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.