of untrained jurors demonstrating jointly the wisdom of the crowd.

Commercial online platforms incorporate a number of systems for crowd dispute resolution. The ODR systems at eBay and PayPal process 60 million cases per year, 90 percent of which are resolved through automation. Another online dispute resolution platform, Modria, has handled more than one million cases in the United States and around the world[3].

2. Online Blockchain Dispute Resolution

Blockchain technology introduces a novel element in online dispute resolution. Never before have disputes between pseudonymous persons been resolved by pseudonymous jurors with a lower risk of manipulation. Blockchain dispute resolution is a type of online dispute resolution. Because blockchain technology helps to manage data, preserve evidence and keep procedures fair, it has the potential to improve traditional proceedings. There are two types of blockchain dispute resolution, depending on the professional skills and number of jurors involved. The first employs professional arbitrators, while the second relies on a crowdsourced model of dispute resolution.

Dispute resolution can be carried out as a main activity or as an additional service.

Kleros and Rhubarb are the most well-known platforms specializing in blockchain dispute resolution. They employ blockchain technology and crowdsource methods to adjudicate disputes fairly and in a decentralized manner. Both Rhubarb and Kleros base their platforms on the ancient Greeks' approach to disputes that offers a reward to the person whose suggested resolution succeeds in bringing the parties to an agreement. Kleros provides advanced technical solutions and services, such as smart contracts and escrow. Kleros uses blockchain technology

[3] Modria. Online Dispute Resolution, p.6. Available at: https://www.tylertech.com/Portals/0/OpenContent/Files/4080/Modria-Brochure.pdf (accessed: 26.09.2019)

to maintain network security, register jurors, organize reward distribution among jurors, and enforce the jury's decision.

Dispute resolution, as an additional service, is carried out by the Baidu and Alibaba-Taobao platforms. In addition to being a search engine, communication and technological service, Baidu has its own online judicial arbitration system. The Baidu blockchain judicial arbitration system was built on blockchain in collaboration with the Qingdao Arbitration Commission to solve the problem of online trials and real-time electronic evidence preservation. The online trading platform Alibaba-Taobao uses public assessors to resolve e-commerce disputes arising on the platform. Alibaba-Taobao arbitration systems, like Baidu, use the immutability of blockchain to construct a trustworthy register of evidence from original sources.

3. The Advantages of Blockchain Dispute Resolution

3.1. Judgments of Unidentified Persons

It is impossible to identify individual blockchain users. They leave only indirect identifying signs such as a crypto address, pseudonym on a social network, email address or IP address. In traditional court proceedings, it is necessary to disclose a person's identity. However, to resolve a small dispute quickly, many online dispute resolution platforms do not require personal identification. In this case, blockchain dispute resolution provides a means for working with anonymous users, making it possible to conduct operations and settle disputes without confirming the identity of either party. It is now possible for dispute resolution systems based on blockchain technology to have unidentified jurors resolve conflicts between unidentified parties. The main idea behind dispute resolution on blockchain is that a number of anonymous jurors, who do not have to trust each other, can reach consensus on a just decision[4]. The main advantage of blockchain dispute resolution is that unidentified judges can openly express their opinion of what is fair with regard to the actions, rights and obligations of nameless persons.

3.2. Reputation Built on Historical Data

Blockchain technology assumes pseudonymity and a lack of identity. Cooperation on blockchain platforms is controversial. It is difficult to trust and cooperate with an unknown person. Axelrod [Axelrod R., 1981: 6] believes that the foundation of cooperation is not really trust, but the durability of the relationship. This

[4] Ast F., Bergolla L. et al. Dispute revolution. The Kleros handbook of decentralized justice. Available at: https://ipfs.kleros.io/ipfs/QmZeV32S2VoyUnqJsRRCh75F1fP2AeomVq2Ury2fTt9V4z/Dispute-Resolution-Kleros.pdf (accessed: 14.08.2019)

quality of durability is only achieved by observing the full history of transactions by crypto-accounts on a blockchain network. Blockchain technology can guarantee the immutability of crypto-account historical data and assure, with cryptographic proof, that the data is real. Therefore, trust in blockchain dispute resolution and the soundness of its reputation could be grounded on the fact that all of a crypto-account's historical data is transparent and easily inspected. The existence and intentions of the parties are verified by the fact of a dispute, the evidence provided, the fee for the case proceeding, and historical data of the account from which the cryptoassets were transferred. The transparency and immutability of blockchain network data can substitute for the traditional approach to reputation that is based on opinion and word of mouth.

3.3. Immutability of Execution

Dispute resolution platforms do not possess coercive power by themselves. In a traditional dispute resolution process, the responsible bodies enforce the award reached through arbitration. However, the verdict of the jury in blockchain dispute resolution can be executed via smart contract without the need for enforcement by a state court. This holds particularly true for cryptocurrencies and other cryptoassets. Because a smart contract is based on blockchain technology, the execution of the arbitrator's award is automatic. This self-enforcement, agreed to by the disputing parties and made possible through modern technology, ensures its execution. The Kleros platform has a smart contract that locks the disputed cryptoassets into escrow and transfers them to the winning party upon adjudication. This process is irreversible. Thus, in many cases, a blockchain dispute resolution could be viewed as the final decision. This is especially true for anonymous parties.

The immutability of a cryptoassets award based on a decision by anonymous online jurors does not abrogate the right to seek protection in a state court, although, in many countries, an arbitration award is final in the sense that awards have *res judicata* effect. To be precise, once an award has been made, and unless the award is successfully challenged, the same matter cannot be brought before a court or arbitration tribunal again [Hörnle J., 2009: 101].

3.4. Cooperative Crowdsourcing

In ancient times, one way to settle conflicts was to enable a crowd to make a judgement. Crowdsource dispute resolution is the practice of replacing judges, arbitrators or mediators with a group of people called the crowd"[5]. The primary purpose

[5] Dimov D. Crowdsourced online dispute resolution. Available at: https://openaccess.leidenuniv.nl/bitstream/handle/1887/50156/Crowdsourced_Online_Dispute_Resolution_3e.pdf?sequence=1 (accessed: 23.09.2019)

of most BDRPs is to organize members of the blockchain community for participation in dispute resolution as jurors. The capability to exchange individual opinions and the possibility to vote by means of blockchain technology make it possible to produce a single collective judgment. The crowdsourced ODR mechanism assists the parties in their negotiations for a settlement by reality-testing their positions against the supposed common sense of the volunteers forming 'the jury' [Hörnle J., 2009: 82].

Crowdsource dispute resolution has become more accessible with the growth of Internet technology. The online crowdsource dispute resolution platform is able to handle a substantially larger number of disputes than conventional arbitration. For instance, from 2012 to 2014, the Taobao User Dispute Resolution Center settled an average of more than 2,000 consumer grievances per day, including 238,000 online-shopping disputes in 2013 alone[6].

3.5. The Wisdom of the Crowd

Crowdsource dispute resolution exploits the wisdom of the crowd principle. According to this concept, all members of a society are holders of the fairness existing within that society. The more members of the society that are included in a certain community, the more power that community has to resolve disputes. The wisdom of the crowd utilizes fairness from bottom to top, as compared to the traditional model of justice in which a limited group of professionals interprets laws and hands doctrinal rulings down from top to bottom.

From a psychological standpoint, crowdsource dispute resolution is a crowd-based socio-cognitive system composed of groups of independently thinking individuals [Surowiecki J., 2004: 42]. The system is based on the idea that a diverse group of autonomous agents, each with different models, perceptions, motivations and rationality, can often analyze or predict scenarios or data more effectively than individuals can, even when those individuals are specialists in their area of expertise[7].

The jurors use a process of metacognition to improve joint action. Metacognition allows the jurors to monitor their own thought processes, taking into account the knowledge and intentions of others [Boddington P., 2017: 81]. A single juror operating alone cannot apply this approach: to enhance fairness, jurors must cooperate and share their thoughts.

---

[6] Erickson J., Wang S. How Taobao Is Crowdsourcing Justice in Online Shopping Disputes. Available at: https://www.alizila.com/how-taobao-is-crowdsourcing-justice-in-online-shopping-disputes/ (accessed: 14.08.2019)

[7] Noriega P. Crowd-based socio-cognitive systems. Crowd Intelligence: Foundations, Methods and Practices. Available at: http://research.gold.ac.uk/id/eprint/10370/ (accessed: 27.08.2019)

In terms of procedural justice, platforms for blockchain dispute resolution employ a group engagement model with discretionary cooperation. That is, it taps into the internal motivation of each member, as compared to mandatory cooperation that is stipulated by a group [Tyler T., 2003: 353]. However, the discretionary cooperation between Kleros jurors and members differ. As a rule, jurors on Kleros and other platforms are willing to cooperate. The Survey shows that more than 76 percent of jurors on Kleros are willing to discuss details of a case with other jurors and members. However, in contrast to jurors, 57 percent of the members of a community are not ready to discuss a case with jurors. Therefore, Kleros community members are less cooperative than jurors are.

The crowd can provide unexpected solution capacity and find a solution faster than individual experts can. According to Rader, when the Roche company had a problem with the precise measurement of sample quality and quantity, it offered a prize and a viable solution was found within six weeks. Moreover, it turned out that the non-winning submissions replicated everything that Roche had tried over its 15 years of proprietary research. The curated crowd of people was able to solve difficult technical problems with a 92 percent success rate, save an average of 60 percent in cost over traditional methods, and solve most problems twice as fast as traditional methods[8]. Crowdsourcing achieves this by dividing a large job that might be too difficult or time-consuming for one person into smaller actions that many people work to solve [Kolb B., 2013: 173].

Crowdsource dispute resolution can resolve a larger number of disputes than professional arbitration. For example, China's Taobao online marketplace employed a crowdsourced resolution process that utilizes online juries to resolve millions of disputes between 2014 and 2017 [Habuka H., 2017: 76]. Thus, crowdsource dispute resolution using cooperative jurors achieves greater effectiveness and fairness than other methods.

3.6. Jurors

Blockchain technology allows the development of a jurors' forum of unlimited size. According to [Dimov D., 2017: 25] crowdsourcing applications are ineffective if too few people participate. But what is the minimum number of jurors required to demonstrate fairness? In simple cases where most members of a population would choose a single solution, a jury of three to five members could accurately represent the opinion of the entire population In a complicated case, the more jurors who par-

[8] Rader S. The Power of Crowd Based Challenges NASA's Practical Toolkit for Open Innovation. Available at: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20170012345.pdf (accessed: 24.08.2019)

ticipate in the arbitration, the fairer the judgment is. Public participation programs are more successful if more people participate [Lawrence R., 1997: 21].

The Taobao User Dispute Resolution Center attracted more than 575,000 jurors between 2012 and 2014. The jurors sat on 31-member panels that reviewed evidence submitted by feuding buyers and sellers. Volunteer jurors can choose cases according to their interests and may participate in up to 20 cases per day[9].

The Kleros platform declared that the resolution of disputes would be achieved through crowdsourcing [Ast F., 2019: 41–42]. In 2019, most juries had few members and even the pool of potential jurors was limited in size. As a rule, first-round juries were composed of from three to five members. The parties determine the exact number of jurors. Kleros has the potential to attract more jurors and operate as a strong crowdsource platform.

According to the Survey, 46 percent of Kleros jurors believe that they can resolve from two to five cases per day. The difference between Taobao and Kleros is reflected in the complexity of the cases they address. As a rule, Kleros disputes are more challenging.

Kleros jurors tend to have solid common sense, strong logic and a good grasp of blockchain technology. According to the Survey of Kleros community members and jurors, 86 percent of jurors and 71 percent of members successfully resolved complex logical tasks; 86 percent of jurors and 57 percent of members correctly understood the meaning of basic legal terms; and 54 percent of jurors and 28 percent of members were able to resolve professional legal cases. Therefore, Kleros jurors have the potential to resolve not only simple conflicts, but also disputes with a medium level of complexity, especially in the blockchain industry.

Thus, the fairness of the crowd-based socio-cognitive dispute resolution process, among others, depends on the number and qualification of jurors taking part in the adjudication process. Small claims can be effectively resolved online.

3.7. Technological Advantages

Online Blockchain dispute resolution is carried out in electronic form. All communication, notifications, documents and evidence, are made digitally. This technology reduces costs and increases speed. The blockchain technology itself ensures that data are secure, immutable and transparent and all operations are carried out on a distributed ledger. Specifically, blockchain technology is used to transfer payments among participants, including rewards for the jurors, and to register jurors and count jurors' votes during the adjudication process.

[9] Available at: https://www.alizila.com/how-taobao-is-crowdsourcing-justice-in-online-shopping-disputes/ (accessed: 14.08.2019)

The most well-known application of blockchain technology is smart contracts that ensure the conditional transfer of values among disputing parties and the court. Agreements incorporated into the smart contract or the execution of the smart contract can be appealed to a dispute resolution platform or national court.

Thus, technology ensures access to the dispute resolution process and justice.

3.8. Wide Audience

The potential audience of a BDRP is not restricted to a certain class of users or nations. The ODR on blockchain is not dedicated only to blockchain users. Standard online and e-commerce disputes could utilize it, too. Blockchain dispute resolution is based on a common understanding of justice and an agreement of a compact society (members of the dispute resolution platform) on the fairness and principles of justice. The society is a more or less self-sufficient association of persons who, in their relation to one another, recognize certain rules of conduct as binding and who, for the most part, act in accordance with them [Rawls J., 2009: 4]. In this sense, a BDRP focuses primarily on the persons associated with such a distributed stateless society. The jury can make judgments and interact across national borders. Everyone who accepts the dispute resolution principles of the platform can take part as a juror or disputing party. The independence of jurors and shared values make blockchain dispute resolution advantageous for many cases all over the world.

3.9. Pluralism of Opinions

Blockchain dispute resolution jurors hail from many different countries and cultures and their varying approaches to fairness are rooted in differing religions, traditions and beliefs.

This technology makes it possible for everyone to act as a juror regardless of his or her nationality, ethnicity, religious persuasion or age. The diversity of jurors' opinions facilitates fairness and prevents vigilante justice.

3.10. Higher Speed and Lower Cost

National court proceedings and traditional dispute resolution are slow owing to the need to examine evidence thoroughly and also due to bureaucracy.

The significant time and money required to resolve disputes in state courts are the reasons why many have switched to online arbitration. From a purely utilitarian point of view, it makes no sense for the claimant to apply to a foreign court to resolve cross-border small claims and spend a lot of time and money on compli-

cated procedures. Cross-border litigation and enforcement are very expensive and time-consuming, and in the case of small claims, the costs and delays involved are frequently disproportionate to the eventual remedy [Hörnle J., 2009: 44].

Blockchain dispute resolution processes information faster than an individual arbitrator can. The opinion poll model allows parties to express their opinions about a dispute without using legal language, revealing their names or taking a fee[10].

Crowd-sourcing is cost effective. For example, volunteers in the Taobao User Dispute Resolution Center resolved disputes without reward[11]. Jurors on the Rhubarb dispute resolution platform cover their own expenses, charging nothing to the disputing parties for rendering a decision[12]. Rader estimates that in-house development is anywhere from three to 10 times more expensive than crowd-based development[13].

Therefore, online dispute resolution generally and the crowdsource model in particular are fast and cost-effective methods for resolving disputes.

4. Drawbacks of Blockchain Dispute Resolution

4.1. Aggregate Decisions Can be Unfair

Not every crowd is efficient. There is a difference between jurors making collective versus aggregate decisions. The collective decision assumes an exchange of opinions to influence the judgment of others. According to [Tideman N., 2017: 5], a collective decision occurs when members of a group make individual decisions that they would not make if the other members were not also making related decisions. A collective decision thus entails a coordination of intentions. If, however, the other members do not influence individuals of the group or crowd, they make what is called an aggregation of decisions[14]. The crowdsourced model of dispute resolution does not work when jurors reach decisions separately. There is no wisdom of the crowd in an aggregate decision. Thus, an aggregate decision is not as fair as a cooperative decision, although this is not so critical in a simple dispute.

---

[10] Martic D. Blind Arbitration Proposal for Anonymous Crowdsourced Online Arbitration. Sintelnet WG5 Workshop on Crowd Intelligence: Foundations, Methods and Practices. 2019. European Network for Social Intelligence, pp. 94–107.

[11] Available at: https://www.alizila.com/how-taobao-is-crowdsourcing-justice-in-online-shopping-disputes/ (accessed: 14.08.2019)

[12] Rhubarb. FAQ. Available at: https://www.rhucoin.com/faq.aspx (accessed: 26.08.2019)

[13] Available at: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20160012792.pdf (accessed: 24.08.2019)

[14] Dimov D. Crowdsourced online dispute resolution. Available at: https://openaccess.leidenuniv.nl/bitstream/handle/1887/50156/Crowdsourced_Online_Dispute_Resolution_3e.pdf?sequence=1 (accessed: 23.09.2019)

An aggregate decision can be fair due to the existence of a so-called focal point. The focal point is the expectation of a conclusion that people whose actions are not coordinated tend to have in the absence of communication. Most situations provide some clue for coordinating behavior, some focal point for each person's expectation of what the other expects him to expect to be expected [Schelling T., 1980: 57]. Thus, jurors can find a common solution without any communication or coordination. The focal point depends on people's level of rationality, which is based on precedent or common knowledge [Sugden R., 1995: 544]. In the international community, however, cultural rationality can be diverse. The focal point can shift even under unintentional contact. The focal points may certainly be different when speech is allowed [Schelling T., 1980: 73].

In practice, many ODR platforms use an aggregate decision model. In a blockchain society, reputation carries less importance due to the anonymous nature of the technology. Most of the judgments on the Kleros platform are aggregate. The jurors have no obligation to discuss the evidence.

There are no formal procedures for jurors' meetings. In terms of procedural fairness, giving people fair procedures means putting more emphasis upon informal dispute resolution [Tyler T., 2000: 121]. Therefore, informal Kleros procedures facilitate fairness.

To prevent manipulation of the result, Kleros prevents jurors from disclosing their votes before the result is made public. The efficacy of the crowd-based solution is dependent on the precision of the information signal received by each agent, which varies with agent sophistication and task complexity [Ma P., 2016: 26].

At the same time, the Survey shows that 85 percent of Kleros jurors are willing to discuss case details with members of the larger Kleros community, and as many as 77 percent of the jurors are willing to discuss the case with other jurors.

Jurors on the Rhubarb platform can discuss and debate the merits of the proposal under consideration until the final vote is due. They can also ask questions or try to convince the disputants to agree to the terms for which they intend to vote[15].

Although the exchange of opinions generally slows the adjudication process, it should be obligatory for the resolution of complicated cases. Otherwise, it would not draw on the wisdom of the crowd and could produce a decision that is less fair.

4.2. Manipulations and Collusions

In traditional methods of dispute resolution, it is essential that the disputing parties trust in the neutrality of the jurors.

[15] Rhubarb. FAQ. Available at: https://www.rhucoin.com/faq.aspx (accessed: 26.08.2019)

By contrast, any blockchain transaction can be concluded successfully without need of mutual trust because the technology effectively secures transactions involving cryptoassets between unidentified persons. Trust in jurors also plays no role because their identities remain unknown both to the disputing parties and, if desired, to each other. For example, jurors on the Rhubarb platform must disclose their names and email addresses, and provide proof of U.S. citizenship. However, Rhubarb does not validate this information. Thus, the anonymous nature of the users, the fact that one person can generate multiple accounts and the complete absence of personal reputation means that manipulation and collusion could be widespread on blockchain dispute resolution platforms. One person could create multiple pseudonymous accounts and act under the guise of several jurors to gain a disproportionately large influence. This is known as a Sybil attack, where a node illegitimately claims multiple identities[16]. The lack of a mechanism for validating identities makes it impossible to prevent various biases and manipulations such as secret agreements or alliances. This creates additional risk for the parties. Relying on jurors with proven reputations mitigates such risk. The anonymity of the members of the crowd participating in online opinion polls decreases their transparency. This, in turn, can have a negative influence on both objective and subjective procedural fairness [Dimov D., 2017: 169]. In the absence of a mechanism for establishing a reputation, blockchain dispute resolution could tend towards becoming less fair.

If jurors follow strong moral guidelines, it can prevent manipulation of the dispute resolution process. In practice, cooperation purely with the motive of achieving a fair dispute resolution could substitute for cooperation based on self-interest or remuneration. The Kleros and other blockchain-based dispute resolution platforms were created to render arbitration as a commercial service. The main motivation of Kleros jurors is to earn money, as compared to the volunteer jurors of the Taobao online retailer, who resolve disputes without reward. Self-interest and egoistic cooperation impair justice. Any manipulation or collusion in the adjudication process is fraud and prevents jurors from treating the parties in a dispute with neutrality and impartiality. By definition, a decision is fair when all parties are treated equally [Hörnle J., 2009: 15–18].

Unbiased, neutral jurors [Mansbridge J., 1990: 176] should make the decisions in dispute resolution. Kleros has successfully introduced a number of procedures, such as appellation and jurors making cryptoasset deposits that make it more difficult and costly to manipulate the process. Kleros also allows participants to ap-

[16] Newsome J., Elaine S., Dawn S., Adrian P. The sybil attack in sensor networks: analysis & defenses. In: Third international symposium on information processing in sensor networks. 2004. pp. 259–268.

peal decisions to a new jury. The essence of appellation is that every appeal doubles the number of jurors. It might be possible to bribe two or three jurors in an initial round, but it is difficult to use subornation for the larger number of jurors involved in subsequent appeals. Additionally, disclosing jurors' identities and establishing their reputations could serve as a deterrent to coordinated manipulative practices. Collusion remains a serious challenge for Blockchain dispute resolution platforms. One of the parties could coordinate with or control the jurors to obtain an advantageous ruling. For a system of justice to be effective, behavior must be shaped by judgments about what is right, regardless of personal interests or gain [Tyler T., 2000: 118].

4.3. Incorrect Judgments Stemming from Herding Behavior

When jurors have little information on a subject, they rely on the judgments of others, resulting in so-called herding behavior or informational cascade. This can be defined broadly as the alignment of the thoughts or behaviors of individuals in a group (herd) through local interaction and without centralized coordination [Raafat R., 2009: 424]. The jurors reach consensus not by a process ofthorough deliberation, but by obeying or aligning themselves with the opinions of others. The process of jury deliberation may engender consensus, but at the cost of potentially amplifying the errors of some jurors, thereby leading to incorrect judgments [Luppi B., 2013: 24]. The main problem is that herding behavior has the potential to violate a disputant's human rights and could lead to rule by so-called mob law."

4.4. Lack of Control Over the Process

Technology can prove a substantial barrier for users, particularly when they have doubts about their ability to operate on a given platform and whether they can obtain the necessary assistance in time [Lu Z., 2017: 364]. Furthermore, disputing parties who apply for arbitration seek intervention by jurors, but not necessarily an imperative ruling that they must blindly obey.

Disputants desire some third-party control in dispute-resolution procedures, but they generally reject any type of autocratic control [Lind A., 1988: 15]. Although major or complicated cases demand more time and less stringent controls, disputants with time constraints who pursue common goals and who agree on a standard that can be applied quickly to resolve differences in belief might agree to more autocratic adjudication [Thibaut J., 1975: 552–554]. Thus, faster and more autocratic solutions are more suitable for small cases.

Due to the peculiarities of blockchain technology, a jury decision in blockchain dispute resolution cannot be changed once it is executed. The automatic execution

built into a smart contract might not reflect the desire of the disputants. And because all blockchain actions are recorded on a distributed ledger, such judgments are, ultimately, irreversible. As a result, parties can essentially lose control over a dispute when they utilize blockchain technology.

4.5. Common Sense Instead of Applicable Law

Alternative forms of dispute resolution, especially international online blockchain dispute resolution, generally have little in common with national laws. In the case of e-disputes, and especially cross-border e-disputes, it is not always obvious which laws apply[17]. The blockchain stateless society tends towards an anarchical vision of fairness. Jurors appeal directly to natural human rights and morality, skipping intermediary national law. In most cases, jurors on a blockchain platform rely more on common sense and logic than they do the laws of this or that country.

According to the Survey, 84 percent of Kleros jurors believe that they should not have to determine a national jurisdiction to which the dispute is most closely connected.

In simple disputes with clear solutions, jurors have wide discretion in applying adjudication standards. However, this approach would be unfair and unacceptable for major or complicated cases. Even when the parties to a dispute choose substantive and procedural law, or *lex arbitr* rules in their agreement to arbitrate, jurors could not apply such laws if they had no specific knowledge of them. Interestingly, the inability to apply a certain law does not necessarily discourage jurors in online adjudication. According to the Survey, even if the parties were to choose the law of Afghanistan for their arbitration case — that is unfamiliar to the vast majority of potential jurors — 61 percent of Kleros jurors were willing to take part in dispute resolution anyway.

4.6. Low-Skilled Jurors

When jurors are highly qualified, their decisions are naturally fair. However, it is necessary to differentiate between someone with a narrow specialization in, for example, blockchain technology, and a broadly qualified judge who has specialized knowledge in logic, justice, forensics and law. Thus, unlike judges in a national court, online jurors often do not possess professional arbitration skills and so their decisions in complicated cases might not be as fair.

[17] Van den Heuvel E. Online Dispute Resolution as a solution to cross-border e-disputes. Available at: http://www.oecd.org/internet/consumer/1878940.pdf (accessed: 05.09.2019)

Cognitive ability and knowledge of a task might be more important than group process when it comes to predicting decision-making effectiveness in complex planning tasks [Devine D., 1999: 630].

4.7. Ethical, Cultural and Communicative Problems

Due to cultural differences, solutions reached might not be good in an ethical sense or acceptable to all the parties. As a rule, jurors try to find the right solution, defining the right as that which maximizes the good [Rawls J., 2009: 42]. However, judgments on the right and the good could be made separately. The good can be defined as excellence, pleasure or happiness. The perception of what is ethically good depends on the culture of a certain community. Thus, jury judgments in international online dispute resolution might be not ethically good or fair for the parties in dispute.

Apart from cultural and ethical problems, there are communicative difficulties. The English language, as the main language used in proceedings, substantially affects the result. Not only is it a barrier for disputants from non-English-speaking countries, but it is also a source of cultural differences. There are notable differences for objects that might be familiar to some cultures but not others[18]. In the international dispute resolution process, the people of different nations have different understandings of the same things.

4.8. Simplification of Procedures and Predetermined Answers

Dispute resolution platforms adjudicate disputes faster than national courts do. This is achieved, in part, by simplifying procedures and standards. In most cases, the resolution of online disputes involves no investigative procedures, hearing of evidence and testimony or discussion or contest. However, online dispute resolution platforms are poorly suited to complicated problems because simplifying procedures can compromise fairness[19]. In disputes that involve conflicting beliefs about objective truth, the principal criterion of the successful dispute resolution is the accuracy or correctness of decisions resulting from the procedure [Lind A., 1988: 36]. A lack of procedural fairness could result in an unjust settlement of the claim. Simplifying the judicial process increases speed but restricts the ability of jurors to express their thoughts, sometimes limiting their options for answering

[18] Jana R. and Lovejoy J. Exploring and Visualizing an Open Global Dataset. Available at: https://ai.googleblog.com/2017/08/exploring-and-visualizing-open-global.html (accessed: 02.08.2019)

[19] Ambrogi R. Is There a Future for Online Dispute Resolution for Lawyers? Available at: https://www.lawsitesblog.com/2016/04/future-online-dispute-resolution.html (accessed: 12.09.2019)

or responding. For example, Kleros limits jurors to the use of Yes/No answers or allows them to input a number or date or to select multiple answers from the available options. When jurors' option are limited, their decisions might be less fair.

Conclusion

The use of technological dispute resolution has grown considerably over the past decade. This research shows that blockchain dispute resolution is effective for disputes between unidentified persons. The social and psychological aspects of blockchain dispute resolution include such concepts as the wisdom of the crowd and such technological solutions as cryptography. The wisdom of the crowd is the major source of fairness in online dispute resolution. In addition, highly motivated and knowledgeable individuals or small groups of individuals could produce decisions that are more effective, wise and fair — albeit more costly and time-consuming. Cryptography and distributed ledger technology guarantee the immutability of data. In the absence of other sources, the reputation of jurors and parties is proven by the fact of disputes, the evidence of the case, the fee for the case proceeding and the historical data of a crypto-account.

The fairness of the judgment depends on the number of jurors and their ability to cooperate on the platform. Collusions and manipulation could harm the adjudication process. The balance between cooperative actions for greater fairness and concerted acts of collusion depend on jurors' motivation and moral integrity.

Platforms for blockchain dispute resolution achieve procedural fairness with the help of fewer formalities and by treating the parties involved with dignity and respect. This form of dispute resolution provides a reasonable cost-benefit ratio. It lacks, however, such traditional elements of procedural justice as a neutral forum and jurors with a public reputation for trustworthiness.

At the same time, blockchain dispute resolution meets many objectives of procedural justice. In particular, it supports process-related goals for public involvement, provides inclusive procedures for public participation, enables interactive procedures and ensures a clear justification for decisions.

Drawing on the wisdom of the crowd, blockchain dispute resolution is a reliable instrument for settling differences between the members of an increasingly far-flung global society.

References

Axelrod R., Hamilton W. (1981) The evolution of cooperation. *Science*, vol. 211, pp. 1390–1396.

Barrett J. (2004) *History of alternative dispute resolution: The story of a political, social, and cultural movement.* San Francisco: Wiley, p. 320.

Boddington P. (2017) *Towards a code of ethics for artificial intelligence.* Cham: Springer Verlag, p. 124.

Devine D. (1999) Effects of cognitive ability, task knowledge, information sharing, and conflict on group decision-making effectiveness. *Small Group Research*, no 30, pp. 608–634.

Habuka H., Rule C. (2017) The Promise and Potential of Online Dispute Resolution in Japan. Available at: https://www.elevenjournals.com/tijdschrift/ijodr/2017/2/IJODR_2352-5002_2017_004_002_017.pdf (accessed: 21.09.2019)

Hörnle J. (2009) *Cross-border internet dispute resolution.* Cambridge: Cambridge University Press, p. 286.

Kolb B. (2013) *Marketing for Cultural Organizations: New Strategies for Attracting Audiences.* N.Y.: Routledge, p.190.

Lawrence R. et al (1997) Procedural justice and public involvement in natural resource decision-making. *Society and Natural Resources*, no 10, pp. 577–589.

Lee C. (2016). The search for peer firms: When do crowds provide wisdom? Harvard Business School Working Paper, no 15, pp. 14–46.

Lind A. (1988) *The social psychology of procedural justice.* N.Y.: Springer Science & Business Media, p. 267.

Lu Z., Xinyu Z. (2017) Study on the Online Dispute Resolution System in China. *Advances in Engineering Research,* vol. 129, pp. 1–8.

Luppi B. (2013) Jury size and the hung-jury paradox. *Journal of Legal Studies*, no 42, pp. 399–422.

Mansbridge J. (ed.) (1990) *Beyond self-interest*. Chicago: Chicago University Press, p. 416.

Raafat R. et al (2009) *Herding in humans. Trends in cognitive sciences,* vol. 13, pp. 420–428.

Rawls J. (2009) *A theory of justice.* Cambridge: Harvard University Press, pp. 4, 42.

Schelling T. (1980) *The strategy of conflict*. Cambridge: Harvard University Press, pp. 57, 73, 309.

Sugden R. (1995) A theory of focal points. *The Economic Journal,* no 105, pp. 533–550.

Surowiecki J. (2004) The wisdom of crowds: Why the many are smarter than the few and how collective wisdom shapes business. In: *Economies*, *Societies and Nations*. N.Y.: Doubleday, p. 296.

Tideman N. (2017) *Collective decisions and voting: the potential for public choice.* Abington-on-Thames: Routledge, p. 360.

Thibaut J. (1975) *Procedural justice: A psychological analysis.* N.Y.: Lawrence Erlbaum Inc., p. 160.

Tyler T. (2000) Social justice: Outcome and procedure. *International journal of psychology,* no 35, pp. 117–125.

Tyler T. (2003) The group engagement model: Procedural justice, social identity, and cooperative behavior. *Personality and social psychology review,* no 7, pp. 349–361.

The Role of Artificial Intelligence in Improving Criminal Justice System: Indian Perspective

Puneet Gawali

M.S. in Digital Forensics and Information Security, Institute of Forensic Science, Gujarat Forensic Sciences University. Address: Gandhinagar, Gujarat, India. E-mail: puneet.dfis1808@gfsu.edu.in

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

Abstract

The increasing cyber-attacks have created havoc in the criminal justice system. Understanding the purpose of crime and countering it is the crucial task for the law enforcement agencies. This research aims to present how Artificial Intelligence and Machine Learning along with Predictive Analysis using soft evidence can be used in sorting out the existing criminal record while making the use of metadata, and therefore predicting crime. Furthermore, it would surely help out the police and intelligence bodies to smartly investigate the cases by referring to the database and thus help the society in curbing the crime by quicker and more effective investigation processes. It would also assist the analyst in tracking the activities and associations of various criminal elements through their recent activities, by extracting the particular details from the documents or records. Prediction of the crime can be understood through this research. The present study reflects the accuracy level of threat from 28 states of India. By researching on this topic, it becomes evident that if proper data is fed to this model, the chances of prediction are higher and more accurate. The study also tried to find out the psychosocial perspectives of the crime and what would be the reason of individual indulges in such crime.

Keywords

Artificial Intelligence, law enforcement, criminal justice, prediction algorithm, accuracy, machine learning, motives, cyber attacks, information technology laws.

For citation: Puneet G., Sony R. (2020) The Role of Artificial Intelligence in Improving Criminal Justice: Indian Perspective // *Legal Issues in the Digital Era,* no 3, pp. 78–96.

DOI: 10.17323/2713-2749.2020.3.78.96

Introduction

In 1956, Artificial Intelligence (AI) was first introduced by its father, John McCarthy, in Dartmouth [McCarthy J., 2006: 12–14]. Digital transformation brings risks, as technology is the first layer [Dmitrik N., 2020: 54–78]. In recent years, technologies based on AI and Machine learning (ML) have progressively increased in their capability and accessibility, showing no sign of abating [Caldwell M., 2020: 1–13]. By understanding the AI law for the future, its advantages and disadvantages that can make AI advisable to humanity [Cui Y., 2020: 187–191]. AI research and its regulation aspire to balance innovation's social security against potential harms and obstructions [King T., Aggarwal N., Taddeo M., Floridi L., 2020: 89–120]. Development, adoption, and promotion of AI are the priorities of the Indian Government to make lives easier for society [Marda V., 2018: 1–19]. The preciseness and verisimilitude of the details about where the crimes occur, furthermore information on the depiction of crimes provided an approach to understanding such crimes in other countries [Furtado V., 2010: 4–17]. McGuire and Holt's further throws light on the impressive and much needed Routledge Handbook of Technology, Crime and Justice [McGuire M., Holt T., eds., 2017: 1–722] that has evidence of criminology's burgeoning of technological interest [Hayward K., Maas M., 2020: 1–25]. The most important lookout to implement this research would be to update judges to be specialist in the field of computer; such laws should be implemented wherein all the judges should be well trained to use this technology[1]. Using Artificial Intelligence which is the main emerging technology invented by John McCarthy and is beneficial as it perceives all the data as it is. In contrast, a human mind has to choose or make a selection from the different pieces of data before reasoning, leading to possible errors[2]. Information technologies and its applications has become more diverse and effective, such as COPLINK. As this COPLINK, is a licensed software that bridges the gap by conducting research as well as solving real world crimes by helping police officers as they serve the community in a sophisticated and understandable way [Chen H., 2003: 271–285]. This COPLINK project unites University of Arizona's Artificial Intelligence Lab with the Tucson Police Department's law enforcement, where crimes analyst, detectives, sergeants use this technology [Hauck R., 2002: 30–37]. In this paper, we have discussed on how the Artificial Intelligence could be used for the resolutions of criminal justice system, since it becomes difficult for the court of law to maintain the database of all the criminal activities, we have tried to sort this issue by feeding some criminal data to the model created by us and

[1] Available at: https://builtin.com/artificial-intelligence (accessed: 25.11.2019)

[2] Available at: https://towardsdatascience.com/advantages-and-disadvantages-of-artificial-intelligence-182a5ef6588c (accessed: 25.11.2019)

therefore improving the way of investigation. Data plays a significant role in the criminal justice system, especially in predictive analysis[3] since the data itself reveals the information of the crime. It is crucial to think about the diverse and vast ethical dilemmas occurring in the criminal justice system, which involves making moral judgments and deciding about wrong and right. Data mining can be used in understanding and designing crime detection models [Nath S., 2006: 41–44].

Such ethics have been maintained since the model cannot be biased and gives accurate results. We understand that using predictive analysis is challenging in policing. Still, it should not mean that law enforcement agencies should not use analytics or intelligence for the improvement of investigation [Isaac W. 2017: 543]. With this research risk assessment and the investigation of the criminal justice system will become more sophisticated. The possible question raised would be who should be accountable for semi-automated decisions? [Završnik A., 2020: 567–583] since the accuracy is directly proportional to the data fed; therefore, the entire model depends on the specificity of the data. This tool can be useful for the lawyers as well those who are expert in technology and those who are not so technically advanced; they can make usage of this tool for predicting using different datasets [Alarie B., Niblett A., & Yoon A., 2018: 106–124].

1. Preparing the Model

The most crucial concept for approaching this topic would be the understanding of recidivism; through this model, we can keep a close watch on the behavior of various states and the crime committed. As shown in the Fig. (1) we can see how through certain steps our data is being processed in order to get the desired results. Different programming languages and environments enable ML research and development of its application. Python language has a tremendous growth within the scientific computing communities in the last decade, so in this case most recent ML and deep learning libraries are associated with Python based [Raschka S. et al, 2020: 193]. Python is used to prepare the model of predictive analysis and using the EDA (Exploratory Data Analysis) when a particular data becomes large or we need to understand some complex relationships in the variables. Through this paper we can perform the molding of such data for better investigation purpose.

First, the data is loaded in python and then we perform data cleaning and exploring the information in the variables. Pandas which provide data frames are imported using python, Matplotlib provides plotting support, and Numpy provides scientific computing within dimensional object support as seen in Fig. (2).

[3] How data plays a significant role. Available at: https://www.aclu.org/issues/privacy-technology/surveillance-technologies/ai-and-criminal-justice-devil-data (accessed: 09.04.2018)

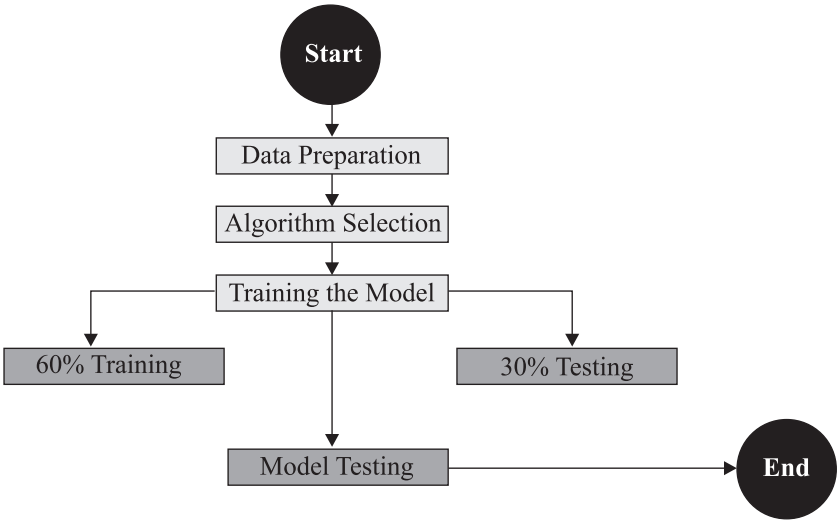

Fig. 1. Model Process Flowchart

```
In [2]:  import pandas as pd                          # pandas is a
         import numpy as np                           dataframe library
         import matplotlib.pyplot as plt              # numpy provides
         import seborn as seabornInstance             N-dim object support
         from sklearn.linear_model import             # matplotlib.pyplot
         LogisticRegression                           plots data
         from sklearn.model_selection import train_
         test_split
         from sklearn import metrics
         import os
         % matplotlib inline
```

Fig. 2. Importing Libraries

Secondly, standardization and visualization of data is very important to ensure that data fits the assumptions of the models. The Universal Rule of Law states that human rights, democracy and development depend on the level of progress the organizations and governments can achieve on the criminal justice front. The primary and crucial objectives of the criminal justice are controlling and preventing crime, maintaining law and order, protecting fundamental rights of victims along with the people in conflict with law, punishment and rehabilitation of those adjudged guilty of committing of crimes, and protection of life and property against crime and criminality in general. It is considered to be the primary obligation of the state under the constitution of India [Dhillon K., 2011: 27].

This paper would thus give an overview how every police station can update their data and predict the criminal behavior of the crime or any data available. Im-

porting various libraries and functions is the positive point of using python in this research paper since the data could be easily adjusted, it can be seen in Fig. 3 and 4.

Accurately predicting rare events is difficult, so the probability of having them in data is low, and the probability of training the algorithm is also low. Therefore, we only need a few percentages of the event to be able to train, to ensure that we have a reasonable chance to define how correctly a person or state is likely to develop the behavior or motive of committing a crime. Importing pandas will let us easily search the columns by name and see how many times this is true. Also, in the last column seen in the Fig.3 threat columns are mentioned which is categorically divided into binary 1s and 0s where 1s define that the attacks are increasing drastically whereas 0s define that the motives are mild. When a crime is predicted there will be questions arise regarding how an algorithm or code can be trustworthy[4]. This research would, therefore, throw light on this area where the data itself would be deciding everything, the more real the data the more effective the accuracy would be. Data mining and predictive analysis play an essential role in our life[5]. Now if we look into the data available very carefully, we can find whichever states having high unemployment rate (according to report by the Centre for Monitoring Indian Economy). It is noteworthy, that such states have high cybercrime rates which further denotes that in various states computer is used as a source to dupe money through various online frauds. The reason behind this is maintaining the anonymity and causing the harm because of vengeance or other motives. Cybercriminals mostly exploit the high-speed internet available at a lower cost to commit various criminal activities without being caught unless the states possess properly well-maintained cybersecurity labs to curb such crimes. The CMIE report further reveals that people belonging to age group 40 to 59 years have been successfully able to retain their jobs whereas people aged below 40 years were expelled out of their respective jobs which lead to social tension, desire of revenge, anger and other motives to launch such cyber-attacks[6].

The data shown in Fig. (3) presents the topmost cyber-crimes happened in various states of India until 2019. So far, which includes such crimes as bullying on social media and not full-fledged crimes wherein a lot of technical skills are required, this shows that certain age groups of people have launched such attacks to malign the image of the victim[7].

[4] How code can be trustworthy. Available at: https://www.smithsonianmag.com/innovation/artificial-intelligence-is-now-used-predict-crime-is-it-biased-180968337 (accessed: 05.03.2018)

[5] What is Data Mining? Definition of Data Mining, Data Mining Meaning — The Economic Times (indiatimes.com). Available at: https://economictimes.indiatimes.com/definition/data-mining (accessed: 07.12.2020)

[6] The recent unemployment data. Available at: https://www.cmie.com/kommon/bin/sr.php?kall=warticle&dt=2020-01-21%2009:51:47&msec=203 (accessed: 21.01.2020)

[7] National Crime Records Bureau Empowering Indian Police with Information Technology Available at: https://ncrb.gov.in/en (accessed: 22.10.2020)

State_UT	Personal_ Revenge	Anger	Fraud	Extortion	Causing_ Disrepute	Prank	Sexual Exploitation	Political Motives	Terrorist Activities	Inciting Hate against Country	Disrupt Public Service	Sale purchase illegal drugs	Developing own business	Spreading	Psycho or Pervert	Steal Information	Abetment to Suicide	Others	Risk
Andhara Pradesh	34	26	733	45	7	0	92	12	1	1	1	0	2	14	2	0	1	236	0
Arunachal Pradesh	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5	0
Assam	239	46	389	153	234	0	113	9	4	3	0	0	0	0	0	0	0	832	1
Bihar	5	8	351	2	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0
Chhattisga	0	1	23	2	25	0	21	4	0	1	0	0	1	0	0	0	0	61	0
Goa	0	0	11	0	12	0	4	0	0	0	0	0	0	0	0	0	0	2	0
Gujarat	17	32	401	24	154	16	23	0	0	17	0	0	1	0	0	3	0	14	1
Haryana	6	9	137	21	11	2	75	0	12	2	0	0	2	0	0	0	0	141	1
Himachal	4	1	18	1	3	1	15	4	0	0	0	0	0	0	0	0	0	22	0
Jammu &	2	0	20	7	7	3	10	3	1	2	3	0	0	1	0	0	0	14	0
Jharkhand	16	6	783	44	16	0	16	1	16	0	0	0	32	0	0	0	0	0	0
Karnataka	27	10	5441	97	49	1	85	22	1	3	3	0	5	5	1	1	0	88	1
Kerala	69	18	93	8	48	3	50	18	3	0	0	0	6	0	0	0	0	24	0
Madhya P	93	10	230	19	109	2	49	1	3	29	1	0	4	20	0	0	1	169	1
Maharash	99	129	1998	31	64	18	724	20	0	33	2	2	13	6	0	3	0	369	1
Manipur	0	0	14	3	0	0	9	0	1	1	0	0	0	0	0	0	0	1	0
Meghalaya	0	0	35	0	3	0	3	3	0	11	0	2	0	6	0	0	0	11	0
Mizoram	0	4	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0
Nagaland	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Odisha	7	0	506	224	0	0	37	0	0	0	0	0	0	0	0	0	0	69	1

State_UT	Personal_ Revenge	Anger	Fraud	Extortion	Causing_ Disrepute	Prank	Sexual Exploitation	Political Motives	Terrorist Activities	Inciting Hate against Country	Disrupt Public Service	Sale purchase illegal drugs	Developing own business	Spreading	Psycho or Pervert	Steal Information	Abetment to Suicide	Others	Risk
Punjab	14	7	48	15	19	4	85	2	0	3	0	2	2	0	0	0	0	38	0
Rajasthan	9	11	499	31	66	14	60	3	0	9	0	0	17	2	0	0	0	383	1
Sikkim	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
Tamil Nad	39	13	55	7	17	6	36	52	2	39	1	0	3	1	0	4	0	20	0
Telangana	19	3	732	51	3	2	77	14	0	3	0	0	0	0	0	0	0	301	1
Tripura	5	0	8	0	0	0	3	4	0	0	0	0	0	0	0	0	0	0	0
Uttar Prac	47	73	2351	199	343	191	343	45	0	59	9	0	75	614	0	0	0	1931	1
Uttarakha	3	41	46	16	12	22	13	0	0	0	0	0	0	0	0	5	0	13	0
West Ben	28	9	68	25	2	3	39	1	0	2	0	0	0	0	0	0	0	158	1
A & N Island	0	0	3	0	3	0	0	0	0	0	0	0	0	0	0	0	0	1	0
Chandigar	0	0	19	3	0	7	0	0	0	0	0	0	0	0	0	0	0	1	0
D&N Have	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Daman &	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Delhi UT	11	4	36	11	4	1	35	0	0	0	0	0	35	2	0	0	0	50	0
Lakshadow	0	0	1	0	0	0	2	0	0	0	0	0	0	0	0	0	0	1	0

Fig. 3. Raw Data (7)

In Fig. 4 we can see the features of data, a feature is something that's used to determine a result, and a column is a physical structure that stores the value of a feature or a result. In Fig. 12, using shape function the data is displayed in the format of rows and columns; here we have 36 rows and 13 columns; also, we check whether there are any null values present in the data sets shown in Fig. 12. Matplot library is used to create a function that cross plots feature so that we can see when they are correlated. Data is then inspected in order to eliminate any additional columns or rows to with no values that we no longer required. The duplicates including the same values are removed the same way. This is done to arrange our data since visual inspection may be error-prone and cannot deal with the critical issue of correlated columns. Thus, pandas help in understanding such null values and therefore identifying it in our data as we can see in Fig. 6, Is Null method will check each value on the data frames for null values. Similarly, Matplot library is used to create a function plots features so that we can see when the data is correlated: the color in yellow denotes the very positive correlation as seen in Fig. 11 and other color denotes that the data is not well correlated. In Fig. 11 we can see that column names on the horizontal and vertical axes is a matrix showing which column contains the data that are correlated with values.

```
In [3]:  os.getcwd()
         os.chdir ('C:/Users/Puneet/CRIME RECORD')
         os.getcwd()

Out[3]:  'C:\\Users\\Puneet\\CRIME RECORD'

In [20]: Cyber_data = pd.read_csv('Cyber new.csv') # read dataset
         Cyber_data.head()

Out[20]:
```

	State_UT	Personal_ Revenge	Anger	Fraud	Extortion	Causing_ Disrepute	Prank	Sexual Exploitation	Political Motives	Terrorist Activities	Inciting Hate against Country	Disrupt Public Service	Sale purchase illegal drugs	Developing own business
0	Andhara Pradesh	34	26	733	45	7	0	92	12	1	1	1	0	
1	Arunachal Pradesh	0	0	2	0	0	0	0	0	0	0	0	0	
2	Assam	239	46	389	153	234	0	113	9	4	3	0	0	
3	Bihar	5	8	351	2	0	0	8	0	0	0	0	0	
4	Chhattisga	0	1	23	2	25	0	21	4	0	1	0	0	

Fig. 4. Selecting the data

As we can see in Fig. (4) and (5), data is fetched from the file path and utilized for the further data cleaning and correlating.

```
In [3]:  os.getcwd()
         os.chdir ('C:/Users/Puneet/CRIME RECORD')
         os.getcwd()

Out[3]:  'C:\\Users\\Puneet\\CRIME RECORD'

In [20]: Cyber_data = pd.read_csv('Cyber new.csv') # read dataset
         Cyber_data.head()

Out[20]:
```

Causing_ Disrepute	Prank	Sexual Exploitation	Political Motives	Terrorist Activities	Inciting Hate against Country	Disrupt Public Service	Sale purchase illegal drugs	Developing own business	Spreading	Psycho or Pervert	Steal Information	Abetment to Suicide	Others	Risk
7	0	92	12	1	1	1	0	2	14	2	0	1	236	0
0	0	0	0	0	0	0	0	0	0	0	0	0	5	0
234	0	113	9	4	3	0	0	0	0	0	0	0	832	1
0	0	8	0	0	0	0	0	0	0	0	0	0	0	0
25	0	21	4	0	1	0	0	1	0	0	0	0	61	0

Fig. 5. Showing the data

2. Molding the Data

After cleaning the data of any extra columns or null values, we proceed to molding the data by inspecting if there are any issues. Algorithms are largely mathematical models which work best with numeric quantities and once the data molding is done, we can use this data for further training the algorithm as seen in Fig. 6 count, mean, std, etc. is calculated so that the data is molded accurately. Therefore, in machine learning, a lot of data manipulation is done for trial and error and predicting the best of the accuracy. When the data is manipulated it's very easy to change the meaning of the data what also helps in understanding if data has gone wrong anywhere. The entire model is created in *Jupyter Notebook*, therefore keeping track of all the changes and updates have been done automatically [Perkel J. et al, 2018: 145–147]. We also have the interactivity of the python interpreter using which we can make our data simpler for the prediction, as seen in Fig.6 and 7.

```
In [6]: Cyber_data.describe()
Out [6]:
```

	Personal_ Revenge	Anger	Fraud	Extortion	Causing_ Disrepute	Prank	Sexual Exploita-tion	Political Motives	Terrorist Activities	Inciting Hate against Country	Disrupt Public Service	Sale pur-chase illegal drugs
count	36.000000	36.000000	36.000000	36.000000	36.000000	36.000000	36.000000	36.000000	36.000000	36.000000	36.000000	36.000000
mean	22.055556	12.805556	418.083333	29.166667	33.666667	8.222222	56.388889	6.055556	1.222222	6.055556	0.583333	0.166667
std	44.940560	25.484807	1007.891615	54.345193	72.200119	31.825516	129.880886	12.094732	3.330475	13.259917	1.645340	0.560612
min	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000
25%	0.000000	0.000000	6.750000	0.000000	0.000000	0.000000	2.750000	0.000000	0.000000	0.000000	0.000000	0.000000
50%	5.000000	3.500000	41.000000	7.500000	3.500000	0.000000	15.500000	0.500000	0.000000	0.000000	0.000000	0.000000
75%	21.000000	10.250000	392.000000	26.500000	20.500000	3.000000	52.500000	4.000000	1.000000	3.000000	0.000000	0.000000
max	239.000000	129.000000	5441.000000	224.000000	343.000000	191.000000	724.000000	52.000000	16.000000	59.000000	9.000000	2.000000

```
In [7]: cyber_data.isnull().any()
Out [7]:  State_UT                          False
          Personal_Revenge                  False
          Anger                             False
          Fraud                             False
          Extortion                         False
          Causing_Disrepute                 False
          Prank                             False
          Sexual Exploitation               False
          Political Motives                 False
          Terrorist Activities              False
          Inciting Hate against Country     False
          Disrupt Public Service            False
          Sale purchase illegal drugs       False
          Developing own business           False
          Spreading                         False
          Psycho or Pervert                 False
          Steal Information                 False
          Abetment to Suicide               False
          Others                            False
          Risk                              False
```

Fig. 6. Null values are checked

```
In [6]: Cyber_data.describe()
Out [6]:
```

Prank	Sexual Exploi-tation	Political Motives	Terrorist Activities	Incit-ing Hate against Country	Disrupt Public Service	Sale purchase illegal drugs	Develop-ing own business	Spreading	Psycho or Pervert	Steal Infor-mation	Abetment to Suicide	Others	Risk
36.000000	36.000000	36.000000	36.000000	36.000000	36.000000	36.000000	36.000000	36.000000	36.000000	36.000000	36.000000	36.000000	36.000000
8.222222	56.388889	6.055556	1.222222	6.055556	0.583333	0.166667	5.500000	18.638889	0.111111	0.444444	0.055556	137.666667	0.305556
31.825516	129.880886	12.094732	3.330475	13.259917	1.645340	0.560612	14.484474	102.147275	0.398410	1.229273	0.232311	349.023454	0.467177
0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000
0.000000	2.750000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	1.000000	0.000000
0.000000	15.500000	0.500000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	14.000000	0.000000
3.000000	52.500000	4.000000	1.000000	3.000000	0.000000	0.000000	2.250000	1.000000	0.000000	0.000000	0.000000	101.250000	1.000000
191.000000	724.000000	52.000000	16.000000	59.000000	9.000000	2.000000	75.000000	614.000000	2.000000	5.000000	1.000000	1931.000000	1.000000

```
In [7]: cyber_data.isnull().any()
Out [7]: State_UT                          False
         Personal_Revenge                 False
         Anger                            False
         Fraud                            False
         Extortion                        False
         Causing_Disrepute                False
         Prank                            False
         Sexual Exploitation              False
         Political Motives                False
         Terrorist Activities             False
         Inciting Hate against Country    False
         Disrupt Public Service           False
         Sale purchase illegal drugs      False
         Developing own business          False
         Spreading                        False
         Psycho or Pervert                False
         Steal Information                False
         Abetment to Suicide              False
         Others                           False
         Risk                             False
```

Fig. 7. Null Values shown in risk column

3. Testing Model's Accuracy

In this section we will discuss the role of the Machine Learning algorithm. An algorithm can be defined as an engine that drives the entire process. For our prediction, we will use data containing examples of the results and try to predict the future using the scikit learn and the algorithm's logic the data is analyzed. This analysis evaluates the data concerning a mathematical model and logic associated the algorithm, and the algorithm then uses the results of this analysis to adjust internal parameters to produce a model that has been trained to best fit the features and give the best results. The best result is defined by evaluating a function specific to a particular algorithm. Therefore, the fit parameters are stored and hence the model is now trained. Further, we use this model to predict on the real data. We use the Scikit learn package in python to predict on the real data. The parameters of the trained model along with the python code is used to predict whether the state is in threat of cyber-attack or no. Selecting an appropriate algorithm from scikit learning was the toughest part which we faced while researching on this paper.

Prediction means supervised learning so eliminating all other algorithms was my main goal, furthermore, prediction can be divided into two more categories regression and classification, where regression means a continuous set of values. Predicting binary outcome whether the threat is there or not; we further eliminated all the algorithms that do not support classification in general and especially binary classification. Naïve Bayes, Logistic Regression and Decision Tree are algorithms which support classic machine learning algorithms and also provide excellent help in understanding more complex algorithms.

```
In [8]:   plt.figure(figsize=(15,10))
          plt.tight_layout()
          seabornInstance.distplot(cyber_data['Risk'])

Out [8]:  <matplotlib.axes._subplots.AxesSubplot at 0x1c303d03808>
```

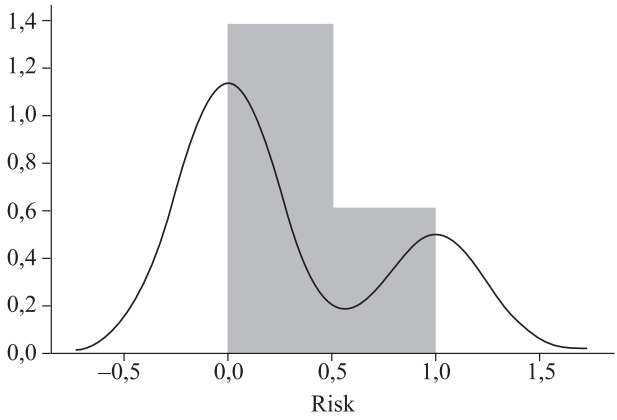

Fig. 8. Graph Denoting the Risk

```
In [13]: df.corr()
Out [13]:
```

	Online Banking Frauds	Cyber Blackmailing/ Threatening Sec 506, 503, 384	Fake News on Social Media Sec 505	Cyber Terrorism sec 66F	Tampering Computer Source	Identity Theft sec 66C	Computer related offence sec 66	Ransom-ware	Offences other than Ransom-ware	Cyber Stalk-ing/Bullying of Women/ Children Sec 354D IPC
Online Banking Frauds	1.000000	0.297261	0.210440	–0.081656	0.297991	–0.029883	0.278153	0.276576	0.322202	0.799312
Cyber Blackmailing/ Threatening Sec 506, 503, 384	0.297261	1.000000	0.472718	0.368497	0.154649	–0.049758	0.156595	0.128745	0.154715	0.300828
Fake News on Social Media Sec 505	0.210440	0.472718	1.000000	0.589458	0.252916	–0.041483	0.231064	0.235354	0.270136	0.205406
Cyber Terrorism sec 66F	-0.081656	0.368497	0.589458	1.000000	0.028105	–0.042616	0.061458	0.034039	0.025907	–0.047158
Tampering Computer Source	0.297991	0.154649	0.252916	0.028105	1.000000	0.065687	0.991130	0.992945	0.937691	0.028343
Identity Theft sec 66C	-0.029883	-0.049758	-0.041483	-0.042616	0.065687	1.000000	0.014784	0.003531	0.074809	0.000353
Computer related of-fence sec 66	0.278153	0.156595	0.231064	0.061458	0.991130	0.014784	1.000000	0.998242	0.955151	0.010488
Ransomware	0.276576	0.128745	0.235354	0.034039	0.992945	0.003531	0.998242	1.000000	0.949917	0.006252
Offences other than Ransomware	0.322202	0.154715	0.270136	0.025907	0.937691	0.074809	0.955151	0.949917	1.000000	0.060779
Cyber Stalking/Bully-ing of Women/Chil-dren Sec 354D IPC	0.799312	0.300828	0.205406	–0.047158	0.028343	0.000353	0.010488	0.006252	0.060779	1.000000

Fig. 9. Correlation Performed

Logistic regression algorithm has a dubious name since in statistics a regression often implies continuous values but logistic regression returns a binary result. The algorithm measures the relationship of each feature and compares them based on their impact on the result. The result and value are then mapped against a curve seen in Fig. (8), which is equivalent to threat or no threat.

```
def     plot_corr(df, size=11):
        """
        Function plots a graphical correlation matrix for each pair of columns
        in the dataframe

        Input:
          df: pandas DataFrame
          size: vertical and horizontal size of the plot

        Displays:
          matrix of correlation between columns. Blue-cyan-yellow-red-darkred
          => less to more correlated
                                          0 ----------------------> 1
                                          Expect a yellow line running from top
                                          left to bottom right
        """

        corr = df.corr()
        fig,ax = plt.subplots(figsize(size, size))
        ax.matshow(corr)
        plt.xticks(range(len(corr.columns)), corr.c olumns)
        plt.yticks(range(len(corr.columns)), corr.c olumns)
        plt.setp(ax.get_xticklabels(), rotation=90, horizontalalignment='right')
```

Fig. 10. Giving the values for correlation

```
In [10]: plot_corr(cyber_data)
```

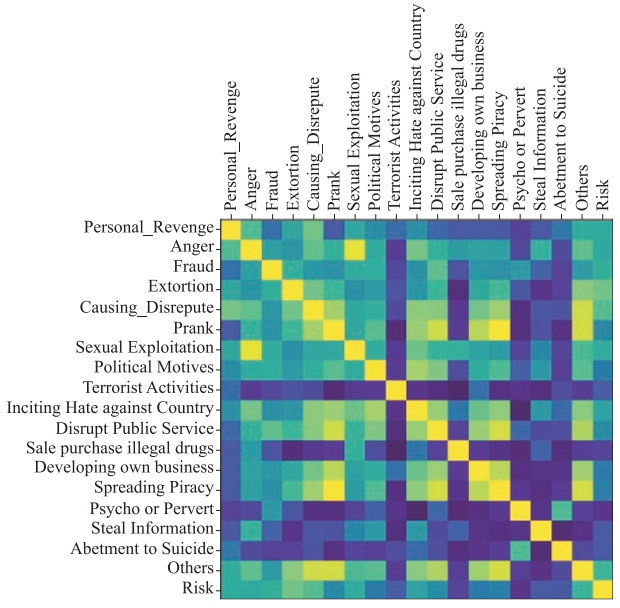

Fig. 11. **Correlation graph**

4. Training the Model

Splitting the cyber data into two sets one for training the model and the other for testing the model, about 70% of the data we have put in the training set and 30% of data in the testing set, after this, we have trained the algorithm with the training data and held the test data aside for evaluation. This training process produces a training model based on the logic in the algorithm and the values of the features in the training data. Care has taken not to use all the data to train since data drives training of the model. The library which handles machine learning, training and evaluation tasks in Python is Scikit learning, it provides a set of simple and efficient tools that can manage many of the tests in machine learning.

Scikit supports machine learning and it is built on Python libraries such as NumPy, SciPy and Matplotlib and supports these and panda's data frames. It is generally a toolset that makes training and evaluation tasks simple; these tasks involve splitting the data into training and test sets, preprocessing data before training, selecting the most important data features, creating train model, tuning the model for better performance.

```
In [11]:  x = cyber_data.drop(['Risk', 'State_UT'], axis=1) # Independent
          Variables
          y = cyber_data[['Risk']]  # Dependent Variable

In [12]:  X.shape

Out [12]: (36, 18)

In [24]:  # Splitting the data into train and test
          X_train, X_test, y_train, y_test = train_test_split(X, y, test_
          size=0.4, random_state=1)

In [14]:  # Building Linear Regression
          reg = LogisticRegression()
          reg.fit(X_train, _train)

          M: \Users\Puneet\anaconda3\lib\site-packages\sklearn\utils\
          validation.py:760: DataConversionWarning: A column-vector y was
          passe d when a 1d array was expected. Please change the shape of y
          to (n_samples, ), for example using ravel().
          y = column_or_1d(y, warn=True)
          M: \Users\ Puneet\anaconda3\lib\site-packages\sklearn\linear_
          model\_logistic.py:940: ConvergenceWarning: 1bfgs failed to
          converge (status=1):
          STOP: TOTAL NO. of ITERATIONS REACHED LIMIT.
```

Fig. 12. Applying regression algorithm

5. Checking the Accuracy

Explanation for code:

Since we know that through our research aimed to predict whether a particular State/UT is at a higher risk of cybercrime when using such variables as Personal revenge, Anger, Fraud, etc. In order to predict this relationship, we have used a statistical technique Logistic Regression. Before we move to modeling, we have to check if there is any correlation between the independent variables, in other words, we have to check if there is a relationship between the independent variables (example Personal revenge, Anger, Fraud etc.). In the correlation plot, we should ignore the diagonal block as the diagonal block in yellow represents the correlation with itself (i.e., Personal revenge and Personal revenge) in which we are not interested. Yellow color represents high correlation, light green color represents moderate correlation, dark green color represents low correlation, and complete dark color represents no correlation. So, from the plot we can say that there is a high correlation between Sexual exploitation and Anger, spreading piracy and prank etc. as if we see the block of these variables in the plot, they are yellow in color. There is a moderate correlation between Spreading piracy and Causing disrepute, Prank and Inciting hate against country etc. as if we see the block of these variables in the plot, they are yellow in color. Similarly, we can say that the variables with darker blocks have less of no correlation. We have divided the data into X and Y where X is the independent variable and y denotes the dependent variable. So are independent variables being Personal revenge, Anger, Fraud, etc. and our dependent variable is risk.

Further checked the shape of X (just a sense check), then divided the variable into train and test, (we will use the X_train and y_train to train the logistic regression model and then test the model using X_test and y_test). Now we have used the function to build a logistic regression model using the data X_train and y_train. We are using this logistic regression when our dependent variable has dichotomous type, i.e., True/False, Absent/Present etc. Now having built a model, we have predicted the expected values of y using X_test. After predicting the expected values for y we will now check the accuracy of the model. The accuracy of the model depends on the number of cases we have predicted correctly, i.e., the number of times we have predicted that the State/UT is at risk. The state was actually at risk and the number of times we have predicted that the State/UT is not at risk and the state was not at risk. As seen in Fig. 11, 12, and 13, we can see that how the model behaves in predicting the accuracy of the threat in the states.

```
Out [14]: LogisticRegression(C=1.0, class_weight=None, dual=False, fit_
          intercept=True,
                    intercept_scaling=1, 11_ratio=None, max_iter=100,
                    multi_class='auto', n_jobs=None, penalty='12',
                    random_state=None, solver='1bfgs', tol=0.0001, verbose=0,
                    warm_start=False)

In  [15]: # Predicting  the cases
          y_pred = reg.predict(X_test)
          y_pred

Out [15]: array([0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0], dtype=int64)

In [18]:  Metrics.accuracy_score(y_test, y_pred)

Out [18]: 0.6666666666666666

In [19]:  cyber_data.head(5)

Out [19]:
```

Causing_ Disrepute	Prank	Sexual Exploitation	Political Motives	Terrorist Activities	Inciting Hate against Country	Disrupt Public Service	Sale purchase illegal drugs	Developing own business	Spreading	Psycho or Pervert	Steal Information	Abetment to Suicide	Others	Risk
7	0	92	12	1	1	1	0	2	14	2	0	1	236	0
0	0	0	0	0	0	0	0	0	0	0	0	0	5	0
234	0	113	9	4	3	0	0	0	0	0	0	0	832	1
0	0	8	0	0	0	0	0	0	0	0	0	0	0	0
25	0	21	4	0	1	0	0	1	0	0	0	0	61	0

Fig. 13. Model predicting the accuracy

Conclusion

Through the study above, we can conclude that by trial and error of various algorithms, we could draw some crucial points with the help of the Logistic Regression Algorithm. This research would surely help the law enforcement agencies understand the root cause of the crime as if there was any political movement, natural crisis, or else massive dropouts in the particular state which led to a person committing the crime. As we cannot rely on this model completely in sentencing the accused, his/her parenting, upbringing, society, and teachings should also be gone through to understand the reason behind committing the crime, as we all know the law enforcement agencies or government can only bestow law upon us. Still, the root cause of this crime should be found out and eradicated. The bigger question is, how will technology shape the judicial function, and to what extent [Sourdin T., 2018. Judge v. Robot: Artificial Intelligence and Judicial Decision-Making. UNSWLJ, 41, pp: 1114], but it will surely benefit the judiciary system in

some or other way. The various sectors can benefit from this new technology provided that it is not used for somebody's harm for it to behave in unpredicted and potentially harmful ways [Cath C., 2018: 1–8]. Thus, the proper judicial monitoring of data fed can enjoy this model's beauty.

References

Alarie B., Niblett A. & Yoon A. (2018) How artificial intelligence will affect the practice of law. *University of Toronto Law Journal*, vol. 68, supplement 1, pp. 106–124.

Caldwell M. et al (2020) AI-enabled future crime. *Crime Science*, no 1, pp. 1–13.

Cath C. (2018) Governing artificial intelligence: ethical, legal and technical opportunities and challenges. *Phil.Trans. Royal. Society*, issue 2133, pp. 1–8.

Chen H. et al (2003) COPLINK Connect: information and knowledge management for law enforcement. *Decision support systems*, no 3, pp. 271–285.

Cui Y. (2020) Building AI-assisted rule of law for the future, seeking advantages and avoiding disadvantages to make AI better benefit mankind. In: *Artificial Intelligence and Judicial Modernization*. Singapore: Springer, pp. 187–191.

Dhillon K. (2011) The police and the criminal justice system in India. *The Police, State, and Society: Perspectives from India and France*. Pearson, pp. 27–59.

Dmitrik N. (2020) Digital State, Digital Citizen: Making Fair and Effective Rules for a Digital World. *Legal Issues in the Digital Age*, no 1, pp. 54–78.

Furtado V. et al (2010) Collective intelligence in law enforcement–The WikiCrimes system. *Information Sciences*, no 1, pp. 4–17.

Hauck R. et al (2002) Using Coplink to analyze criminal-justice data. *Computer*, no 3, pp. 30–37.

Hayward K., Maas M. (2020) Artificial intelligence and crime: A primer for criminologists. *Crime, Media, Culture*, pp. 1–25.

Isaac W. (2017) Hope, hype, and fear: the promise and potential pitfalls of artificial intelligence in criminal justice. *Ohio St. J. Crim.* L., vol. 15, p. 543.

King T., Aggarwal N., Taddeo M., Floridi L. (2020) Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and engineering ethics*, no 1, pp. 89–120.

Marda V. (2018) Artificial intelligence policy in India: a framework for engaging the limits of data-driven decision-making. *Philosophical Transactions of the Royal Society: Mathematical, Physical and Engineering Sciences*, vol. 376, pp. 1–19.

McCarthy J. et al (2006) A proposal for the Dartmouth summer research project on artificial intelligence. *AI magazine*, no 4, pp. 12–14.

McGuire M., Holt T. (eds.) (2017) The Routledge Handbook of Technology, Crime and Justice. L.: Taylor & Francis, pp. 1–722.

Nath S. (2006) Crime pattern detection using data mining. In: 2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent, pp. 41–44.

Perkel J. (2018) Why Jupyter is data scientists' computational notebook of choice. *Nature*, vol. 563, pp. 145–147.

Raschka S. et al (2020) Machine Learning in Python: Main developments and technology trends in data science, machine learning, and artificial intelligence. *Information*, no 4, p. 193.

Sourdin T. (2018) Judge v. Robot: Artificial Intelligence and Judicial Decision-Making. UNSW *Law Journal*, vol. 41, pp. 11–14.

Završnik A. (2020) Criminal justice, artificial intelligence systems, and human rights. *ERA Forum Springer*, no 4, pp. 567–583.

Expression Through Socialising Media in India: Why Fixing the Existing Legal Dilemmas Is Critical?

Meera Mathew

Assistant Professor, Symbiosis Law School, Deemed University, PhD. Address: NOIDA Sec-62, Block-A, 47 & 48, NOIDA (PIN-201301), Uttar Pradesh, India. E-mail: meera@symlaw.edu.in

Abstract

The emergence of the social media and its virtual communication space has enabled people at large to interact and communicate from the conventional mode of one-to-one to many-to-many. It exploded onto the technology in the last decades for commercial and entertainment purpose and rapidly it had become very much prevalent globally. Initiated as a friend-finder it went on to the extend encompassing every features of media where the users had a dominant role. When mass media and digital media was through certain modes, social media not only changed the mode but the creators and audience. From passive news listeners, it became active creators and sharers of contents in the form of information. With the enablement of technology, anybody with an internet access and own opinion can be part of social media. Under the guise of user-generated content, be it in sharing of news or opinion or images or videos and now even the live video promoting political, social, cultural aspects, social media do not hold any accountability because only users are producing contents. Also, being an intermediary, it is free from any liability for the user generated data under Indian Information Technology Act, 2008 and the existing global consensus under safe harbour doctrine. The law in this area is still relatively unsettled. The misuse of social media got reported with various incidents of such as impersonation, anonymity, profile account hacking, privacy threats, sexual or aggressive solicitation, cyber-bullying, and many such related serious issues. However, in all these matters, social media was provided with a benefit for its passive involvement of choosing the users or the contents posted. The liability was always on the content producers. It is certain degree of due diligence social media platform needs to observe that too very minimal! This paper endeavours to question the existing privilege available to social media at par with conventional media and also highlights the social-legal dilemma it put forth with unprecedented use of data. It further dwells upon the legal impediments in challenges that social media pose for the lack of legislation- especially for data protection and user profile anonymity detection. It thus attempts to find out whether social media is to be equated like media or should it be viewed as mere platform for people to express. If it is just a platform to express, whether the current Indian legal framework is sufficient enough, to deal with the ramifications arising out of social media especially when most of them are social media companies incorporated and registered under foreign jurisdictions.

Keywords
expression, social media, legal issues, Indian legal system, Information technology.

For citation: Meera M. (2020) Expression through "Socialising" Media in India: Why Fixing the Existing Legal Dilemmas is Critical? // Legal Issues in the Digital Age, no 3, pp. 97–124.

DOI: 10.17323/2713-2749.2020.3.97.124

Introduction

The internet service websites, blog pages, mobile technologies, social media and networking sites web have entirely altered previously prevailed communication model. The internet, digitalization and social media are transforming news from its traditional practice from its original notions of press and media. The degree at which exchange of communication existed had been multi-folded with sudden increase in information collected and circulated. Today every news-media has its social media webpage including *Twitter* handles or *Facebook* pages thus stories are searched on internet service providers to know if any user has uploaded anything that became 'viral'. Moreover, it has become a necessity for mainstream print media to have their websites, live videos, journalists' blogs, invited newsrooms debates where invitation is extended to community participation [Knutson A., 2009: 437–474].

The bloggers consider themselves as journalists and break *scoops* and stories. With notable shift to mobile news access news has now become omnipresent-available on every platform at any time. Regardless of their professions, resources or training today, *netizens* are disseminating news to the public themselves. Personalized and participatory stories having maximum views or shares are now converted as news.

Further the technological changes and ongoing perception of news", its practices of reporting are greatly influencing at its quantity, quality and nature of reporting, whether online or in print. While print media still have a noteworthy readership, the digital media and new media sites have clearly had a fading impact on the print medium. Social media has divulged in innovative ways to interconnect and collaborate the population through technology. Smart-phones and tablets have redefined customer computing and provide instantaneous access to information from any locality. For instance, observe the development and muti-fold uses of a smart phone [McPeak A., 2015: 235–292]. On it, one can listen to music, phone people, text, watch videos, send and receive emails, surf the internet, play games, watch videos, store pictures and plan the travel with calendar and many other things. Instead of carrying disc-man, walk-man, laptop, diary, camera, telephone today all in one is possible. This is the convergence where all contents and in-

formation is carried by one tool [De Sola P., 1983: 76]. The much notable characteristic of social media is the upsurge in 'citizen journalism', under which individuals determine what could be the news and accordingly publish it via blog or platforms and disseminate the same unlike the earlier prevalent mainstream journalism. This has created a discrepancy in the online communication (often equated to 'chatting' from one to one) the social communication where (any tweet or Facebook post is as much a publication as a newspaper article from one to many or many to many). The commencement of an online-based 'activism' accompanied by the Web 2.0 technology conveys an occasion for its collaborating platform, includes blogs and social network sites an online skill for users to stimulate a profile — public or semi-public, with a view to network with other whom they share a conjoint relationship, and traverse others' profiles and networks. This content creation can turn out to be adverse, menacing or can have a prospective to stir up a rebellion.

The internet as a whole and social media in particular exaggerate the possibility for contents to initiate riot just by taking the circumstances out of the background and using it or even manipulatively generating it. Similarly, it is to be seen how far the privacy constraints are trespassed. Unlike the normal media, it is perplexing for the mass dynamics to enforce a similar controlling impact on social media, which goes on to another argument for why social media need to be regulated like traditional mass media. Apart from that, safe-harbor provisions where limited liability prevails for Internet intermediaries exists to be eroding the notion of traditional news media. Debates on this limited liability though raise confusion, intermediaries moot that they cannot control or regulate content online and therefore should only have restricted accountability. Given the mass quantity of data they handle, social media platforms mainly rely on report notifications from users who raise about the content if it deems misleading or unbefitting. There exists diverse global regime worldwide to determine the liability, with various impact [Stacy A., 2017: 1375]. This lack of unanimity in determining Intermediary liability is again an issue when it is a foreign company functioning in various jurisdictions having different legal scenario. Hence this necessitates to discover the issues and challenges involved in social media and examine how far Indian legal framework tried to fill the gap created by these issues. Also the case studies are done so as to analyze how other countries have done their best to resolve the same.

1. Legal Issues

1.1. Hate Speech or Inciting Posts/ Mob lynching

Speech that provokes or generates animosity adds to target, downgrade and dehumanize specific groups, resulting them to be in sidelined whereby society gets

stratified and divided. The risk of inciting speech is linked to that posed by the very crime in promoting speech. While hateful-speech cases happens in all categories of media, and should be preserved the same irrespective of the medium, the existence of the Internet, especially social media makes a difference here. There is no unanimously recognized account on hate speech. Besides, a direct association — ethical and legal consequences — cannot be recognized between the dissemination of hate speech and violence. For the very term hate makes it a subtle notion and exposed to precise exposition. It is a concept that creates misunderstanding and, given its actual nature, is temperately easy to control[1]. This makes new media to control all the writings based on hate speech.

In India the provisions to curb hate speech are laid down in different way. Under Indian Constitution, interests of the sovereignty and integrity of India", the security of the State", friendly relations with foreign states", public order", decency or morality or in relation to contempt of court", defamation or incitement to an offence are the aspects under which Art. 19(2) are applied where freedom of speech can be restricted. Apart from this, Indian Penal Code has specific sections along with specific provisions under the"Scheduled Castes and Scheduled Tribes (Prevention of Atrocities) Act, 1989; Protection of Civil Rights Act, 1955;"Indecent Representation of Women (Prohibition) Act, 1986; The Religious Institutions (Prevention of Misuse) Act, 1988; The National Security Act, 1980 etc Further there are certain specific media laws that govern hate speech that are even applicable to digital media. Despite blocking access to content under Section 69A[2], takedown of content under Section 79 of IT Act[3], 2008 and other modes of self-regulation policies are prevailing.

The question is whether the principles as adopted in offline media is to be the same for online media? The content flowing through internet-facilitated mobile phones and on social media, has reconfigured the technique in which the law, police, and civil society have coped with this issue[4]. The multinational flow of in-

[1] Law Commission of India."267th Report of Hate Speech. Delhi, 2017."

[2] S. 69 A, IT Act, 2000 states: Intermediaries failing to comply with the direction issued could be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine."

[3] S. 79, IT Act, 2000 exempts intermediaries from liability in certain instances. It states that intermediaries will not be liable for any third party information, data or communication link made available by them.

[4] See S. Narain. Social media, violence and the law: Objectionable material and the Changing Contours of Hate Speech Regulation in India. *Culture Unbound*, 2018, no 3, p. 388–404. The cases of communal violence reported in India such as in Pune in 2014, in *Muzaffarnagar* in 2013, the issues cropped up at *Azad Maidan*, Mumbai in 2012, and the emigration of persons from the North-East states from cities such as Bangalore and Pune in 2012, show that the police have charged, arrested or even acknowledged those liable for acts of vehemence or making confrontational dialogues, but

formation, the effortlessness of inter-platform interchange, and the pace and scale with which information move, has challenged the conventional fact-finding and investigation procedure for police force.

The hate speech and its repercussions were first discussed exhaustively in 1919 *Schenck case*[5], where Judge J. Holmes made a difference between speech having malicious formation and speech with unintended result. By interpreting constitutional protections and dealing with the extend of harm speech can cause by elucidating proximity and degree, the"doctrine of clear and present danger test was formulated. This test though used in cases later reformulated in *Brandenburg* case, which focuses on imminent lawless action test[6]. The protections of this test, when applicable, have proven very difficult to overcome. Recently, this provision was interpreted by the US Supreme Court ruled in the case of *Anthony Elonis*[7]. With United States having a history of liberal speech with no apparent Constitutional restrictions, the judgment was merely a proposal to draw a distinction between regulating the manner of speech, as distinct from its matter!

When the offline media has been switched over to offline media, whether the same theories and principles exist is a matter of concern. Social media having the capacity to instantaneously spread messages to the crowds, unhindered by time or space, it is to be viewed seriously by law makers. Online activism can be in the method of advocacy or mobilization but there exists a thin line from advocacy to incitement. These multi-ford issues that hate speech inflicts on its targets and ap-

---

have not been competent to track dangerous speech disseminating as videos, images or text to a certain source.

[5] *Schenck* v. *United States*, 249 U.S. 47 (1919)

[6] In this, the Court held: Freedoms of speech and press do not permit a State to forbid advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action. Thus, governmental restriction on Brandenburg's speech was held unconstitutional.

[7] For more read: the case *A. Elonis* v. *United States* 135 S. Ct. 2001 (2015)". In this case, after his wife and children moved out of their home, Anthony Elonis made various postings on the internet that caused others to fear for their physical safety."Under this, the Pennsylvania amusement-park worker who took to Facebook to post violent rap lyrics aimed at his estranged wife, co-workers and the FBI agents who came to investigate him. Under the pseudonym 'Tone Dougie', Elonis went online to vent, penning lyrics such as: 'There's one way to love you but a thousand ways to kill you… Hurry up and die, bitch, so I can bust this nut all over your corpse.' The Supreme Court ruled that the original court case, which saw Elonis convicted for making online 'interstate threats', did not sufficiently prove that he intended for the posts to be threatening — an important requirement for him to be found guilty. Though circuit court found him guilty under under 18 U.S.C. § 875(c), Supreme Court did not. The Supreme Court failed to deal with the issue whether incitement and threats are subject to the same constitutional protections and, if not, why not. Further, the Court might have described the kind of subjective intent required before one could be prosecuted for either incitement or threats. Regrettably, the Court shed very little light on these constitutional questions, and its statutory analysis offered too little direction to be helpful for lower court.

propriately explains that the menace of hate speech should be weighed against the prevalent societal, cultural and the historical environment. In *Pravasi Bhalai Sangathan* case[8], the Supreme Court had examined the 'tendency' and the 'proximity' tests involved in speech and expression but left it without describing or defining the hate speech considering it as judicial overreach. Contrary to the protected and responsible speech as reflected under Freedom of speech and Right to life[9], some expressions and speech are intended to demean, overawe, or inflame violence or prejudicial action against a group of people. Finally with the Law Commission in its Report-267 stated that, certain parameters on identifying hate speech are extremity of the speech, status of the author, contents delivered, status of the victims, potentiality and context in which the speech was delieverd[10].

Coming to Mob Lynching, the statistics imply that, many are reported to have been killed in in the past few months in barbarousness fueled by *WhatsApp* messages[11]. Lynchings can be defined as extra-legal murders executed by a bunch of vigilantes who act like observants taking law in hand and with no justification kill individuals often accused of outrageous crimes. The objective behind lynching is to punish particular criminals and crimes but indirectly it also passes an unrighteous message to public to have social conformity with moral norms be it on social hierarchy, status, and gender behaviours[12]. The recent judgment of *Tehseen Poonawalla* v *Union of India and Ors*[13] where the three-Judge Bench of the Supreme Court headed by C.J. Dipak Misra had recognized the act of lynching as unlawful and in the light of growing instances of mob lynchings increased by misinformation arising out of social media messages.

This leads to the conclusion that Information being a vital element to society its distortion will have violent implications. Right to participate and right to disseminate are different. When right to participate is an affirmative right that is vested with citizens under the realm of right to know through access to certain governmental information, right to disseminate comes with inherent responsibil-

[8] *Pravasi Bhalai Sangathan v. Union of India* 2014 SCC OnLine SC 22. Available at https://main.sci.gov.in/jonew/judis/41312.pdf (accessed 03.10.2020)

[9] To be read with Article 19(2) on the grounds of public order, incitement to offence and security of the State."

[10] Law Commission of India, 267th report on Hate Speech (March, 2017)."LCI suggested for an Amendment in IPC to insert new section 153C (Prohibiting incitement to hatred) and section 505A (Causing fear, alarm, or provocation of violence in certain cases)."

[11] "Since 2017 *WhatsApp* misinformation has contributed to more than 80 different lynching incidents across India See BBC news report 12 November 2018. Available at: bbc.co.uk/mediacentre/duty-identity-credibility.pdf (accessed: 10.12.2019)

[12] Salam Z. *Lynch Files: The Forgotten Saga of Victims of Hate Crime.* SAGE, 2019, p. 120–130.

[13] Writ Petition (Civil) No. 754 of 2016.

ity. With social media, those barriers are falling and suddenly platforms generousness is helping ordinary citizens create new enterprises of all kinds. Many a times, public association in such lynchings happen due to random, silly and trivial reasons. However when the substantial law when interpreted in procedural aspects, it usually gets watered down for its strict interpretations. Ideally, for a speaker to be prosecuted for incitement, therefore, the State must show:"(i) The perpetrator/s having intention to incite another; (ii) The perpetrator/s have done something actively to cause imminent violence; and (iii) The perpetrators' overt acts were in a context that makes possible that such violence will occur.

With the criminal law interpretation of proving beyond reasonable doubt and *mensrea* to be specifically proved, it has lot of shortcomings. Secondly blocking of content online is used often to prevent the circulation of online hate speech. The process of issuing blocking orders is ambiguous, and the reasoning offered in orders is not subject to public scrutiny. This lack of transparency means there are few avenues available for the public to hold the executive accountable for misuse of its power to block online content. With the online media working under the self-regulation principle[14], what it can be done to improve the scenario to have a uniform policy for all the social media. For instance, in *WhatsApp*, the terms of use do provide that a user account, or access to the account may be modified, suspended or terminated for any reasons, including violation of the 'letter or spirit' of the terms. It also states that 'creation of harm, risk, or possible legal exposure' for *WhatsApp* can lead to the modification, suspension or termination. However, there is no reporting or other enforcement mechanism specific to 'hate speech'[15].

1.2. Jurisdiction

In the common law method, the application of jurisdiction had been founded on where the dispute is governed. With the digital media and social media the main concern was on how to govern the matters when affected parties are from different jurisdiction. The transnational nature of cyberspace, globalization of the Internet and the inapplicability of territorial jurisdiction has been challenging for nations vexing to implement at their laws in cyberspace. The past principles of *forum conveniens* or *forum non conveniens,* traditional state sovereignty, the juris-

[14] For instance, many social media in its policy advertisements prohibits 'hate speech' on race, ethnicity, national origin, colour, religion, disability, age, sex, sexual orientation, gender identity, veteran status or other protected status, inflammatory content which is likely to evoke a strong negative reaction or cause harm. See T Gelashvili, *Hate Speech on Social Media: Implications of Private Regulation And Governance Gaps* Lund, 2018, p. 27.

[15] WhatsApp Legal Info — Key Updates. Available at: https://www.whatsapp.com/legal/# key-updates (accessed: 30.09.2018)

diction concerning content hosted and passed on the internet, regulation of free flowing content on borders were the concerns. When the foreign registered company, provides Internet users with access to various services beyond geographic boundaries the applicability of laws and regulations was a challenge

Jurisdiction denotes the dominion of a court to listen to a matter and determine the case. Deprived of jurisdiction, a court's finding becomes futile and powerless. The Internet generates uncertainty for sovereign territory since system restrictions traverse and surpass state boundaries. Under international law 'jurisdiction' is sometimes referred to as the law of 'extraterritorial' jurisdiction. The extraterritoriality also poses a challenge for judicial cooperation, in as much as legislative differences also affect very important questions relating to cyber-crime, such as data protection and communications secrecy. Additionally, it poses difficulties that arise from the technical conformation and functionality of the Internet (such as on server setting, IP validation, various encrypting dealings for concealing identity from spam outbreaks, etc.) that causes a number of indecisions and complications in procuring evidence or outlining accountability.

Even trans-boundary defamation upsurges a range of concerns, especially the private international law demands about which courts should adjudge matters and what would be the applicable law. A defamatory statement if appears online it can be published wherever internet is accessible. The decision of a French trial Court to *Yahoo Inc*. to install filtering system to avoid people from offering to sell Nazi Symbols thereby hurting the sentiments of German people was significant for the jurisdiction[16]. In its initial ruling this trial court held that the U.S. website for Yahoo Inc. can be made answerable to French jurisdiction because it could be accessed from German people in France. The issues arose for its divergent legality existed in different jurisdictions. In USA, the sale of *Nazi* Items are protected under First Amendment. Where as in France such sales are prohibited under Article R 645-1 of the French Penal Code. These challenges of overlapping jurisdiction advances these complex questions: With the cross-border aspect of internet, is there any universal doctrines or theories that may prevail over and which court will have jurisdiction? How far any sovereign national government can assert the application of its laws and regulations to any Internet activities that has its primary activity originated from a different jurisdiction? Conventionally there exists three fold approach one as *Prescriptive jurisdiction* second as *Adjudicative jurisdiction* and the third as *Enforcement jurisdiction*.

[16] See:"*Yahoo! Inc.* v. *La Ligue Contre Le Racisme et L'Antisemitisme*, 145 F. Supp. 2d 1168, 1171 (N.D. Cal. 2001). In this case Yahoo Auctions, being one of the applications offered through the Service allowed its users to communicate through the use of the Service, to buy and sell items in an online auction, where Nazi memorabilia was also found as auction items."

Today when different parties and their nationalities are in question, there are certain presumptions pertaining to jurisdiction that the courts apply. In normal cases the court applies the general jurisdiction by applying the long-arm rule by stretching it over parties in other states to examine if the necessities in statute have been met and whether or not the application of jurisdiction would infringe the defendant's due process rights. In other words, a municipal court can exercise personal jurisdiction over a non-resident defendant-be it a company or corporation, only so long as there exist 'minimum contacts' between the other party and his or her nation State. When the court cannot apply general jurisdiction, the court will search for specific jurisdiction and accordingly it will be applied, for instance section 75 of the Information Technology Act deals with extraterritorial principle[17]. In the infamous incident of *Blue-whale challenge* as well, the effects doctrine was applied holding the administrator of a group or a community page responsible for their acts committed from one state or country, into another state's victim[18].

1.3. Curtailment to Right to Privacy

There exists a blurry line between the public and private sphere where one cannot state what constitutes public and private information. Also, with the unprecedented dissemination of information on social media websites there also lie the difficulties in defining sensitive personal information *vs*. Personal information, and this consistently has repercussions upon user's privacy. An enormous bulk of social networking sites fixed a certain privacy background as default so that everybody can view a person's record unless privacy settings are clearly altered. Information tracking mechanisms exist in many websites and advertising companies. Users' own favourites, behaviours and routine are easy to be pursued whenever a user log on to the internet he/she outrun a mechanized trail. This information is beneficial in corporate marketing especially in promotions that aim the individual customer. If a user logs on to any online shopping store for example myntra.com, then by default that user will get recommendations of such similar websites and in e-mail get hot offers from myntra.com. This condition leads to a rational conclusion that somewhere social networking sites are involving users' personal information for revenue purposes. Additional aspect of privacy infringement in social networks is the lasting accessibility of user's information to anyone. Even if user deletes the profile, the social media company still retains the data.

[17] *Karmanya Singh Sareen and Anr.* v. *Union of India* Writ Petition (C) No. 7663/2016] on 23.09.2016

[18] Rosenblatt B. Principles of Jurisdiction. Available at*:* http://cyber.law.harvard.edu/property99/domain/Betsy.html (accessed: 03.09.2019)

Safeguarding the privacy mandates isolation from unwanted publicity. This wish to embrace something personal often seems to be in clash with freedom of expression.

The frequent challenge between privacy and free speech thus fails to strike stability among the two competing interests". Therefore, at times, privacy is quoted as 'sweeping concept' by jurists and with the social media, there is no overarching conception of privacy. The jurisprudential principle on which privacy rights vest is often connoted as informational autonomy that implies the right to control the flow of information about oneself"[19]. However there are certain blurred areas where privacy right cannot be determined. For instance: (i) Can an individual in public space demand privacy? (ii) Can a public person demand for same privacy as any other infamous person? (iii) Can an exposed information be withdrawn in the name of privacy? (iv) Can privacy right be protected after the exposure of the private data? (v) Can truth be a defense in privacy right validation like defamation matters?

Thus it can be seen that the periphery of private or personal seems clouding and with technological advancement one cannot reasonable have privacy. Everyone's life is tracked and revealed. The argument in support of free speech would be sustained by the significance of the speech in terms of the public interest it serves."Accordingly, when personal information placed is watched in public space, human dignity is despoiled regardless of the public reaction to that information. It is therefore suggested that if the main aim is the right to privacy, revelation of private facts would be warranted only if it is outweighed or overridden by a public awareness in revelation [Birks P., 1997: 65].

The inspiration to provide readers with the most meticulous detail about the private lives of celebrities and public figures is definitely not a newsworthy information. Against this background, it is essential therefore that privacy law provides practical and effective protection if it is to respond to the examples cited above.

There can be a number of instances of privacy infringement in offline mode. Gazing at one's window at home that faces the dining table — In this window being a space to a room cannot be termed s public space. Same is the case with a car parked on road. Road may be a public space, but the car parked and the space within the car is private space. Gazing once by default and looking there several times to get any information are different. Listening to private conversations happening over the telephone is definitely an intrusion to privacy. It is for that reason the Supreme Court stated that phone tapping is a breach to privacy

[19] *See*, P. Regan. *Legislating Privacy: Technology, Social Values, and Public Policy.* University of North Carolina Press, 1995, p. 85–89.

right[20]. Similarly is the snooping at a profile in social media. The activities of a person that appear on newsfeed is different from being checked every time. These instances reveal that a there are certain moral conditions inevitable for invasion of privacy[21]. Privacy, as a result consists of access to an individual's information or any information concerning him [Rachels J., 1975: 323]. Every individual ought to disclose certain aspects of his private life and does not expect a loss of privacy on the ground that others gain access to him. If he chooses to allow himself any information to go public, then he cannot complain about privacy. But if he chooses not to allow others gaining access to his personal activities or information, any intrusion or a disclosure of his personal data would violate his right of privacy.

True that,"with the onset of web 2.0 and social media, individuals are facilitated to publish on computer networks without revealing their true identity. With the social media's unlimited search and memory capacity, even minute particulars of personal information can have a gigantic bearing, even years after they were shared or made public. It cannot be equalized to normal speech theories as to promote truth, political and social participation and self-fulfilment. Rather, this unauthorized access to personal information to large groups of people invites the harm.

Social media, in its original format, was not considered with privacy measures rather it was about divulging, involving, connecting, and access to information. With the *Camridge Analytica* exposure, it is felt that data about each of the users, held by third party stakeholders, is proliferating. The essential aspect informational privacy, in a world inundated in data, has become a matter of concern. The control over one's information as privacy is not a new origination that means limiting unrestrained usage of one's information -by protecting from undesirable usage of information about oneself. It is the skill to hold oneself -in the form of information — from unpredicted use of that information -such as by law enforcement, professional opponents, or even family members, characterized against or produced by marketers and others who classify all about oneself. This notion of safeguarding information about oneself from causing maltreatment is the main thrust behind core notions of privacy exemplified in the judicial clarification of privacy through various ground-breaking judgments.

1.4. Changing Privacy Policies and Setting

Many social media websites keep changing the policies and install new features in the websites without giving due notifications to the users. Social media web-

[20] *PUCL* v. *UOI* (1997) 1 SCC 301.

[21] Hong Kong Law Reform Commission, Consultation Paper on Stalking (Apr.,1998).

sites are the hub of collection of private user information that can infringe upon a user's privacy rights if no sufficient steps are taken while introducing new features. Many of these policies are highlighted only when user reads in the privacy settings or policy settings. There initially it was mentioned that the website owner obtains the rights to use and distribute the users' private information". Devoid of providing any reasonable notice, the terms of the exchange between the user and the social media website had been constantly changing and being presented with new features and services including the advertisements, Beacon[22], Newsfeed and Platform. This consequently has been leading to default modification in the privacy settings and the privacy policy. The algorithms and technology of social media drive the margins of disclosure—both voluntary and involuntary—along with privacy policy in the terms and condition. With the emerging trend to log in to all social media websites and apps with websites also letting the sites to access the data results in invasion to privacy [Gavison R., 1980: 421].

With the changing realms of the public and private and considering those as relative terms and shift according to individual perspectives, defining the privacy policies in social media platform is difficult. Additionally there is no supervisory system as it works under the principle of self-regulation. Necessary to have privacy is not about trying something to hide. It is about calling for safeguarding the control of one self. This is the self-regulatory regime with definite policies. Thus can be seen that many of these issues deal with the questions of: (a) Whether the effect by way of harm is to happen to create safeguard for infringement of privacy? (b) Whether 'private' refers to a category distinct from confidential? and (c) Whether privacy revelations have any safeguard under right to freedom of expression? It is the need of the hour to view privacy as protecting one's identity. By safeguarding against revelation of the information, the discrimination can be prevented, providing a kind of remedy in anticipation of the harm[23]".

1.5. Identity Theft

Identity theft is when a person fraudulently attains and operates in someone else's character. Thereby one 'appropriates' another's identity and uses it without consent. From social media, once the network circle is understood, spamming and phishing are done and thereby spam emails are composed to potential targets.

[22] Hashemi Y. Facebook's Privacy Policy and Its Third-Party Partnerships Lucrativity and Liability. *Boston University Journal of Science*, 2009, no 15, p. 159.

[23] Prominent privacy scholar Anita Allen suggests that there has been the rapid erosion of expectations of personal privacy **...** people expect increasingly little physical, informational, and proprietary privacy, and **...** prefer less of these types of privacy relative to other goods. See generally Allen A. Coercing Privacy. *Wm. & Mary L. Rev*. 1999, vol. 40, p. 729–730.

The emails composed in such manner randomly avail information such as Social Security Number, bank account details, etc. Social media seek such information that can identify users and its privacy settings allows users to select how the information can be used. Users have the choice to take in location information with their posts which will be stored to provide features for services. Once user gives the location and geographical place, then user will start receive new trends, stories, ads and suggestions for people to follow. Such feeds are helpful for the perpetrators to do identity theft and do the transactions through social media with spamming and the phishing.

1.6. User Tracking and Cookie

'Cookie' is a term developed from HTTP cookies to track the general visitors to website in order to trace how often the persons visit were developed so a site could generally identify a visitor and keep track of how many times one visited the website. They are minutes of data stockpiled in browsers. Such information had been used for direct promotion programmes that target the individual customer. Such general information collection soon advanced as the past browsing behaviour of the visitors' within a site, and also use the personal information willingly provided while registering for the content. Currently, it is a general trend for most of the websites and advertising companies to track user as he or she leaves behind an electronic trail. For instance, if one individual visits a website, the website via cookie acknowledges that individual as user A. If that person leaves the site and then browse the site once more, the cookie information stored in the website will recognize that A is the same user who was browsing the site previously. The area of concern is when an unapproved website uses any user/visitors details for proxy and initiates attack by conferring fabricated gathering of data to and take up the user's activity. Many social media have acknowledged the prevalence of cookies in their websites. Additional part of privacy infringement in social media is the permanent obtainability of any user's information to other users. Many social media servers have permanently keep the user account even though the user deletes complete information of account.

1.7. Default Search Result

"Initially the users' profiles were openly available as default search by non-user on many social media. By this, anyone not being on social media could also trace 'users' names, profile photos, address book, list of friends and even the pages which they are member in or even the places they checked in and so on. However with various criticisms from all over the world, they did change the settings. Even

then there are various social media such as *Linkedin*, *Google Plus*, *Academia.edu. in* where users' profiles are traceable with public search option."The arguments debunking the privacy on FB revolve around the rationale that users key-in the information, and it is a social networking site, hence users waive of their privacy by taking part in such networking and being a part of social media". To address this, the best case judgment would be of *Y.G. v. Jewish Hospital of St. Louis*[24], a couple incapable to conceive a child endured *in vitro* fertilization at the opposite party hospital. The process was effective however they had decided to keep it confidential for personal reasons like- disclosing their involvement would affect the religiously-especially when church condemned the practice. Hence only the hospital authorities and their very near relatives knew of the couple's participation in the *in vitro* program. However, the issues cropped up when the couple was invited by the hospital's successful fertility programme for which they got clicked by a camera crew. After the transmission of this program, the couple was traced and they stated that media breached their privacy right. The question was if any reasonable foreseeability existed for their breach of privacy? The court disallowed this contention, holding that being present in the party within hospital invitees clearly meant that the couple chose to disclose their involvement to only the other *in vitro* couples. This case is an example of stating that privacy right and letting the information go out of one's hand is not within the concerned person's limit. How much ever precautions one takes, certain information may go out of reach and in such case the other party has to be made liable.

1.8. Anonymity

The prevalence of anonymity in onsite medium is occasionally applauded for it enhancing the freedom of online communication. Anonymity however gives perpetrators opportunities to commit unwanted activities under the mask. Anonymity revitalises embarrassments and can lead to uncommon doings thereby it can lead to misbehaviour, for instance harsh or rude language and acts that are critical or dangerous. With each computer portal to the web holding a unique Internet Protocol (IP) address that is logged every time a user visits a website, one's anonymity is nearly always traceable. However certain damages caused by anonymous user can be irretrievable. Anonymous services are often taken as advantageous by perpetrators and that can affect safety and security at large. If activities are done in idiosyncratic or outwardly performed for fun or amusement, it should not be tracked. But the kind of communal, hate messages or misinformation generated by anonymous profiles are detrimental in nature.

[24] 795 S.W.2d at 502.

"Currently, under the civil litigation, the legal system provides for a remedy in lawsuit and it is known as a *John Doe* lawsuit. Under this the complainant can lodge the plaint by suing an"unknown defendant."The best example of anonymity is the case of Rahul Pashupal and his wife Reshmi for launching the webpage and Facebook by label *Kochusundarikal* depicting pornographic images of minor girls along with others, with abusive and sexual comments and made wide circulation in social network and made advertisements through the Internet[25]. There are reports that assert that marriages of women victims were blocked due to their online victimization[26]. However many women at this instance choose to endure these pains without reporting petrified of social stigma[27]. When cyber-crime strikes, persons take it individually and essentially blame themselves for some cases of cyber-crime. Even when it comes to online pestering or being approached by a sexual predator, some victims yet blame themselves. There are certain profiles creates by anonymous people and track certain people and to find the whereabouts. There are cases reported where thieves see a status update of a family being on holiday for a lengthy period of time and jump at the perfect opportunity to steal some valuables."

1.9. Cyber Bullying and Trolls

In India, there is IT Act of 2000, amended in 2008 that deals with cyber bullying under Section 67. However there are certain loopholes, especially when bullying has become rampant among school going teenagers. Targeting a person and harassing and embarrassing to negative, aggressive, and mean-spirited objectives are condemned for the repercussions it will have. With the prevalence of social media, the creation of web-page within social networking sites depicting pornographic pictures of minor children, with abusive and sexual comments and was circulated among the public widely is also widespread. Additionally, social media facilitated the rising number of bullying. There are various cases reported about bullying. The social-media page or web-links are created by student-administrators by name confessions are increasingly reported as bullying platform[28]. Apparently various colleges, schools with batch division number have these confession pages. The ac-

[25] *See* Crime No. 34/2015 of Cyber Crime (Case against Rahul Pasupal procuring the minor girls for the purpose of sexual abuse and was a part of a racket involved in the trafficking of minor girls for sexual abuse having wide B.A.Nos.866 of 2016 and 867 of 2016 2 spread roots through out Kerala and even outside.)

[26] *See* J. Finn & M. Banach. Victimization online: The downside of seeking human services for women on the internet. *Cyber Psychology & Behaviour,* 2000*, no 3,* p. 785–796.

[27] Human Rights Watch,'Events of 2018' Available at: https://www.hrw.org/world-report/ 2019/ country-chapters/india (accessed: 22.05.2019)

[28] Gowri M. Confessions or Cyber-Bullying. *The Hindu*. 4 July 2013.

cess and admittance is possible with administrator who stays anonymous when grant the entry pass to the requested ones. Given the fact that candid comments enthuse the group, the members promote such confessions. The outburst of such emotions can vary from experiencing feelings of resentment, hurt, humiliation and anxiety. These emotions can cause teenagers to adults to pursue vengeance on the bully, to pull out into themselves or even commit suicide[29]. This is sort of bullying for the targeted person. User publishing personal information on social media pages is inclined to bullying for the disclosure of information that is kept private in real lives. The easiness to generate fake profiles again provide an occasion to state anything about another individual without the apprehension of any outcomes. This is corresponding to online hostility and cyber nuisance.

Whereas trolling is another way of targeting celebrities and politicians for their embarrassing statements or funny moments or their public appearances or statements. It can be humorous however it is characterized as an irregular behaviour with destructive bearings on online communities. Trolling has been drawing attention after social media as it generates provocation to absurdity. Trolling is contextual and cannot encompass all its behaviours. Compared to the traditional forms of bullying trolling cannot be identified for the mass generation of it by trollers and that it occurs 24 hours a day, 7 days a week and are shared like viral ones. It can also have a far reaching effect for the videos and posts being shared across social networking sites can be seen by large audiences. Cyber bullying is a modern version of until then prevailing conventional offline bullying. The difference is that under cyber bullying with bullies are not known to the victim. Trolling is done by anonymous group who are totally unrelated to targeted ones. This fails the police and the authorities to keep stride with progressing technology and the voidness in current laws to report the matter to be investigated upon.

1.10. Cyber Stalking

Stalking until causing harassment is unknown since most of the social media do not publish who visited profile list". Even if such list is published to the user who wants to know who all have seen his or her profile, that cannot be called as stalking since the purpose of such profile is social connection and for the very purpose people have to see, view and search for people they know. It is pertinent here to state on *Ritu Kohli* Case[30], being India's first case of cyber stalking. Though these are offences under Information Technology Act under 67 A, 67 B of the IT act as

[29] Cyber Laws Compendium on Bullying. Available at: https://cyberbullying.org/bullying-laws (accessed: 08.08.2018)

[30] Orkut Community rules. Available at: http://www.worldpulse.com/en/community/users/mukut/posts/22772 (accessed: 02.11.2018)

blackmailing, cyber-bullying, Cyber stalking or harassing, sending obscene messages through any electronic mails, not much developments ensuring the safety of women and children happened so far. Additionally, there could be intimidations of physical or sexual vehemence by email that degrades her identity and other traits (for instance sexual orientation).

1.11. Standard Contract and One-Sided Terms of Service

The terms in a contract are termed as standard when they are not premeditated to negotiate the interests of opposite party/ies rather take one way encompassing the interests of infinite customers[31]. Indeed, with the e-commerce transactions and boom of C2C, B2B, B2C *etc*, the users have no choice but to get into a social media site. From the earlier notion of consumers as king, today it has moved to consumer in need of goods or services and that gave corporate giants to control consumers. The users who want to be members in social media lack the bargaining power and thereby they lack the power to negotiate or modify the terms of the contract. Even then, the standard form of contract is preferred for it supports competence in contract law, which saves time and negotiation charges.

The enormous volumes of data (for instance uploaded pictures or video slides) in the clutches of the social media have been agreed to be used by the terms and conditions they put forward by way of standard form of contract. The user's categorical and blind approval of social media terms of Use and further users' disclosure of information about themselves in order to be able to interact with other people are increasing their venture, obligation and confidence in the social media itself. This means users do not only have an association with other users but also with the social media itself, which gains strength as the users get more involved in it.

As put forward by Aaron Chiu, As long as the site is dominant and competitors remain far from the tipping point, it can dictate the terms by which users will be bound [Eisenberg M., 1982: 741].

This issue of unconscionability had been tested by judiciary in various cases on the grounds of unequal bargaining power and substantive unfairness. But it had been held that:"…unequal bargaining positions, undue length, fine print, confusing language, and misleading terms, or the fact that a contract is a standard form

[31] Neumayer K. Contracting Subject to Standard terms and conditions. *International Encyclopedia of Comparative Law*, vol. 6, 1999, p. 12–17. The author states: "As social media users, our rights are established through non-negotiable, one sided and deliberately opaque 'terms of service' contracts. These documents are not designed to protect us. They are drafted by corporations, for corporations. There are few protections for the users-the lifeblood powering social media".

agreement, or contract of adhesion is nebulous concept...however they are enforceable unless the substantive terms are also unconscionable

"The grey area here is whether that consent is adequate. It is governed by the self-regulatory regime of contracts between the social media site and the user via the site's privacy policy. However the basic test of unconscionability of a contract remains the same. It is to find out:

"whether the clauses involved are so one-sided and it gives no scope of compromise"

"If it aims to oppress or unfairly give a setback upon the other party?"

"These clauses thus are analysed taking into account the conditions that were present at time of making of contract, overall commercial circumstances and the facts and situation of the particular case[32]".

1.12. Information Mining

Social media websites write in their policy their policy vaguely stating that they do information mining. Many companies for their business purposes use data mining algorithms, implanted in bigger knowledge discovery procedures and systems, are programmed analytical tools that have lately practised a speedy surge in use. Social media has facilitated users to generate unimaginable amounts of structured and unstructured data. The arena of data mining is attaining implication appreciation to the accessibility of large amounts of data, effortlessly composed and stored via computer systems. With the prevalent and endless assortment of information about persons from manifold sources, many data brokers are equipped identify user characteristics and certain inclinations without having any information conventionally considered personally identifiable information. When these data are amalgamated and extracted, they can deduce a person's choices, connections, information on finance, address, usage of bank transaction, insurance, medical records, and political interests. There are apprehensions that with the accumulative level of storing of private information there is a larger danger that unsafe or even derogatory practices might be generated.

1.13. Use of Third-Party Apps on Social Media

From what it had been visualised, many social media websites had expanded into an abundant giant information source with users their friends and various pages, communities, occasions, and group pages many personal data and interac-

[32] Facebook Principles. Available at: http://www.facebook.com/principles.php (accessed: 20.06.2019)

tion information. Thus gradually social media is presented by the large quantity of information communication between third-party developers and users itself. When social media offers applications –Apps- initiated by third party application providers, it provides access to users' personal information via installed Apps. This admittance happen outside the loop of communal conviction with the user not being attentive whether anyone had installed the App collecting any data.

Various studies show that many unsecured social media profiles and apps do a hacker's work by collecting details. They can study who the top people in an organisation are to be targeted at to gain information and thereby to start phishing attacks or learn employee job roles, addresses and contact information [Eisenberg M., 1979: 67]. That's the reason why the third-party apps permission to gain access to an individual's profile including their contacts are often difficult to verify. Additionally there are no set rules or regulations for app developer to follow when it is provided to a greater platform for usage. The platforms like Google or Android or Apple have their own developer program policies, along with the developer distribution agreement. With the growing concerns over customer data many platform calls for regulations that increase transparency with regards to how apps make use of customer data. By way of developer license agreement a clause is added so that developers will be accountable the way they handle user data. Google recently modified its regulation in line with European Union's GDPR and it calls for more clarity regarding usage of data from how they amass it to what it might be used for is available to all users. In his testimony before the US Senate post *Cambridge Analytica* exposure, Facebook CEO stated that there is a prospective legal risk connected with social engineering and hoaxing outbreaks against users and the magnitudes of leakage because of app developers as a result of social media is irrepressible.

1.14. Memes

"Undoubtedly, social networking sites proffer individuals both with a vibrant forum for self-expression and with a platform for concerning to an extensive array of speech in society at large. Memes are usually hilarious representation or image of some incident. Initiated as advertising slogans, its usage and diffusion provide a speedy and active way of generating interest. However some can turn out to be sarcastic and defaming. Comical memes are also shared purely for fun which provides some one-line dialogue from cinemas and re-count it to the taken notions and situations. Another issue is copyright violation. Simply retweeting someone else's memes can possibly be generating a legal action. In legal footings, it is a 'derivative work' and merely the copyright owner has the legal claim to generate such work. Even though the individual claims to have made a fair use of the copy-

righted work, it can be used as a defense under the requirements of the Copyright Act. If any legal issue crops up with memes sharing and re-sharing, it can land up trouble to those who have re-shared the same. In USA, Warner Bros were sued under infringement of copyright after they being found using the famous 'Nyan Cat' and 'Keyboard Cat' in their game *Scribblenauts Unlimited* [Swirsky E., Hoop G. et al, 2014: 60–61]. Some memes are so mean that it generates a lot of distress and injurious consequences to the targeted victims.

1.15. Evidence Submission From Social Media

"Social networks are with time becoming a source for the discovery and search of criminal activity by members. Information concerning to a user's social media page can be accepted as evidence in the court of law. A glaring example is the case where police had to investigate on the stolen goods where a woman was suspect. The police in such cases look for her profile then went onto examine her posts, activity streams, status updates, messages and happened to see her update regarding display of goods she had shoplifted[33]. Social media profiles is decisive to know the identity of especially to spot the location of the executor of a crime."

"Evidence from social media websites, commercial websites, and private and employer-owned e-mail accounts are used for both civil and criminal matters. In discovery requests, this electronic content often included, and courts generally apply the similar paper discovery rules to electronic discovery. Social media content, even though posted or created private, is not shielded from discovery. For the larger interests of society and to maintain equity, evidences can be brought forth no matter how and in what scenario the related evidences are used by the culprit. In *Giacchetto* case, the Federal Court of New York stated[34]": "A party to an action can request a protective order to limit the scope of discoverable information and can sometimes include a 'pull back' stipulation or court order in which the party can call back a privileged document that was inadvertently produced during a discovery request"

Due to the prevalence of 'hacking' in social media accounts — whereby an unapproved user accesses other user's account — it could create a chance for reasonable repudiation concerning any specific instance of generated account. If authenticity of produced document is contested, its legitimacy has to be established and ensure that the evidence has not been tampered. The other issues involve when individuals often have countless social media and email accounts, in which they may or may not use their actual names.

[33] *Romano* v. *Steelcase, Inc.*, 907 N.Y.S.2d 650.

[34] *Giacchetto* v. *Patchogue-Medford Union Free Sch. Dist.*, 293 F.R.D. 112 (EDNY2013).

2. Duties and Responsibilities of Information possessor or Carrier *vis a vis* Intermediary performing dissemination responsibilities

As per the common law jurisprudence, if there exists a contractual relationship, any sort of contravention of confidentiality is considered to be a breaking of contract and hence the infringer will be liable for damages. There are certain scenarios where despite having a contract, for the relation or fiduciary relation that exists with the parties, such confidentiality is implicit. There comes a responsibility not to disclose confidential information, even though such a responsibility is not mentioned in the provisos of the contract. Any such breach can result in a legal action for damages endure due to division of the confidential information and also an injunction to hold down the further spread of the confidential information. In the case judgment of "*Saltman Engineering Co Ltd. & Others* v *Campbell Engineering Co Ltd.*[35] the court held that the responsibility to maintain confidentiality exist even in the absence of a contract. In social media with the people having multi-facted connections when get into dissemination. These issues above mentioned once again reiterate that within traditional speech doctrine, different types of media are given different possibilities of protection and deference with respect to content control. On one end of the scale, newspapers are provided with great extent of editorial choice in deciding upon what content they should distribute. On the other end, telephone companies-categorised as common carriers-cannot standardise the content that traverse their lines. Cable, broadcast and other media are positioned between these two limits and obtain some amount of flexible mechanism. Social media having the traces of media how far is the information carrier is the dispute especially when vast amount of data and information are disseminated. Media as information carrier, it signifies the conventional concept of the press clause as defending all news media (from non-news media) which carry out a recognized and valued function in assembling, editing and disseminating information to the public. Secondly, it indicates an independent role for media not merely restricted to information-gathering period but also to the editing/scrutiny or the publication process or dissemination stage. By this it mandates to distinguish between 'publishers', 'disseminators' and other speakers in this regard.

The term 'dissemination' in its literal sense means spreading ideas or information by propagation[36]. Under Art. 10 of the European Convention on Human Rights (ECHR) 193, media is made accountable in imparting accurate information

[35] [1948] 65 RPC 203. Available at: https://www.jade.world/cases/19633AllER413 (accessed: 03.12.2020)

[36] Li T. Beyond Intermediary Liability: The Future of Information. *Yale law Journal*, 2018, vol. 52, p. 129.

to public[37]. By ratifying this Convention, all the nation-states have had an 'affirmative duty' to grant independence to the editorial staff of newspapers. This is unlike a common right of access to newspapers assuring the publication of everybody's information or ideas, whether in the form of articles, opinions or comments. That differentiates free speech and free press under every Constitution of democratic nations[38]. Freedom to impart is here of a more responsible task since Art. 10 of ECHR provides that a state may require the licensing of 'broadcasting' audio or visual media. Their publication depends on the private publisher's or Editor's free decision. By this, usage by any private citizen or organization to have access to broadcasting, unlike freedom of speech, is limited. Simultaneously it guarantees media to have a core set of skilled professionals safeguards that news production standards are inordinate and that extensively held ethical values are followed.

"The concept of reporters' privilege is not of contemporary vintage. Generally, these *de facto* protections from common law have played a critical role in shielding the press and preserving the flow of information to the public. This conferment of privilege keeps apart publishers from speakers for the responsibility they have. The goal of the privilege is to nurture whistle-blowing and other lawful revelations. As in all privilege situations, a potential of confidentiality should be assumed and it is to be tested to the degree permissible by law"[39]. Law confers the privilege to journalists or reporters in mainstream media as qualified privilege where the information if found fair, accurate and not actuated by malice[40]. Thus it needs to strike the right balance on[41]: (1) How much of this communication is vital to society; (2) In the absence of a privilege, if such communication will be inhibited; and (3) The cost to the legal system by losing access to the privileged information. To get privilege, it needs to be shown that the concerned entity or person has been in

[37] Art.10, European Convention on Human Rights (ECHR) 1953 states: …Public broadcasting services have to be protected by the freedom of expression. Freedom of press forecloses the state from assuming a guardianship of public mind. That watchdog approach helps in discovering the truth to people at large who can thus form opinions

[38] Press clause and Speech clause are the dual clauses implicit in Article 19 (1) (a) of Indian Constitution.

[39] Zampa J. Journalist's Privilege: When Deprivation Is a Benefit. *Yale Law Journal*, 1999, vol. 108, p. 1435. The author states: …Common law confers the privilege to journalists in terms ofthe social institution in which they operate and the democratic functions that they provide for society…"

[40] See Section 499 of Indian Penal Code, 1860 with the Exceptions provided.

[41] In the US judgment of *Reporters Com.* v. *American Tel & Tel*, it was held that there has to be three minimal tests conducted: That there is a reason likely to consider that the reporter holds information which is clearly related to a definite possible abuse of law. That the information it pursues cannot be gained by alternate ways, which is to say, from sources other than the reporter. That there includes an interesting and superseding interest in the information. See *Reporters Com.* v. *American Tel & Tel*, 593 F.2d at page 1039.

journalistic work of reporting or dissemination or circulation of information under public interest to impart newsworthy information to public. This conferment of privilege is on the basis of what dynamic, robust and active role news media journalists play in imparting information. For instance, newspaper delivery boy cannot be made liable for any information in the form of new paper he is delivering to people. How can a librarian be made liable for any contents of the books he is taken care of in library? These are the passive roles — often equated like *Postman rule* — are for carriers of information who is not aware of contents.

Here a categorical distinction is to be made between Information owner, Information possessor or holder, Information Disseminator or Information Carrier. The distinction is important in terms of conferring this Media as a watchdog has its distinct responsibilities and it can be carried out with the privileges or immunities provided by State. Qualified privilege at Common law applies where communications take place for honest purposes, and, therefore, this privilege can be defeated by malice. Such qualified privilege arises on occasions where there is a legal, moral or social duty to publish the information in question or when the person who receives the information has an interest in receiving it. It does not matter if the information given turns out to be untrue, provided that the statement was not made with malice[42]. Journalist-source privilege is termed as qualified privilege for the responsible task he performs. The"goal of most legal privileges is to promote open communication in circumstances in which society wants to encourage such communication [McCullough C., 2014: 176].

"For this reason, in social media, though people are self-content providers and self- editors and self- disseminators", they cannot call themselves like a reporter or editor or mainstream media persona for the lack of accountability journalism [Alexander T., 2017: 612].

Mainstream media whose main task was to gather, identify, edit and report the news has thus a qualified privilege in opposition to disclosure of any information, documents, or items obtained or prepared in the gathering or dissemination of news in any judicial, legislative, or administrative proceeding in which the compelled disclosure is sought. Unlike this, Social media provide multitude of services such as access to the platform, letting users to amass and publish content, do marketing and advertisements related work, to post photos, videos any documents etc."It is the medium amongst a person and the internet, letting them to upload, share or disseminate the content in any format. When users involve in internet shopping they do not use 'media' in its normal sense. The content and posts submitted by users are not verified or moderated, not edited or amended.

[42] *See* Smith D. *A Theory of Shield Laws: Journalists, their Sources, and Popular Constitutionalism*. LFB Scholarly Press, 2013, p. 252–255."

People express themselves without the help of an editor posting their contents. Social media gives everybody the occasion to circulate individually whatever they like."There are no stringent limitations on format, access, or contents. This leads to the conclusion that the social media is not a mainstream media as it was understood. They are using a 'medium' — a mediator for their activities.

Paradoxically, it does not recognize the content of the *cache*, nor do they are aware the content of the hosted material. This service as internationally termed as hosting service only diffuse the content that their 'customers' have submitted distinct from"a newspaper editorial office, which receive articles and reassess them and edits them individually before publishing, these sites."Therefore, hosting providers globally are not held liable for information for no actual knowledge of any unlawful activity or information if happens within the platform. In addition, upon obtaining such knowledge they have to expediently remove or disable access to the information. Many judgments had been rendered in this line that if the recipient of the service (the content provider) was acting under the control of the hosting service provider, the latter cannot be exempted[43]. Public policy positively encourages the proposal that individuals who have information of noteworthy value should normally be supported to express that information to the society. Society would want to promote the communication, and without a privilege the communication will regularly be chilled. Hence extending the legal right, privileges and immunities to social media is not constitutionally valid and that will result in irreparable harms to State, society and people at large. These raise the questions as to : If the people have a right to know, what is it that they have a right to know and who has the correlative duty to provide what the public has a right to know? Is the right to know a fundamental right derived directly from the Constitution, or is it a right that stems from a broader societal goal? These questions suggest that certain limits within the social media exist that cannot be made applicable to media. When people are posting the so-called news, there exists these issues on what to be posted and what not to be posted. And once the so-called information is posted, it cannot be called back. The affected parties can challenge only if the posted information is false. If the information is true and it ought not have published, there exists a moral right not to publicize everything. This is a dark area when there are certain information that cannot be shared or circulated for its pertinence to notions of personal autonomy and privacy. This means there exists certain unwarranted disclosure of information that might affect people at large. Those who uphold that there is a constitutional right to know, or that there ought to be, would define the concept as a right to receive information or communication and the right to ac-

[43] In the judgment — it was held that hold hosting service provider cannot be made liable if it did not: (a) Initiate the transmission; (b) Select the receiver of the transmission; and (c) Select or modify the information contained in the transmission.

quire or gather information. The latter notion has been argued as justifying a right to keep one's sources of information confidential. Privileges are granted by law to guard the content of confidential communications made throughout a privileged association. By this, the communication may not be admitted into evidence if the privilege is correctly emphasized by the person who made the communication.

Having observed the summary of Justice B.N. Srikrishna Committee report on Data Privacy and Personal Data Protection Bill, 2018, also considering the functioning of Indian polity balancing both — a vertical federal structure along with horizontal working with three organs of government structure"- imbibing the separation of powers, there is a necessity to have a legislation dealing with the way people's data is collected, utilized and shared by corporate companies. For this there is a need to divide the data as general data and highly sensitive data. Though under section 43 of IT Act, 2008 has provision to hold a corporate body accountable if any recklessness comes in handling data happens, or not creating reasonable rules on data processing, what all can come under sensitive personal data is still a dilemma. There is a need thus to lay down various conditions such as consent requirement", legitimate purpose", purpose limitation", succeeding withdrawal of consent etc. to inflict on the body corporate while amassing any such information. There is a lacuna currently on Rules require the prior consent of the provider of the information while disclosing sensitive" personal data to a third party. Consequently, a crucial foundation for processing of personal data is the individual consent that mandated the necessity to have a proper consent formation. Neither the consent be made uninformed nor momentous rather it functions in an all-or nothing fashion."

Another finding of the report was that — data flows in India is a consequence of a simplistic assumption that data flows are an unadulterated good", hence the data flow happening within and outside Indian jurisdiction can cause substantial damage. This provides an unlike character to the expression in various jurisdictions choosing the person whose data is being amassed as the data subject and the body that assemble the data as the data controller". This arises from an assumption that the association involving the individual and bodies with whom the individual distribute the personal data is one that is based on a primary expectation of faith. In spite of any contractual association, an individual suppose that the personal data will be applied reasonably, in a mode that accomplish necessary significance and is logically estimated. This is the trademark of a fiduciary association. Pursuant to this, conditional on the temperament of data that is collected, the rationale behind such collection, the bodies with which involvement do take place, data principals envisage shifting degree of reliance and reliability. For bodies, this deciphers to an obligation of care to cope with such data reasonably and dependably accepted by the Principals and therefore it could be called as data fiduciaries". On

this basis the proposal of the Committee was that such flows cannot be unencumbered, and definite responsibilities need to be forced on data fiduciaries who yearn to reassign personal data beyond India. At the same time India's national interests may require local storage and processing of personal data with obligations on data fiduciaries and rights of data principals. Anyone who uses personal data has an obligation to use it fairly and responsibly. This is the cardinal tenet of the proposed framework.

This approach will safeguard individual autonomy plus privacy which can be attained within the facets of an open and reasonable digital economy. At the same time, in lieu of legitimate interests of state as provided under Justice *Puttaswamy* Judgment[44], there may be instances where rights and obligations of data principals and data fiduciaries do not affect in entirety. This manifests in limited instances where consent may not be used for processing to serve a larger public interest such as national security", prevention and investigation of crime", allocation of resources for human development", protection of the revenue"[45]. "However, on the right to be forgotten,"the Bill notes that 'data principal' which means the individual or the person providing their data, has a right to right to restrict or prevent continuing disclosure.""But the bill does not allow for a right of total erasure like the European Union does. Another highlight is that the bill mentioning about handling of "anonymisation proportionate to personal data, wherein it proposed that the irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, meeting the standards specified by the Authority.

Conclusion

Social media rely on information that tend to soften privacy concerns, signifying that the information is voluntarily (though users have no choice) submitted by users. Social media creates a new generation of audience-producers and this hazes the central line amongst access to the means of online content production and ownership or control over these resources where privacy is at stake! It has been observed that by the virtue of liberty, freedom and right, every human being has the right to communicate his or her opinions and ideas and share information in whatever form in accordance with legal parameters. The freedom of speech and expression has various facets and one among it, the freedom of press is a public service with a duty to the people[46]. The open course of information, which is so

[44] *K.S. Puttaswamy(Retd) v Union Of India 2017 (10) SCALE 1.*

[45] See BN Srikrishna Committee. *Report on Data Protection Framework*. June 2018.

[46] Arun C. Making Choices: Social Media Platforms and Freedom of Expression Norms in: L.

necessary to effectual self-governance, is considerably important with the subsistence of a free and robust press. For this, the press must occupy in numerous precise positions and display some unique features. Since they are viewed as so essential to a flourishing and vigorous democracy, these desirable position and features have progressed into a set of debates concerning the media.

The degree at which exchange of communication existed had been multi-folded with sudden increase in information collected and circulated. Today every news-media has its social media web page including *Twitter* handles or *Facebook* pages thus stories are searched on internet service providers to know if any user has uploaded anything that became 'viral'. Moreover, it has become a necessity for mainstream print media to have their websites, live videos, journalists' blogs, invited newsrooms debates where invitation is extended to community participation. The bloggers consider themselves as journalists and break *scoops* and stories. With the notable shift to mobile news access news has now become omnipresent-available on every platform at any time."Regardless of their professions, resources or training today, *netizens* are disseminating news to the public themselves. Personalized and participatory stories having maximum views or shares are now converted as news. In a democratic country, news should be based on what the people need to know not on what the public wants to know. This upsurge in 'citizen/selfie- journalism', through social media is jurisprudentially affecting the information matrix and constitutionally envisaged rights and freedom.

References

Alexander T. (2017) Social Media Accountability for Terrorist Propaganda. *Fordham Law Review,* vol. 86, pp. 612–615.

Bill J. (1972) Class Analysis and the Dialectics of Modernization in the Middle East. *International Journal of Middle East Studies*, no 3, pp. 417–434.

Birkinshaw P. (1988) *Freedom of information, law, practice and ideal.* L.: Weidenfeld and Nicolson, pp. 140–146.

Blanchard M. (1986) *Exporting the First Amendment: Press-Government Crusade of 1945-1952*. N.Y.: Longman, pp. 34–38.

Brownlee J. (2019) Low Tide after Third Wave: Exploring Politics under Authoritarianism. *Comparative Politics,* vol. 34*,* pp. 477–498.

Chiu A. (2011) Irrationally Bound: Terms of Use Licenses and the Breakdown of Consumer Rationality in the Market for Social Network Sites."*South California Interdisc Law Journal,* vol. 21, pp. 167–213.

Bollinger and A. Callamard (ed.) *Regardless of Frontiers? Freedom of Expression and Information in the 21st Century.* N.Y.: Columbia University Press, 2019, p. 382–383.

De Sola P. (1983) *Technologies of Freedom*. Wash.: Belknap Press, p. 76.

Donath J., Boyd D. (2004) Public displays of connection. *BT Technology Journal*, no 1, pp. 71–82.

Finn J., Banach M. (2000) Victimization online: The downside of seeking human services for women on the internet. *Cyber Psychology & Behavior, no* 3, pp. 785–796.

Franklin B. (1737) Freedom of Speech and Press. *Pennsylvania Gazette*. November 17.

Hackworth B. (2011) Are Consumers Following Retailers to Social Networks. *Academy of Marketing Studies Journal*, no 5, pp. 1–23.

Knutson A. (2009) Proceed with Caution: How Digital Archives Have Been Left in the Dark. *Berkeley Technology Law Journal*, vol. 24, pp. 437–474.

McDermott K. (1982) Liability for Negligent Dissemination of Product Information: A Proposal for Assuring a More Responsible Writership. *Forum,* no 18, p. 557.

McPeak A. (2015) Social Media, Smart phone, and Proportional Privacy in Civil Discovery. *University of Kansas Law Review*, no 1, pp. 235–292.

Mill J.S. (1964) *Representative Government*. L.: Everyman's Library, pp. 26–28.

Moore P., Salloukh B. (2017) Struggles under Authoritarianism: Regimes, States, and Professional Associations in the Arab World. *International Journal of Middle East Studies,* vol. 39, pp. 47–70.

O'Reilly T. (2007) What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. *Comm. & Strategies,* vol. 65, pp. 18–19.

Smolla R. (1992) *Free Speech in an Open Society*. N.Y.: Knopf, pp. 271–277.

Stacy A. (2017) Paying for Privacy and Personal Data Economy. *Columbia Law Review,* no 6, pp. 1375–1376.

Ten C. (1969) Mill Liberty. *Journal of the History of Ideas, no 30,* pp. 47–68.

Van Niekerk B., Maharaj M. et al (2013) Social Media and Information Conflict. *International Journal of Communication*, no 7, pp. 1162–1184.

Wacks R. (1989) *Personal Information: Privacy and the Law*. Oxford: Clarendon Press, p. 432.

Yigit F., Tarman B. (2013) Impact of Social Media on Globalization, Democratization and Participative Citizenship. *Journal of Social Science Education,* no 1, pp. 75–80.

Zhu J. (2009) Roadblock and roadmap: Circumventing press censorship in China in the new media dimension. *University of La Verne Law Review,* vol. 30, p. 404.

Internet Freedom of Speech and Privacy Protection: Is There a Contradiction? (A Study of Rating Sites)

Elena Ostanina

Associate Professor, Department of Civil Law and Process, Law Institute, Chelyabinsk State University, Candidate of Juridical Sciences. Address: 129 Br. Kashirinyh Avenue, Chelyabinsk 454080, Russian Federation. E-mail: elenaostanina@mail.ru

Abstract

While the Internet promotes widespread communication, this communication is often anonymous. How to draw the line between freedom of speech and privacy? The specifics of protecting privacy and business reputation against violation by rating sites are discussed in this article. Do the activities of rating sites need special legal regulation? The author believes that the general rules on privacy and freedom of speech are sufficient for regulating these new relations. The respective court practice of Germany, the UK and the USA is analysed. The tentative conclusion is that rating sites do not contradict the law if they do not disseminate information about the private lives of people or encourage rude and scornful assessments. The problem of using personal data is examined. The author holds the view that the activities of rating sites can be beneficial for society and therefore should not be banned entirely. However, site owners should be allowed to use personal data only upon the consent of the owners of the latter.

Keywords

freedom of speech, reputation protection, privacy, site, damage, site owner.

For citation: Ostanina E.A. (2020) Internet Freedom of Speech and Privacy Protection: Is There a Contradiction? (A Study of Rating Sites) // *Legal Issues in the Digital Age,* no 3, pp. 125–139.

DOI: 10.17323/2713-2749.2020.3.125.139

Introduction

Uber was apparently the first Internet platform to introduce a rating system. This system provides a convenient means of assessing the quality of services. Today, many organizations offer ratings of their employees, while some organizations, including Uber, also provide ratings of their customers.

The spread of ratings is facilitated by social networks with theirs system of "likes" and "dislikes" and subscriber metrics. Ratings are common both in professional activities (ratings of restaurants, cafes, schools, universities and sites) and in interpersonal relations.

Many specialists such as medical doctors, teachers, and lawyers are being rated today, often without knowing anything about it.

In Russia ratings have not been the subject of litigation so far, although official and unofficial ratings have evoked a lot of emotions (both positive and negative). In foreign civil proceedings, rating sites have been subjected to evaluation on several occasions. Let us consider this experience in more detail.

1. Privacy protection versus freedom of speech: a general characteristic

People living in the digital age are not ready to part with confidentiality and the secrets of private life [Roessler B., 2005: 62]. Still, maintaining confidentiality is somewhat more difficult on account of the digital traces left by every person. Messages remain after communication on Internet forums, and photos are posted on social networks. All this information is stored for a long time after being posted. The author of such information may subsequently change his or her mind, yet it will take a lot of time and effort to remove it from the Internet. Even if an individual is careful, third parties can post unwanted information. This aspect of privacy protection needs careful analysis. Such significant freedoms as the freedom of speech and the right to privacy interact here. Freedom of speech is a right that does not have clear boundaries established in advance. The boundaries of this right are delineated on a case-by-case basis. The values that can be violated during the exercise of the freedom of speech and the values that should be protected must be compared. There are strict guidelines for this, of course. In particular, the dissemination of false information discrediting honour, dignity and business reputation is not allowed.

2. Germany: Spickmich judgment (2009) — assessments and the freedom of speech

In Germany an extensive and controversial practice has already developed with respect to the legitimacy of rating sites. This practice began with a lawsuit by a school teacher who believed that her privacy had been violated by a site on which users compared schools (www.spickmich.de).

The circumstances of the case were as follows: the defendants developed an online website for schoolchildren, where teachers and teaching in various German

schools were discussed. The site www.spickmich.de kept and posted information about the names of teachers, the names of schools, the subjects taught, student ratings of teachers, and quotes by teachers. This information was accessible to registered site users. Registration on the site required entering the correct name of a school, the location of the school, a username and an email address. Registration was confirmed by a link sent to the indicated email. Users could share information about themselves, send messages to other users or create their own "clubs" or groups of "friends" and "classmates" on different pages of the site. The site had the rubrics "my page", "my friends", "news", and "my city".

However, the subject of controversy was the rubric "my school". On the site, users could evaluate their school building, equipment, extracurricular activities and teachers. When evaluating teachers, one could use predefined criteria such as "cool and funny" (*cool und witzig*), "popular" (*beliebt*), "knows how to motivate", "humane", "good lessons", "fair grades", "appearance", etc.

It was possible to rate all the criteria or several of them, albeit not less than four, on a scale of one to six points. The teacher's overall assessment was a sum of his or her individual ratings. The evaluation result was displayed in the form of a certificate that could be printed out. In addition, users could write quotes of their teachers in the "Quotes" section. If no new ratings appeared for a teacher in 12 months, the old grades and quotes were automatically deleted. The message "there is a contradiction" appeared on the site when the ratings of several users significantly differed from each other.

In early May 2007, the plaintiff discovered that a certificate with her name, the name of the school in which she taught, and her subject (German) had been posted on the website www.spickmich.de. The certificate was based on four student ratings and indicated an overall score of 4.3[1]. No quotes were given. The name, school and subject were indicated on the website in exactly the same way as on the school's open-access website.

In her lawsuit, the teacher demanded that her name and information be removed from spickmich.de.

The court rejected the lawsuit[2]. The Court of Appeal agreed with the decision of the trial court, arguing that the assessments made by the defendant constituted an expression of opinion and that the plaintiff's personal non-property rights had not been violated, since all the assessments related to her professional activities.

Criteria such as a teacher's sense of humour ("cool and funny"), appearance, and humane attitude also related to the professional qualities of the plaintiff, since a person must control his or her speech and behaviour in professional activities.

[1] In German schools, the maximum score is usually 1, so a score of 4.3 is apparently quite low.

[2] Available at: https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=23.06.2009&Aktenzeichen=VI%20ZR%20196%2F08// (accessed: 20.09.2020)

In such activities, it is also important to see the consequences of one's actions and their perception by others. Ratings can serve as a guide for schoolchildren and parents, as well as increasing transparency.

The Court of Appeal further noted that, insofar as teachers give grades to students, students should also be allowed to rate teachers.

The rules of registration on the site ensured that the site was used only by interested parties whom this information concerned in one way or another — students, parents and teachers. The rating page could not be found by entering the teacher's name in an Internet search.

The anonymity of the assessment also assured the legality of the publication. Legislation in force at this time allowed the anonymous use of the Internet.

In the learning process, students depend on teachers and their grades. This makes the anonymity of the reviews justified: otherwise, students could fear negative consequences.

The system of registration on the site means that the owner of the site could take measures against inappropriate, offensive, false or defamatory statements. Therefore, the anonymity of publications was justified. As for the teachers' quotes published on the site, no false quotes had ever been identified. It cannot be said that any personal data of the plaintiff was disclosed, since the name of the teacher, the name of the school and the subjects that the teacher taught could easily be obtained from the school's open website.

In its decision #VI ZR 196/08 of June 23, 2009, the German Supreme Court upheld all the arguments of the court of appeal as well as emphasizing the admissibility of the collection, storage and transmission of personal data as part of a rating forum on the Internet[3].

The sixth composition of the German Supreme Court examined in great detail the arguments of both the plaintiff and the defendant, making the Spickmich case a significant precedent for the development of the theory of privacy and the freedom of speech.

The German Supreme Court noted that the defendant (the owner of the site) provided an information and communication service. The defendant was not responsible for information posted by third parties. He would have been responsible if he had known about the illegality of the information, yet, in this case, such illegality was not evident. It is true that the plaintiff did not give permission to collect and use her personal data. However, the site reflected only limited information about the plaintiff that was already freely available on the school's website. The defendant did not try to take personal advantage of this data; he processed it automatically by calculating the average score of ratings given by users.

[3] German Supreme Court Decision #VI ZR 196/08, June 6, 2009. Available at: https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=23.06.2009&Aktenzeichen=VI%20ZR%20196%2F08 (accessed: 10.09.2020)

When considering the use of the personal data of the plaintiff, the judges cited several legal sources. These sources showed that sites that rate specialists enjoy the privileges of mass media and are allowed to collect all necessary information for the rating, including personal data from open sources. Information can be collected from open sources without the consent of individuals to whom the information relates; otherwise, journalistic activity would become impossible.

The decisive criterion for the judgment was that personal data was used only to create a news message (in this case, a rating).

One should use only information without which the news message or rating cannot be created.

Personal information should not be used simply to embellish news or evoke emotions. However, in the present case, personal data had been used in a "modest" fashion.

Further, the court decision discussed the question of whether the defendant had taken a legitimate interest in the storage and processing of the plaintiff's personal data.

The German Supreme Court ruled that the site's activities met public demand for information about schools.

The court also noted that the defendant reasonably limited the dissemination of information — site users could see information about teachers and schools, including reviews and ratings, while third parties not registered on the site could not.

To the question of whether the ratings and reviews violated the plaintiff's privacy rights, the court replied in the negative. There was no violation, since communication with students did not pertain to the private life of the plaintiff.

Everyone has the right to decide what to do with his or her personal data (this is what the German Armed Forces calls the "right to informational self-determination"), but the desire for confidentiality should not be excessive.

Information related to private life is particularly protected, while information relating to professional activities, i.e., human interaction with society, cannot be absolutely confidential. Despite the fact that a number of assessments such as "sense of humour" and "humaneness" related to the personality of the plaintiff, they also reflected how the plaintiff behaved in the professional sphere. The ratings were not expressed in an offensive manner and did not affect the human dignity of the plaintiff. Therefore, while recognizing that ratings, reviews and Internet publications in general can threaten privacy, the German Supreme Court did not see a violation of the right to privacy in this case.

The court was not convinced by the plaintiff's argument that she had not registered on the site and that the ratings had been made by anonymous users. It decided that the right of site users to freely express their opinions was not contingent upon the plaintiff's registration on the site.

The German Supreme Court agreed with the appellate court that the anonymity of ratings is acceptable on such sites. Otherwise, the freedom of speech would be limited by the fear of repression. The court also judged that the owners of the site showed reasonable discretion, providing the note "there is a contradiction" to draw attention to differences in ratings made by users.

The German Supreme Court emphasized that every reasonable user of the site was aware that the ratings could be biased. However, even biased assessments can be useful to people, including the teacher himself.

In view of all the above arguments, the court upheld the decisions of previous instances. The plea to exclude information about the plaintiff from the content of the rating site was denied.

This court decision was widely discussed in later literature [Barendt E., 2016: 112]; [Ungern-Sternberg S., 2019: 8–15].

The decision can be viewed in a positive light. Indeed, our competence as rational and social agents depends on a constructive adaptation of social control mechanisms [Schoeman F., 1992: 204]. The German judges who considered this case were credited with (1) creating the guideline that, in contrast to private life, official affairs and actions can be discussed, (2) justly drawing attention to the fact that records should be made available only to authorized site users, and (3) correctly defining the main problem that reviews and comments posted on the Internet can violate privacy [Cheung A., Schultz W., 2018: 332–335].

3. Germany: two Jameda cases (2014 and 2016)

Court practice in this domain was further developed in two cases involving the owner of the Jameda website. While these cases, which relate to ratings of doctors, are slightly less cited than the Spickmich case, they have also had a noticeable impact on the development of the theory of the protection of privacy on rating sites.

The first case led to German Supreme Court Decision #VI ZR 358/13 of September 23, 2014[4]. The Jameda website provided useful information about medical organizations in Germany and, in particular, allowed patients to rate the doctors they visited.

Individual ratings were combined to make doctor ratings. Only registered users were entitled to make ratings; registration required the confirmation of an email address.

The information about doctors posted on the site include their name, education, academic degree, specialization and place of work.

[4] Available at: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=69297&pos=0&anz=1 (accessed: 15.09.2020)

The plaintiff (a gynaecologist), after learning that the site has information, including several ratings, about him, demanded that it be removed by the site owner. The latter refused.

The trial court dismissed the lawsuit, and the appellate court upheld the decision.

In the appeal, the plaintiff insisted that the defendant made illegal use of personal data. The plaintiff said in the cassation appeal that the defendant had used the personal data of doctors not only to the benefit of site users but also for commercial gain, since the defendant offered a paid service for promoting doctors' profiles. A site user who searched for a "gynaecologist" first saw the profiles of doctors who concluded agreements for promoting their profiles and only then the profiles of other doctors in the order of their rating.

The argument about the commercial use of personal data was very strong. However, the plaintiff did not submit this argument to the court of first instance, while higher courts do not consider new evidence. Therefore, the German Supreme Court rejected this argument for procedural reasons.

As a result, the arguments of the prosecution only cited the facts that the plaintiff had not allowed the use of his personal data, had not expressed his consent to being rated, and held the view that, in the absence of his consent, the respondent's website did not have the right to use information about him. In its assessment of these arguments, the German court noted the following.

First of all, the inclusion of the plaintiff in the doctors' rating without his consent violated the plaintiff's right to informational self-determination. In addition, the professional activities of the plaintiff had been seriously damaged by the information and ratings posted on the respondent's website. However, this violation was nothing more than a guarantee of the patient's rights to express his or her opinion freely. There is major public interest in making potential patients more aware about doctors to inform their choice. Patients at the stage of choosing doctor are vulnerable and do not always dispose of sufficient information. The site run by the defendant was designed to help patients make a choice.

Although the evaluations on the site did not paint a complete picture of treatment (since these evaluations were made by patients, not professionals), the opinions of other patients can also be important for a patient choosing a doctor.

Secondly, the site allowed people to rate and write reviews anonymously; however, such evaluations could only be made by registered users, and so the respondent had information about the evaluators' email addresses. In the event of inaccurate information or a review expressed in an offensive form, a person could file a complaint against the defendant, for which a special tab was provided on the site.

Thirdly and most importantly, the plaintiff demanded that information about him be deleted from the ranking of doctors on the respondent's website. If his claim had been satisfied, other doctors would most likely have requested not to

be evaluated, either. This, in turn, would have put doctors who did not refuse to participate in the rating in a vulnerable position. They would have run the risk of negative reviews and competing with doctors about whom no reviews had appeared on the site.

In addition, if the site contained information about some doctors only, this would harm the very concept of the site and make it ineffective. The claim was denied.

In later practice, this case was interpreted as showing that sanctions should be proportionate and that it is undesirable to delete personal data from a work or a site if the deletion leads to the inability to use the work or site (except in cases of major violations).

The second case was brought in 2016 against the same defendant — the Jameda website. It led to German Supreme Court decision #VI ZR 34/15 of March 1, 2016[5].

A negative review was published on the defendant's site. The patient was dissatisfied with the quality of the dental services provided to him. The plaintiff (the dentist) was given the lowest score in three categories: (1) treatment, (2) explanation, and (3) trust. The rating was made anonymously, and a review in free form describing the poor quality of services was attached to it.

When the plaintiff found out about the negative review on the site, he sent a letter to the site owner asking him to delete the review or, at least, to give him information about the patient who made it. The plaintiff claimed in his letter that, as far as he could tell, he had never treated such a patient.

After receiving the plaintiff's letter, the site owner contacted the patient and asked him for brief information (2–3 sentences) about the circumstances of the visit and the treatment. The patient provided brief information in three sentences without any supporting documents. After that, the defendant informed the plaintiff that he could neither delete the review nor give any information about the patient's personality. The dentist took the matter to court.

The plaintiff argued that a negative review on three important points for a doctor, posted on a well-known site, violated his personal rights and damaged his business reputation. The plaintiff demanded that the negative rating made by the patient be removed from the respondent's site. The trial court satisfied his claim. The appellate court annulled the decision of the court of first instance and rejected the lawsuit.

The German Supreme Court, considering the cassation appeal, turned to the classical theory of protecting business reputation from inaccurate publications, recalling that there are two types of publications. Some only contain an assessment and cannot be checked for reliability. Others contain a statement of facts and can

[5] Available at: https://dejure.org/dienste/vernetzung/rechtsprechung?Text=VI%20ZR%2034%2F15&Suche=VI%20ZR%2034%2F15 (accessed: 17.09.2020)

be checked for accuracy, which can lead to liability for the dissemination of false information.

In this case, the patient's rating and assessment included two components.

The first was his opinion about the poor quality of treatment. The second was a statement of fact.

The statement about a fact (that the plaintiff had provided dental services to the patient who made the review) could be checked for accuracy.

Further, referring to the duties of the site owner, the court indicated that the latter is not obliged to take measures to verify every review posted on his site. However, if a complaint is received from a person with vested interests, the site owner must take reasonable verification measures.

At the same time, these verification measures should be proportional to the possible violation of the rights of the plaintiff. In this case, a negative assessment on the site could have seriously hurt the interests of the plaintiff by aggravating his competition with colleagues and complicating his further employment. Given the anonymity of the assessment, self-defence, i.e., protection without the help of the site owner, was virtually impossible.

Therefore, after the plaintiff had filed the claim, the site owner should not have limited himself to requesting the person who made the review to write 2–3 sentences about his treatment. The site owner should have tried to get acquainted with documents confirming that perform who left the review had indeed visited this dentist.

As a result, the court of cassation sent the case for new consideration to the court of appeal, specifying that, during the new examination, it was necessary to find out (1) whether the patient who left the review had been treated by the plaintiff and (2) whether the defendant had taken reasonable measures to verify this fact[6].

The three cases examined above all deal with the same problem: the conflict between freedom of speech and privacy.

The concept of "informational self-determination" formulated in the Spickmich case is significant for the development of judicial practice. It concerns a person's right to determine what exactly should be disclosed about him or herself and in what form.

4. USA: freedom of speech above all

In the United States, disputes between specialists evaluated by various sites and the owners of these sites have also been subject to legal proceedings on several oc-

[6] BGH, VI ZR 34/15, March 1, 2016. Available at: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=74291&pos=0&anz=1; https://dejure.org/dienste/vernetzung/rechtsprechung?Text=VI%20ZR%2034%2F15&Suche=VI%20ZR%2034%2F15 (accessed: 15.09.2020)

casions. In a few cases, the specialist who received a negative rating knew the person who made it. Such was the case in Dietz Development, LLC v. Perez[7]. The lawsuit was brought directly against the person who had left a negative review on the website. The case involved a client who had hired a contractor to carry out repair work. The client did not like the result of his work and wrote a negative review on the Y. website. The contractor answered on the same site, and the client replied to the comment. By the time the court began to consider the defamation lawsuit filed by the contractor, there were a dozen messages from both parties on the Y. website, and some of the expressions were not acceptable. The court ruled that the parties had mutually insulted each other and denied the claim for damages.

Even more interesting is the case Reit v. Yelp (2010)[8], which resembles the Jameda case (2014) in its circumstances. A dentist filed a lawsuit against the owner of the Yelp website to receive compensation, restore positive reviews and remove negative reviews from the site, which posted reviews about companies and specialists.

There were ten positive reviews and ten positive ratings about the plaintiff on the Yelp website. Then an unknown person left an anonymous negative review and gave a bad rating, and this negative review automatically deleted all earlier positive reviews [Cheung A., Schultz W., 2018: 325–326]. The plaintiff believed that removing positive reviews after receiving a negative one was the respondent's strategy to motivate professionals to pay for advertising on the site. The defendant did not deny that he offered advertising on the site for money yet drew attention to the fact that the review had been posted by a third party freely and at its own initiative and that the client who left the review had therefore exercised his right to freedom of speech.

The court described in detail the value of the freedom of speech, comparing (as in the Spickmich case) site maintenance activities to journal publishing. The court went even further in its comparison, drawing an analogy between the automatic selection of only the latest reviews and editorial activities. The parties discussed at length on what grounds the "editing" had been carried out: the plaintiff argued that positive reviews were hidden in favour of negative reviews, while the defendant explained that old reviews had been hidden in favour of new reviews.

At the same time, the decisive argument concerned the status of the owner of the site. The content — the response — came not from the owner of the site but from a third party. As the legislation in force at the time of the dispute put the responsibility on the "content provider", the lawsuit was denied.

Moreover, the court emphasized that, even if the defendant had used reviews set aside by third parties for their commercial purposes, this was no reason to restrict the freedom of speech.

[7] Dietz Dev., LLC v. Perez, No. CL 2012-16249, 2012 Va. Cir. LEXIS 139 (December 7, 2012), revised, 2012 Va. LEXIS 227 (December 28, 2012). See also: [Cheung A., Schulz W., 2018].

[8] Reit v. Yelp!, Inc., 907 N.Y.S.2d 411 (Sup. Ct. 2010).

Similar circumstances and a similar decision occurred in the case Braverman v. Yelp[9]. However, this approach that, first and foremost, protects the freedom of speech (including anonymous freedom) is open to criticism. If complete freedom is given to anonymous ratings and anonymous reviews written in any form, a person's reputation is essentially in the wrong hands and out of his or her control [Cheung A., Schultz W., 2018: 326, 335].

5. UK: freedom of speech does not mean freedom of defamation

In the UK, the key to the legal regulation of the activities of rating sites is considered to be the case Law Society & Ors v. Kordowski[10]. In 2011, the court decided that the activities of the website "Solicitors from Hell" (solicitorsfromhell.co.uk) were against the law [Scaife L., 2015: 254]. However, the defendants claimed that the site had been created in order to identify and shame unscrupulous solicitors.

The goal of the site shows that it was specially created to collect negative reviews. In order to leave feedback, you had to pay a registration fee. A lot of negative reviews were collected, some of them related not only to the professional activities but also to the identities of solicitors. The plaintiff brought the case as a person acting in the interests of a group of solicitors and law firms in England and Wales. The plaintiffs had found out about posts on the site when they searched for the names of their businesses on Google. The messages and reviews on the site were anonymous.

The court ruled that the personal data of the solicitors had been used without their consent, that the website contained numerous inaccurate and offensive statements, and that it therefore violated the Data Protection Act 1998 (DPA) [Ruhmkorf A., 2014: 55–56].

In addition, the site owners obviously encouraged negative reviews.

Just as in the German Spickmich case, the court drew an analogy with journalist activities and considered the argument that journalists also cite specific names in their publications.

However, this analogy was not in the defendant's favour. Judge Tugendhat stated that "today anyone with access to the Internet can do journalism for free..."[11].

He contrasted the actions of journalists and the actions of the defendant. Journalists cite specific names in their publications when discussing ideas or events

[9] Braverman v. Yelp, Inc., No. 158299/2013, 2014 WL 712618, at *5 (N.Y. Sup. Ct. 2014). Cited: Cheung A., Schulz W. Op. cit.

[10] The Law Society & Ors v Kordowski [2011] EWHC 3185 (QB). See: [Ruhmkorf A., 2014: 557–567].

[11] Available at: https://www.bailii.org/ew/cases/EWHC/QB/2011/3185.html (accessed: 16.09.2020)

of importance to society (leading to a prevalence of public over private interests, which is justified), while there was no discussion of socially significant ideas in the activities of the solicitorsfromhell website [Erdos D., 2015: 119–154].

The court conducted a comparative legal review of precedents and the literature and examined recent cases in the United States, where attention had been paid to the freedom of speech, and concluded that, even in the United States, freedom of speech did not mean freedom of defamation. As a result, the court noted that a ban on the further activities of the site would protect the public from deliberately inaccurate information as well as protecting the court from further defamation lawsuits that would undoubtedly be brought if the defendant continued his malicious activities[12].

The website rateyourlecturer.co.uk, which opened after the closure of solicitorsfromhell.co.uk, also evoked complaints [Ruhmkorf A., 2014: 9].

Therefore, the activity of rating sites is obviously associated with an increased risk of responsibility. At the same time, it seems that the case of the solicitorsfromhell website should not be interpreted as a complete ban on all rating sites, ratings and reviews in the UK. Lawyers, medical doctors, and other professionals who interact with numerous clients should pay attention to feedback, which can be received, in particular, from such sites. Therefore, if the site does not explicitly call for negative reviews, the evaluation of specialists can be recognized as being legitimate, especially if this information is obtained from open sources.

6. France: anonymous teacher ratings are not good for education

In France, the court examined a case whose circumstances were very similar to the Spickmich case.

The dispute surrounded the activities of the site note2be.com that provided a forum where students could discuss the professional qualities of teachers and rate them. The French court ruled that this kind of teacher assessment on a site harms the education system[13], all the more so as the personal data of teachers was being used without their consent [Erdos D., 2015: 16–17]. As a result, an injunction was issued against the further activities of the site.

Our comparative analysis suggests that rating sites are fraught with a conflict between freedom of speech, on the one hand, and privacy, on the other. The boundaries of privacy as a right are not defined for all possible situations ahead of time. It is necessary to evaluate the interests that a rating site protects and the interests that

[12] Available at: https://www.bailii.org/ew/cases/EWHC/QB/2011/3185.html (accessed: 16.09.2020)

[13] TGI, 3.03.2008, № RG 08/51650. Available at: http://www.foruminternet.org/specialistes/veillejuridique/jurisprudence/IMG/pdf/tgi-par20080303.pdf; [Scheuer A., Schweda S., 2011: 13].

it jeopardizes and compare them. In any case, information relating to family and personal relationships is more protected than information about professional life. Information relating to professional life is generally open to discussion (provided, of course, that the latter assumes a correct form).

7. Types of sites

One can provisionally distinguish two types of rating sites: (1) sites which post consumer reviews of services delivered to them (sold goods, performed work) and (2) sites that publish ratings of personal qualities. The Russian sites "flamp.ru" and "otzovik.com" are examples of the first type. It should be said that these sites have taken reasonable measures to prevent the violation of personal intangible goods.

In particular, the otzovik website has a user agreement that sets down the following obligations: "Users are obliged to refrain from publishing information or other materials that (a) discredit the honour, dignity or business reputation of other users or third parties, (b) contain calls to violence or promote discrimination against people on racial, ethnic, gender, religious or social grounds, or (c) violate the intellectual rights of users or third parties" (clause 4.4)[14].

An undoubted benefit of such sites is that the information they publish allows potential consumers to receive information about a seller or contractor quickly and easily. Such sites serve as a "low-cost and time-saving means" of assessing the quality of goods and services and are therefore useful to both consumers and society at large [Hinz A., 2011: 745–764]; [Serna F., Inesta J., 2018: 11][15].

The opposite of such professional (or "quasi-professional") sites are interpersonal sites, where the object of the assessment is the personal qualities rather than the professional characteristics of an individual. This type of site is, of course, the most dangerous.

For example, it is noteworthy that the Spickmich website (which published reviews about teachers), initially included the evaluation criterion "sexuality, attractiveness". However, this criterion was subsequently removed [Gounalakis G., 2010: 566, 570]; [Ruhmkorf A., 2014: 8, 9].

Conclusion

The Internet has simplified the dissemination of notes, reviews, and publications as well as facilitating communication. However, it has also made the boundaries of privacy more vulnerable. While the ratings and reviews discussed in this

[14] Available at: https://otzovik.com/term.php (accessed: 15.09. 2020)

[15] Available at: http://www.investigacion-psicopedagogica.org/revista/articulos/24/english/Art_24_570.pdf (accessed: 9.12. 2020)

article are not the greatest threat to privacy, this area of Internet activity is interesting insofar as it leads to the conflict of different interests such as

the freedom of speech;

the right to privacy;

the interest in obtaining full information about the professional qualities of a specialist or the qualities of a product.

In themselves, ratings are just a means that is neither good nor bad. They existed before the appearance of the Internet (for example, the most popular actor, a best-selling book, etc.).

The advent of the Internet simply made ratings more convenient and accessible. Today, all Internet users have an opportunity to participate in the assessment (rating) process and see the material "traces" of their participation.

There is even a peculiar fashion for ratings today. It is useless (and unnecessary) for legislators to fight this process. The task of legislators and judicial practice is only to set down the acceptable boundaries of these freedoms.

The most important problem for court practice is harmonizing the freedom of speech with the ban on the use of personal data without the consent of the person to whom this data relates.

Almost every rating site that evaluates specialists indicates their first and last name, place of work, and even phone number. The best scenario is when personal data is posted on rating sites only with the consent of the person concerned.

Encroachments on privacy in the name of progress, innovation, and ordered liberty jeopardize the continuing vitality of the intellectual culture that we endorse today [Cohen J., 2013: 1904–1933].

Another important issue is the subject of liability. If a publication containing inaccurate and defamatory information indicates the name of the author, the latter is liable for the publication. However, if it is anonymous, then the only protection option for a person whose intangible benefits it affects is to contact the site owner. The site owner becomes liable only if, after receiving a claim from the person concerned, he does not take reasonable measures to verify the complaint or, after receiving evidence of the inaccuracy of the information specified in the complaint, does not delete the defamatory review and indicate its inaccuracy.

References

Barendt E. (2016) *Anonymous Speech: Literature, Law and Politics*. L.: Bloomsbury, 200 p.

Cheung A., Schulz W. (2018) Reputation Protection on Online Rating Sites. *Stanford Technology Law Review,* no 21, pp. 322–326.

Cohen J. (2013) What Privacy is For. *Harvard Law Review,* vol.126, pp. 1904–1933.

Erdos D. (2018) Intermediary publishers and European data protection: Delimiting the ambit of responsibility for third-party rights through a synthetic interpretation of the EU acquisition. *International Journal of Law and Information Technology,* vol. 26, pp. 189–225. Available at: https://academic.oup.com/ijlit/article-abstract/26/3/189/5033541 (accessed: 09.08.2019)

Erdos D. (2015) From the Scylla of Restriction to the Charybdis of License? Exploring the Present and Future Scope of the 'Special Purposes' Freedom of Expression Shield in European Data Protection. *Common Market Law Review,* vol. 52, pp. 119–154.

Hinz A. (2011) Attitudes of German Teachers and Students towards Public Online Ratings of Teaching Quality. *Electronic Journal of Research in Educational Psychology*, no 24, pp. 745–764. Available at: http://www.investigacion-psicopedagogica.org/revista/articulos/24/english/Art_24_570.pdf. (accessed: 19.12.2019)

Roessler B. (2005) *The Value of Privacy.* Cambridge: Polity Press, 288 p.

Ruhmkorf A. (2014) Ratemylegalrisk.com — The Legality of Online Rating Sites Relating to Individuals in Data Protection Law. *Intellectual Property Forum*, vol. 96, pp. 8–9, 55–67.

Scaife L. (2015) *Handbook of Social Media and the Law*. N.Y.: Informa Law, 388 p.

Scheuer A., Schweda S. (2011) The Protection of Personal Data and the Media. *Limits to the Use of Personal Data*, no 6, pp. 7–28.

Schoeman F. (1992) *Privacy and Social Freedom.* Cambridge: Cambridge University Press, 240 p.

Schulz W. (2018) Regulating Intermediaries to Protect Privacy Online — the Case of the German NetzDG. HIIG Discussion Paper Series, 2018-01. Available at: https://www.hiig.de/wp-content/uploads/2018/07/SSRN-id3216572.pdf. (accessed: 11.12.2019)

Serna F., Iniesta J. (2018) The delimitation of freedom of speech on the Internet: the confrontation of rights and digital censorship. Available at: https://pdfs.semanticscholar.org/6220/95b49c43687ba4766e1888f5bbdaa46559c5.pdf?_ga=2.69714838.764201525.1565323822-198308019.1565323822 (accessed: 11.12.2019)

Strahilevitz L. (2008) Reputation Nation: Law in an Era of Ubiquitous Personal Information. *NW. L. Rev.*, vol. 102, pp. 1668–1738.

Ungern-Sternberg S. (2019) *Demokratische Meinungsbildung und künstliche Intelligenz* (Democracy, Public Opinion Formation, and Artificial Intelligence). In: Antje von Ungern-Sternberg S. *Demokratie und Künstliche Intelligenz*. Tübingen: Mohr Siebeck, pp. 1–28. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3400756 (accessed: 11.12.2019)

Comment

Fake News: Legislation and Judicial Practice

Liudmila Tereschenko

Associate Professor, Department of Administrative Legislation and Procedure, Institute of Legislation and Comparative Law under the Government of the Russian Federation, Doctor of Juridical Sciences. Address: 34 Bolshaya Cheremushkinskaya Str., Moscow117218, Russian Federation. E-mail: adm2@izak.ru

Abstract

The article examines relations new to Russian practice regarding the introduction of the concept of "fake news" into the legal field, dissemination of fake news and the problems of legal enforcement of the indicated norms, including administrative and criminal liability.

Keywords

fake news, information security, disinformation, Internet, false information, harmful information, freedom of speech, administrative liability, criminal liability.

For citation: Tereshenko L.K. (2020) Fake New: Legislation and Judicial Practice // *Legal Issues in the Digital Age,* no 3, pp. 140–147.

DOI: 10.17323/2713-2749.2020.3.140.147

False information has always existed alongside genuine information. The legislator may describe it in differing ways: false information, deceptive information, disinformation, falsified information, but in recent years the term "fake news" appeared at first in literature, then in legislation. It cannot be said that all the abovementioned terms convey an identical meaning, but they do stress the one common characteristic of specific information — its invalidity, inconsistency with reality, and actual state of affairs.

The reasons for the invalidity of information can vary (incorrect selection of the methodology of a study, an inadequate empirical base in scientific and/or sociological studies, deliberate falsification of data, knowing dissemination of false information, etc.) From the legal viewpoint the most interesting and important issues are situations in which the creation and dissemination of false information

are deliberate and exercise a negative influence on the information security of both individual persons and society as a whole.

State attention to the problem of knowing dissemination of fake information has grown considerably due to the widespread use of the Internet by various social strata, and in the face of the COVID-19 pandemic this problem has increased greatly in importance, and in view of its global nature, governments are striving to find the best way to resolve it[1].

Knowing fake information may also pursue different aims and be shaped by various purposes, including: concealment of its identity (creation of an account in the name of another person, or a non-existent one) and dissemination of fake information from another's name; increasing the significance of the fake information by claiming expertise in a specific field, creation of tension, public panic, performance of fraud, etc.)

In the conditions of the COVID-19 pandemic, fake information has been employed often in fraudulent activity. For example, internal affairs bodies have been receiving information concerning the sending of fraudulent SMS messages to citizens, demanding payment of fines for alleged breaches of self-isolation, that must be paid immediately[2]. The term "fake" now refers not just to information, but to sites that are confusingly similar to official sites, to which the recipient is instructed to transfer payment of a fine.

However, the danger of fake information is not limited to fraudulent activities, it extends to fake information regarding the coronavirus infection itself, its spread, methods of countering it and so forth. The Internet contains an enormous body of information about COVID-19, much of it quite contradictory. People are warned about the danger of inoculations that may have a negative effect on their health and even pose a threat to their lives, advising refusal to inoculate; that bodies of state power are allegedly considering forced inoculation, etc. Other information claims

[1] See, for example, Philippines Act of 2017 "On the knowing dissemination of false information and other related illegal offences." False information causing panic, chaos, discord, violence or hatred, as well as information containing elements of propaganda aimed at smearing or discrediting a person; Singapore Act of 2019 "On protection from the Internet dissemination of fake information and manipulations." Establishment of criminal liability for publication of fake news; Germany Act of 2017 Net Enforcement Act (NetzDG). Malaysia Anti-fake News Act of 2018 envisages punishment for initiation of false information and reposting of the same. Fake news are any news, information, communications and reports that are fully or partially false irrespective of format (journalistic or newspaper article, television program, video/audio recording, other format capable of conveying words and thoughts), as well as legal literature: A.D. Scherbakov, Fake news as an object of criminal/legal regulation: Malaysian experience // Miezhdunarodnoye ugolovnoe parvo i jurisprudentcia. 2018. N 4. P. 18–21 (in Russian); A.N. Ilyashenko. Z.I. Khisamova. Aspects of bringing to book on criminal charges for disseminating fake news in social networks in pandemic conditions // Rossiysky sledovatel. 2020. N 9. P. 12–15 (in Russian)

[2] For greater detail see N.D. Denisov. Negative changes in cybercrimes in the pandemic period and means of countering them // Bezopasnost biznesa. 2020. N 4. P. 37–42 (in Russian)

that the new coronavirus epidemic is no different from customary influenza, so there is no need to observe the recommended heightened measures of public safety (observing social distancing, use of gloves and face masks, inoculations, etc)[3]. As a result, people are provoked into actions endangering life and health, and hindering the reduction of the coronavirus threat.

A heightened degree of the public danger posed by fake information regarding the new coronavirus infection presupposed the reaction of the state to its dissemination. The Federal Law of 18.03.2019 № 31-FZ "On the introduction of amendments to Article 15.3 of the Federal Law "On information, information technologies and protection of information"[4] established the concept of "false socially significant information", denoting "information disseminated under the guise of reliable communications that pose a threat to the life and (or) health of citizens, property, the threat of mass violations of public order and (or) public safety or the threat of disruption of the functioning or termination of life support facilities, transport or social infrastructure, credit organizations, energy suppliers, business activity or communications."

It is important for law enforcement activity to correlate this determination with a list of socially significant diseases and a list of diseases that endanger the surrounding public. The indicated lists have been affirmed by the Resolution of the Government of the Russian Federation of 1 December 2004 № 715 "On approval of the list of socially significant diseases and list of diseases that pose a danger to others"[5]. In the new version of this resolution, dated 31 January 2020, the coronavirus infection was included in the list of diseases that pose a threat to the surrounding public.

Simultaneously with the determination of the Federal Law "On information, information technologies and protection of information" the concept of "false socially significant information" was addressed by Federal Law № 27-FZ of 18.03.2019 "On amendments to the Code of Administrative Offences of the Russian Federation"[6] (hereinafter — CoAO). Article 13.15 of the CoAO was augmented by parts 9–11, pursuant to which the dissemination of information endangering the life and health of citizens, property, posing the threat of mass public disorders and threatening the functioning of life support facilities carry the following administrative fines:

for a first offence by private citizens — 30 to 100 thousand rubles; for public officials, 60 to 200 thousand rubles; for legal entities, 200 — 500 thousand rubles;

[3] See, for example, the Resolution of the Ikryaninsk district court in the Astrakhan region dated 22.06.2020 on case № 5-193/2020.

[4] Rossiyskaya gazeta. 20.03.2019.

[5] SZ RF. 2004. № 49. Art. 4916.

[6] SZ RF. 2019. № 12. Art. 1217.

for a repeated offence by private citizens — 100 to 300 thousand roubles; for officials, 300 to 600 thousand rubles; for legal entities, 500 thousand to 1 million rubles.

If the dissemination of fake information has caused "a person's death, caused harm to a person's health or property, provoked mass public disorders and (or) endangered public safety, termination of the functioning of life support facilities, threatening transport or social infrastructure, communications, credit organizations, energy supplying objects or business activity", the fines are increased correspondingly:

for private citizens — 300 — 400 thousand rubles;

for public officials– 600 — 900 thousand rubles;

for legal entities — 1 million — 1,5 million rubles.

The increasing danger to the public caused by fake information in the conditions of the spread of coronavirus infection has indicated the need to introduce not just administrative liability, but criminal liability. In 2020 the Federal Law of 01.04.2020 №100-FZ "On amendments to the Criminal Code of the Russian Federation and Articles 31 and 151 of the Criminal Procedure Code of the Russian Federation"[7] introduced criminal liability for the public dissemination of knowingly false information under the guise of reliable information regarding circumstances posing a threat to the life and safety of citizens and (or) measures being enacted to ensure the safety of the population and territories, methods and means of protection against the indicated circumstances (Art. 207.1 of the Russian Criminal Code), and the public dissemination of knowingly false information in the pandemic period (Article 207.2 of the Russian Criminal Code).

Within the short period of the introduction of criminal liability for the public dissemination of knowingly false information it became clear that questions requiring clarification arose in court practice, pursuant to which the Supreme Court of the Russian Federation conducted an amalgamation of separate questions of court practice relating to the application of legislation and means of countering the spread of the new coronavirus infection (COVID-19) on the territory of the Russian Federation, and presented its findings in reviews № 1 and № 2 "Review on selected issues of judicial practice related to the adoption of measures to counter the spread of a new coronavirus infection (COVID-19)"[8].

One of the main questions at present is the matter of accessibility to justice for private citizens and legal entities in pandemic conditions. In the report presented

[7] SZ RF. 2020. № 14 (part I). Art. 2030.

[8] See Review on selected issues of judicial practice related to the adoption of measures to counter the spread of a new coronavirus infection (COVID-19) on the territory of the RF № 2" (approved by the Presidium of the Supreme Court of the RF on 30.04.2020). Available at: URL: https://www.vsrf.ru/files/28856 (accessed: 18.09.2020)

by Vyacheslav Lebedev, Chairman, Supreme Court of the Russian Federation, at the Forum of chairmen of the supreme courts of BRICS countries "Protection of consumers' rights in contemporary economic conditions", attention of the courts was drawn to the circumstance that the terms for procedural activities missed due to measures for countering the spread of the coronavirus infection (limitation of citizens' freedom of movement, their presence in public places, state or other institutions) are subject to reinstatement in accordance with procedural legislation. The Chairman of the Supreme Court of the Russian Federation noted that the lack of opportunity for a timely approach to a court with a claim is also grounds for the restoration of limitation periods for claims"[9].

As was noted earlier, criminal and administrative liability were introduced regarding fake news. Pursuant to this, a question of principle arose in practice: what criteria differentiate administrative liability for breaches of the law envisaged by parts 9 and 10 of Article 13.15 of the Russian CoAO from criminal liability under Article 207.1 of the Criminal Code in the event of a physical entity disseminating knowingly false information about the new coronavirus infection (COVID-19) in the mass media and information and telecommunication networks under the guise of reliable information?[10] The difference between illegal actions carrying criminal liability and administrative liability is surely the first question requiring a definitive answer, a mandatory condition for bringing to book, as parts 9 and 10 of Article 13.5 of CoAO indicate that an entity is charged with administrative liability if the actions of the entity disseminating knowingly false information do not contain elements of criminal liability.

Let us compare the norms of Article 207.1 of Criminal Code and parts 9 and 10 of Article 13.5 of CoAO. However, it must be mentioned at the outset that amendments concerning fake information were included in the CoAO article entitled "Abuse of freedom of information", thereby linking it to the mass media.

The Criminal Code established that "The public dissemination of knowingly false information under the guise of reliable information concerning circumstances posing a threat to the life and safety of citizens, and (or) measures employed to ensure the safety of the population and territories, means and methods of protection in the indicated conditions…" Clearly, the Criminal Code contains no indication of the means of the public dissemination of fake information, the main issue being the fact of its public dissemination.

In its Review, the Russian Supreme Court draws attention to the circumstance that within the framework of criminal liability, the public dissemination of knowingly false information may be manifested not only in the use of mass media and information and telecommunication networks, but also in the dissemination of

[9] SPS Konsultant Plus.

[10] Question 13 of review № 1.

such information by public appearances, meetings, distribution of leaflets, display of posters, etc.

Part 9 of Article 13.5 of CoAO describes the same situation in more detail, and stresses the role of the mass media, and information and telecommunication networks: "The dissemination of knowingly false socially significant information in the mass media under the guise of reliable information, causing a threat of damage to life and (or) health of citizens, property, threat of mass violations of public order and (or) threatening the functioning or termination of life support objects, transport or social infrastructure, credit organizations, energy supplying objects, business activity or communications…" and part 10 of the same article envisages liability for "the dissemination of knowingly false socially significant information in the mass information media and also in information and telecommunication under the guise of reliable information resulting in the creation of obstacles to the functioning of life support objects, transport or social infrastructure, credit organizations, energy supplying objects, business activity or communications. Furthermore, Article 13.15 was later augmented by two more parts: 10.1 and 10.2 concerning the same issues.

The position of the Supreme Court of the Russian Federation in the matter of differentiating criminal and administrative liability comes down to the following. The actions of a physical entity may contain elements of punishable criminality and be qualified under Article 207.1 of the Criminal Code if they occur in the public dissemination of knowingly false information, under the guise of reliable information, concerning circumstances threatening the life and safety of citizens, including circumstances of the spread of the new coronavirus infection (COVID-19) on the territory of the Russian Federation and (or) measures employed to ensure the safety of the population and territories, methods and means of protection in the indicated circumstances, and such dissemination of knowingly false information with consideration of the conditions in which they are performed, the aims and motives behind such actions (for example, provoking public panic, disruption of law and order), pose a genuine public danger and damage relations in the sphere of social security that are protected under criminal law.

Furthermore, the criteria for differentiating between the administrative liability envisaged by parts 10.1 and 10.2 of Article 13.15 of CoAO and the criminal liability envisaged by articles 207.1 and 207.2 of Criminal Code are viewed by the Supreme Count as subject composition. The Review notes that differentiation must be performed in accordance with the subject of the breach of the law. Administrative liability for actions envisaged by parts 10.1 and 10.2 of Article 13.15 of CoAO concerns only legal entities. Citizens, including public officials, managers of a legal entity may be charged with criminal liability if their actions contain components of a crime covered by Articles 207.1 and 207.2 of the Criminal Code.

The components under study relevant to the CC RF and CoAO contain categories of evaluation, and also indications of circumstances the content of which is covered by other legislative acts. For instance, the question arises what should be deemed circumstances that pose a threat to the life and security of citizens (art.207.1 of the Criminal Code). The answer to this may be found in the notes to the same article and in a great number of legislative norms concerning emergency situations of a natural or technogenic nature. The notes indicate that circumstances threatening the life and safety of citizens are deemed to be emergency situations of a natural or technogenic nature, ecological emergencies including epidemics, epizootics and other situations caused by accidents, hazardous natural occurrences, catastrophes , natural and other disasters causing (capable of causing) human victims, inflicting damage on people's health and surrounding ecology, significant material losses and disruption of the livelihood of the population. Such a position served as grounds for the Supreme Court of the Russian Federation to relegate the circumstances of the spread of the new coronavirus (COVID-19) infection on the territory of the Russian Federation to circumstances that threaten the life and safety of citizens as indicated in the note to article 207.1 of the Criminal Code of the Russian Federation and clause 2 of notes to article 13.15 of the Code of Administrative Offences of the Russian Federation regarding administrative breaches of the law.

Evaluation categories should include, for example, such terms as "knowingly false information" regarding circumstances that threaten the life and security of citizens", "publicly disseminated information" and "socially significant information." It is very difficult to prove that an individual disseminating a specific piece of information is aware of it being "knowingly false" because he may be sincerely convinced of its objectivity due to the reliability of the source of that information. For such a situation the Russian Supreme Court has established that knowingly false information is deemed to be information (news, communications, data, etc.) that is initially inconsistent with reality, and was known to be so by the disseminator.

There is also a problem with the relegation of publicly disseminated information to the socially significant category. It is not by chance that alongside amendments to the CC RF and CoAO RF, changes were made to Federal Law № 149-FZ of 27 July 2006 "On information, information technologies and protection of information" concerning the nature of socially significant information.

Regarding circumstances threatening the life and safety of citizens, it is important to bear in mind the mention of the coronavirus in an earlier Resolution of the Government of the Russian Federation of 31 January 2020 № 66 stating circumstances of the spread of the new coronavirus infection on the territory of the RF relate directly to circumstances that threaten the life and saafety of citizens. The qualification of actions by a physical entity under art. 207.1 CC RF is also influenced by the aims and motives behind the actions in question.

In the course of law enforcement procedure there may be a question concerning such a sign as the degree of public nature in the dissemination of information. In the view of the Russian Supreme Court (question 13 in its Review) the knowing dissemination of fake information shall be deemed public if such information is addressed to a group or an unlimited number of persons and is expressed in any form accessible to them. Moreover, it is advisable to take other circumstances into account, including places, method of dissemination (e.g. the mass posting of messages to mobile communication subscribers, use of messaging services such as WhatsApp, Viber and others.

We find it regrettable that practically no use is made of the conceptual framework set out in the Federal Law "On information, information technologies and protection of information" determining actions performed with information. This envisages access to information, provision of information and dissemination of information where access to information is the possibility of receipt of information and its use; provision of information mean actions aimed at the receipt of information by a specific circle of persons or transfer of information to a specific circle of persons; dissemination of information means actions aimed at receipt of information by an indefinite circle of persons or transfer of information to an indefinite circle of persons.

As a result, practically any operations with information are regarded in the Review as its dissemination, even if the information is received by a clearly specified circle of recipients. Consequently, the sending of a message to several of one's friends on WhatsApp shall be seen by the courts as dissemination of information[11].

In conclusion, we find it necessary to note that the struggle against the coronavirus infection and fake news must not violate the fundamental human right to freedom of speech on one hand, or to soften or revoke the prohibition of censorship, which is guaranteed by the Constitution of the Russian Federation.

[11] See the Resolution of the Buynaksk city court in the republic of Dagestan dated 02.07.2020 on case N 1-110/2020.

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.