

Who's afraid of AI? Is Romania's judicial security endangered by means of AI tools?

Valentin - Stelian BĂDESCU,

*The author is a lawyer in the Bucharest Bar and an associate scientific researcher of the Institute of Legal Research of the Romanian Academy.
valentinbadescu@yahoo.com*

Ruxandra Ioana BĂDESCU,

*The author is an economist, doctoral student of the Doctoral School of Business Administration within the Academy of Economic Studies in Bucharest.
ruxbadescu@gmail.com*

Abstract

"How can people be connected with technology so that, collectively, the actions of these working entities are more intelligent than any person, group of people, computer, or computer network ever undertaken? The answer can come through two approaches: "the first involves the creation of new ways of interconnection between individuals, obviously facilitated by technology, to potentiate collective intelligence, the second envisages the connection of individuals with systems equipped with artificial intelligence, to generate a higher level of collective intelligence." Artificial intelligence is a component of digitization, being thus deeply interconnected with it and aiming to amplify and facilitate progress in the field. Together, they are driving forces of innovation and transformation in modern society. But for the protection of Romania's judicial security, as well as for the promotion and respect of human rights in the digital age, the time has come for cyber security to be treated as a human rights issue. And that's because cyber security is inexorably linked to the security of individuals, a fact that represents one of the foundations of human rights. Cybersecurity and human rights are complementary, interdependent and mutually reinforcing.

Keywords: artificial intelligence, forensic security, cyber security, human rights, digital rights.

1. Argument - warning: towards a new geopolitical azimuth

In February this year (2024) I was at the theatre, at the Odeon where the play "Who's Afraid of Virginia Woolf?" was playing [1]. I don't like this Virginia. Good song, but it negatively charged me a bit, like the phones that were flashing during the show. It was just one of the avatars of artificial intelligence (AI - Artificial intelligence). And since I didn't have a title for the present work, I compiled theater with scientific research trying to be original. But the originality belonged to another author, Liviu Papadima, who, in an article well done he confessed his fear of the computer [2].

As far as I am concerned, whether I have succeeded or not will be appreciated by you, my readers and judges, and the present work could very well have been titled Challenges and Perils of AI. I said, however, after much thought, Who's afraid of AI? First of all, I think you already know that by AI we mean many others like it, all the devices and gadgets that fill our everyday life with their endless quarrel between nothing and something. I'm not going to list them, you, my readers, know them better than I do. Then maybe you will be confused and say to yourself: "What's the point of fear in this thing?" Well, it kind of is. Where do the letters go when I type? What does it sit on? What do they stick with? Give me back the multiplication table! Give me the grain of the letter on the white paper, when the black tape of the typewriter hits and leaves behind a wonderful mark, if you only erase

it by spreading a ball of paste on top with a fine brush. I first encountered a computer when I was about thirty years old and I was in charge of records and material insurance at a military technical repair section within the 57th Tank Division in Bucharest, a large unit that has been disbanded today. In those years, the 80's of the last century, we had to make the transition from the classic records, on documents, to the computerized one. I worked in parallel, it was double work, I filled out the registers and at the same time kept the cards that I sent to the Army Computing Center, from where I received, like a month after the listing, whole sheets of paper, processed according to the primary data that I sent us. Next came the confrontation of these lists with our registers. There were also errors! Well, 1 and 0, meaning 1 (something) and 0 (Nothing) was doing its job as they knew. Then, at the Military Technical Academy, where the first computer in Romania and the electronic scoreboard of the old Steaua stadium were made.

A little later, I went every day to the Library of the Romanian Academy, I spent hours searching for interesting books through the catalogs with thousands of drawers in which there were, in each, hundreds of cards, each about the size of a palm, stacked one after the other on a kind of iron rods, so that they don't fly out of the files. It was a thrilling search, and after I found something that interested me, I had to fill out another sheet, on which I copied a large part of what was written on the one in the catalog and sat down with her properly in the queue, to end up I handed it to a librarian, who gave it to another, who went in search of the required book. Wow, what a reading factory! Until one day when, arriving at the scene, I was directed to a long hall, with a lot of tables placed along the walls and a lot of readers staring at a bright screen. "No, no - I said desperately to my companion - I want it in the catalog room!" And he, smiling, replied that I could order the books I wanted much more easily online. Let it be! I will never forget how I sat down at the table, with my heart as a flea, with my eyes glued to the instructions pinned to the wall next to me. My hands were shaking from the fire and I had seven tendrils in each finger.

On the table, a keyboard full of buttons, in my head, the firm conviction that at some point I will press the wrong thing and from the screen or from the keyboard - most likely, from both - the Quarrel of Nothing with Something will erupt a flame followed by some thick wisps of smoke, and I will get up and take her to the doctor without looking back. Probably some have not had such dramatic and embarrassing moments. For the youngest, handling these things came as naturally as riding a bicycle or going to the ice rink - although these are not from here or there either. The strange part is not only that some people continue to be afraid of IT, but also that they are afraid of the fearlessness of others. In this paper, you will also find arguments why artificial intelligence is not a threat to humanity, but a huge opportunity.

And now, instead of an argument, on the content, with a preliminary title resuming the question from the title, we discover that man was afraid of any invention that changed his planetary destiny until he understood its meaning. He was afraid of the locomotive set in motion by the power of steam. He was afraid of the mysterious force of electricity, because he associated it with the destructive lightning that fell from the clouds. He was afraid of another, astonishing energy of the atom, because he saw what hell it produced in Hiroshima and Nagasaki, but now he uses it in nuclear power plants. It is true that many

inventions of his own mind—and, without realizing it, he was afraid of himself—were at first deadly, but then they made his life better, carried him, as they say, on the "path of progress". Even now, he is frightened by the onslaught of AI, of robotization, in the not-too-distant future of his android counterpart. Now, the fear is justified because their jobs are threatened, starting tomorrow. But something like this also happened when the mechanical loom war appeared, the electric lathe, the threading machine, the rotary printing press, to give a few examples. In the meantime, synergistic production systems, robotics and mechatronics have become necessary. In less than a century, the entire process of industrial production, changing and moving, according to the Tofflerian vision, from the "factory basket" to virtual technologies such as 3D programs. The road is irreversible. But it depends on how the change produced in the new digital age is managed through AI, which is a commonly used but often misunderstood term that tends to conjure up images of intelligent, decision-making systems - either humanoid robots of the popular imagination, or at least intelligent computer systems capable of substituting human action.

Such systems are certainly included in the AI category, but so are other less sophisticated systems. Indeed, as a term, "AI" is so broad and imprecise that it is of limited use in analyzing the ethical and legal issues arising from its use. A measure of this lack of precision is that the phrase "Artificial Intelligence" is defined in the Oxford English Dictionary not as a process but as a field of study: "The study of how to produce machines that have some of the qualities that the mind human beings have, such as the ability to understand language, recognize images, solve problems and learn."

However, as the phrase is now more commonly used, it describes various processes performed by computers. Whether a program is run by a general-purpose programmable computer or performs the functions of a highly specialized device such as an automatic door-opening sensor, the use of algorithms is at the heart of all computer processes. An algorithm is a process or set of rules to be followed in calculations or other problem-solving operations. Such algorithms are represented by a structured series of logical steps, each of which is able to receive an unambiguous answer, and whose structure can be represented visually with the help of a graph. The use of algorithms predates the invention of computers.

Algorithms have been used by mathematicians for millennia, but only with the invention of machines capable of processing algorithms - that is, computers - have they come to be an inevitable influence in all areas of our lives. Some algorithms, while not intrinsic threats to our fundamental rights and freedoms, can still cause legal problems. For example, if a door open sensor malfunctions while a person is walking through the door, the door could close on them and injure them. Other algorithms such as a system sophisticated sorting and decision-making on applications for a job, can affect human rights. Some algorithms may even be able to affect the rule of law and other democratic principles. Clearly, the pervasive nature and increasing sophistication of computer algorithms requires a prudent and coherent response to the multiple problems that may arise from their use. Therefore, when considering legal issues arising from the use of computer systems, it is useful to distinguish between cases involving simple algorithms and those where algorithms operate in a more complex and non-transparent manner.

As useful as these distinctions can be, it is counterproductive to become obsessed with what is essentially a definitional game. When defining the term "AI", some people would include any algorithm processed by a machine, whether a programmable computer or a chip to open a door, while others would restrict the use of the term to only more complex algorithms. There may even be discrepancies within any group as to what programs do or do not qualify as "AI." I believe that human AI will open the door for us to meet other intelligences in the Universe, but it can induce challenges and dangers even as ChatGPT, Bing AI, Amazon Q and others have become generative AI assistants. Despite the fact that they have begun to be used in countless fields of activity, for obtaining information, generating images, writing texts and children's homework, AI assistants present a number of dangers for both users and beneficiaries.

Moreover, cutting-edge technologies such as Virtual Reality, Augmented Reality and Artificial Intelligence are increasingly present in our lives, and their use in the context of e-government is a topic of major interest for researchers and policy makers alike. In recent years, we have seen an exponential growth in the number of AI applications used in government, from electronic voting systems (offline or online – often supported by blockchain technologies) and public service management platforms to behavior monitoring programs citizens and facial recognition systems. Their integration into e-government can bring numerous benefits, including: increasing efficiency and transparency in administrative processes, improving the quality of public services and increasing access to public information. However, there are also concerns about the risks to citizens' privacy and the potential negative impact on individual rights and freedoms [3].

As a result of the in-depth documentation, know that I started to fear the future. It seems that the question is no longer if, but only when artificial intelligence will surpass human algorithms (human intelligence), and then we, bipeds without feathers (as Plato called us), will be put in front of the real risk of losing superiority on Earth. When it does, we will witness the most beautiful own goal of all time. A wonderful own goal from the scissors kick. In a way, the fate of man was linked to that of the dinosaurs, since, if they had not disappeared, it is very likely that none of us, homo sapiens, would have existed. Dinosaurs lived for several tens of millions of years, and we have only a few tens of thousands. Someone says that there are only three zeros, and zero means nothing. The dinosaurs had no choice.

A huge asteroid came and changed, after the collision, the climate of the Earth. Unlike the dinosaurs, man's destiny is largely in his hands because, compared to the dinosaurs, who were not animals endowed with superior intelligence and had no way to anticipate and prevent the Earth's collision with the catastrophic asteroid, man benefit from such a facility. It seems, however, that although man has intelligence, he does not really use it. Let's not forget that, to a certain extent, different from one individual to another, man is the sum of his relations. On the question of the correlation of consciousness and artificial intelligence, Harari said in Homo deus: "Just as airplanes fly faster than birds without ever growing feathers, so computers may come to solve problems much better than mammals

without acquire feelings". Well, AIs will destroy us and they won't even be sorry, because they don't have feelings. It is sad that no one complains to you!

H. Moravec also draws attention, warning: "We, the people, will benefit for a while from their work, but sooner or later, just like in the case of natural children, they (natural intelligences) will follow their own fate , and we, their old parents, will die in silence». An old aphorism says that the wheel turns. Based on this, I believe that before eliminating us, smart devices will make us work, becoming their slaves. Only when we become totally useless will we be eliminated. And so we will see what hell means, but we will not go to another universe, but everything will happen here, where today we are still masters. Until when? Probably not very long, if we don't wake up. What will happen to man, when artificial intelligence will be more and more present in everyday reality, when new technologies will be widely used and information flows will be exponentially faster? People need to ensure that artificial intelligence will be used for noble purposes, for the benefit of humanity. Maybe this way we have a chance against artificial intelligences. There is no foreseeable danger that cannot be removed, as asteroids can be deflected or destroyed by human intervention, natural or man-made pandemics can be prevented or annihilated, and artificial intelligence can be controlled within an appropriate legal framework.

Depending on how we manage the next few years, we may or may not have a future. If we look in history, we will see that outdated weapons or techniques have been taken out of use and taken to the museum. Will this also happen to man? Will he end up in the history museum? It's as if I see a humanoid robot 100 years from now walking around the museum and saying to those it's with: "What you see are humans - primitives who, without understanding why, created us and then became useless .

We believe that they are tired of life or have achieved the purpose for which they appeared. Strange species"! What else could our created successors – artificial intelligences – say? I can hardly imagine. Possibly, he could also say: "Some of the people were brilliant, but, unfortunately, also imbeciles"! I could not contradict them, for even the lower species do not self-destruct. So let's not forget that there is a real risk that AI devices will, in the not too distant future, conclude that humans have become obsolete machines that need to be replaced or that need other operating systems. Let's use our brain, because it is, at least for now, the most sophisticated informational structure in the universe and the impact of technology and the uses we give it will be measured on the way from homo sapiens to homo technologicus.

2. About the impact of technology and the uses we put to it. What we lose and what we gain on the way from homo sapiens to homo technologicus

The massive complication of problems is a revolution in technology greater than the industrial revolution or the dawn of the nuclear age. The end of the world caused by evilly manipulated or out-of-control technology is one of postmodern man's ways of imagining his apocalypse. From the fear of some of the scientists involved in the Manhattan Project that the atomic bomb they tested on July 16, 1945 would could have ignited the atmosphere and led to the extinction of life on Earth to the recent anxieties about the possibility of

general artificial intelligence - software with human-like intelligence and self-learning - becoming a reality that will backfire to those who generated it, the apocalyptic imaginary included, alongside natural cataclysms, a diversity of causes of human origin [4]. Nuclear apocalypse is the scenario where man has the most control over the end. Promethean man, the one who creates the means by which he alters or manipulates his environment eventually invented the fire that has the power to turn his world to ashes. Become masters of the apocalypse because we have the power to trigger it, now we live under its constant threat [5]. We frequently encounter estimates regarding the ability of the current nuclear arsenal to destroy the planet [6]. The outbreak of a nuclear conflict between the great powers of the world seems a rationally inconceivable scenario; for this reason, we are told, the doctrine of mutual assured destruction guarantees peace: no nuclear-armed entity would dare launch a nuclear attack for fear of the catastrophe that would follow. It is a theory that does not take into account the human errors that could generate such a conflict and, starting from the hypothesis of rational decisions, ignores the fanaticism of those for whom the reward from a world "beyond" justifies any action, including the destruction of the world "beyond" here".

A known threat seems less unsettling than an assumed one. We do not think obsessively about nuclear winter, just as residents of a region with strong seismic activity do not think every day that they might lose their lives in a devastating earthquake, even though the probability of one occurring is higher than elsewhere, of the world. Instead, the specter of imagined catastrophes generates intense anguish. Genetic engineering, biotechnology, nanotechnology or artificial intelligence are just some of the subjects of catastrophic scenarios that start from the premise of technology out of control.

Concern about the negative effects of some interventions on nature about which man has not reflected enough is not recent. Fictionally, we first encounter it in Mary Shelley (1831), whose *Frankenstein* is the result of an experiment carried out without concern for the consequences, and later, in the rich science fiction literature built around this theme. In reality, generative artificial intelligence is the latest example of a technology whose impact has only begun to be glimpsed and whose regulation has only become a concern after its launch [4].

From microchips to artificial intelligence to quantum computing, emerging technologies are transforming the world, including our lives. In many ways, despite some obvious advantages, these developments make our work harder than ever, giving us powerful new tools to confuse, evade and spy on us. And yet, no matter how much the world changes, life remains an interaction between people and technology. There will continue to be secrets that people can find out and clandestine interactions that only those in charge know. Technological advances, particularly in signal intelligence, have not rendered such human operations irrelevant, as some predicted, but have revolutionized their practice.

To be effectively connected and informed in the 21st century, we must combine a mastery of emerging technologies with the interpersonal skills and individual daring that have always been attributes of the human personality. That means having the tools and knowledge to operate in a constantly technologically surveilled world. Perhaps, even in

the future, equipped with sophisticated AI models that can digest huge amounts of open-source information so that we can make value judgments [7]. It is a time of historic challenge for all of humanity, with geopolitical and technological change posing as great a test as any we have ever faced. Success will depend on combining traditional human intelligence with emerging technologies in creative ways. It will require, in other words, adapting to a world where the only sure prediction about change is that it will accelerate [4].

The fear of losing control of the results of our technical-scientific inventiveness is sustained by the speed with which we produce and perfect them. The pace of technological progress puts under pressure our ability to reflect on their impact, and the motivation to develop ever better performing technologies that perform tasks better and/or cheaper than the competition, so to make a difference from the point of view economically, to generate profit discourages the very triggering of this reflection. Even when it is realized, how effective can such a predictive approach be? Günther Anders believes that man has become unable to adequately represent the tools he creates, which are increasingly complex and autonomous in relation to their fatally limited human producer [8]. The gap between the ability to produce tools with advanced functions and the ability to represent them to us does not cast our claim to predict all their effects in a favorable light.

In 1993, scientist and sci-fi author Vernor Vinge described an "opaque wall" that prevents us from imagining what society will look like after - and if - the technological singularity becomes a reality, i.e. after the moment when a machine would become more intelligent than man [9]. At that point in their evolution, the technologies would be so advanced that they would irremediably exceed our ability to understand or control them; what would follow is impossible to predict precisely because we will have lost control.

If, for example, artificial intelligence were to become adaptable, autonomous, able to make its own decisions, perform tasks for which it was not specifically programmed and understand the context in which it acts, there would be a risk not only of taking control but also decide that we are dangerous and/or useless, therefore dispensable, and act accordingly. The end brought about by the fundamental changes produced by the singularity at the level of society is one of the technological apocalypse scenarios.

The unpredictability of the technological future is reflected in the contradictions in the opinions of specialists regarding the time, manner or possibility of producing some supposed radical changes. While the techno-pessimists make apocalyptic predictions, the techno-optimists project paradisiacal images onto the "opaque wall". Modern utopians believe that progress is inevitable and directly driven by the evolution of technology, which will solve all of humanity's problems and lead to the emergence of the perfect society. As the promise of a perfect society is familiar in our part of the world, we know the danger of the illusion of infallibility built on the foundation of a good cause. Blind trust in the positive purpose of technology cancels the critical approach to its impact in society and represents one of the greatest risks for the future [4]. In this regard, we will proceed further to analyze the challenges and dangers of AI.

3. Technology, the drug of the digital age or about the challenges and dangers of Artificial Intelligence

3.1. Specific matters

"How can people be connected with technology so that, collectively, the actions of these working entities are more intelligent than any person, group of people, computer, or computer network ever undertaken? It is the question that Mr. University Professor asks himself. dr. Cătălin Vrabie in his cool volume, offering us two approaches: "the first involves the creation of new ways of interconnection between individuals, obviously facilitated by technology, to enhance collective intelligence, the second considers the connection of individuals with systems endowed with intelligence artificial, to generate a higher level of collective intelligence [10]. Artificial intelligence is a component of digitization, being thus deeply interconnected with it and aiming to amplify and facilitate progress in the field. Together, these are driving forces of innovation and transformation in modern society [11].

Artificial intelligence is the field of science and engineering concerned with the theory and practice of developing systems that exhibit the characteristics we associate with intelligence in human behavior. There has been a lot of talk about artificial intelligence, with claims that AI agents will become more intelligent than humans and even show humanity. As with any new and powerful technology, artificial intelligence comes with risks and opportunities. Many human jobs will be done by machines, but these are all algorithmic jobs, leaving the truly creative ones to humans.

Most importantly, AI can help us become better critical thinkers, which is the best way to preserve democracy. From this perspective, the fear is unjustified, since artificial intelligence differs fundamentally from human intelligence, being complementary, artificial intelligence being better at some tasks, but unable to perform others that can be performed by human intelligence. AI is the field of science and engineering concerned with the theory and practice of developing systems that exhibit the characteristics we associate with intelligence in human behavior, such as perception, natural language processing, problem solving and planning, learning and adaptation, and acting on the environment.

The main scientific goal of artificial intelligence is to understand the principles that enable intelligent behavior in humans and artificial agents. This scientific goal directly supports several engineering goals, such as developing intelligent agents, formalizing knowledge, and mechanizing reasoning in all areas of human endeavor, making working with computers as easy as working with humans, developing human-machine systems by exploiting complementarity between human and automated reasoning [12].

I am not one of the strongest supporters of artificial intelligence because I cannot understand what an AI agent can and cannot do. There are indeed some very impressive AI achievements, such as Deep Blue (the IBM chess program that beat world champion Gary Kasparov), AlphaGo, which plays Go better than any human, IBM's Watson, which beat on the best human Jeopardy players and gives AI systems super-intelligence abilities.

The latest is ChatGPT, which represents and integrates what has been posted on the Internet and can answer any question.

It does this by "reading" a large amount of existing texts and learning how words appear in context with other words. They then use what's been learned to predict the next most likely word that might appear in response to a user request, and every word after that. This is like the autocomplete capabilities on search engines, smartphones, and email programs. Its natural language generation capabilities allow it to compose responses and write stories and letters for different age groups and with different levels of detail. Can compose music, essays and poems, write and debug computer programs, play games, generate ideas for creative tasks, write custom resumes and cover letters, etc. These results are so impressive that Geoffrey Hinton, one of the inventors of deep learning, claims that AI can "understand" and even surpass human intelligence.

He points out that they are based on neural networks that already contain more neurons than the human brain and can learn much faster than humans. And yet he is wrong, computers are significantly less intelligent than humans. Talking about the limitations of AI assistants we mean their limited knowledge. Thus, they are trained on a set of data that reaches only up to a certain point in time and therefore, they do not have the ability to provide real-time information or updates beyond that date. Without the ability to verify information AI assistants may provide answers based on misconceptions or misinformation they were trained on.

So, they can generate answers that seem plausible, but are incorrect or meaningless, not having the ability to understand the concept of truth. In addition, it does not assume responsibility for the information provided and the biased, potentially offensive answers that are against ethical norms. They lack the ability to understand the user's intent or the purpose behind a question, generating answers based on patterns learned during training that do not always align with the user's expectations, nor can they provide professional advice, scientific information, or synthesize and analyze of complex data. Furthermore, AI assistants may generate answers that appear coherent, but do not guarantee the accuracy, correctness or timeliness of the information.

Therefore, they should not be used as the sole source for important decisions, especially in areas that require expertise or specialized knowledge, and we should be careful when reading text that appears to be written by an AI assistant. In this sense, I have noticed that there is quite a debate in the scientific community about the natural way in which we choose to develop AI compared to the need to adopt certain guidelines for its development and use. For example, Max Tegmark talks about the need for clear rules in the field of reference, exploiting the possibilities offered by artificial intelligence not only in the immediate future, but also in the distant prospect of colonizing the cosmos. His book, *Life 3.0*, invites us to meditate on the most delicate social, military, legal and ethical issues generated by the development of artificial intelligence, and Max Tegmark's central idea is that we have the capacity and moral duty to influence the evolution of life, including in the legal environment [13].

3.2. Artificial intelligence and legal professionals

I think we also need such a discussion in the field of law: and I think about the possibility of replacing lawyers with robots, given that many of the current tasks performed by lawyers would have the ability to be "digitized". Richard Susskind talks in his book, *Tomorrow's Lawyers: An Introduction to Your Future* [14], about the essential change of the profession in the years to come and how the lawyer will be forced to adopt ad hoc solutions, highly specific to the needs of the clients. In other situations like registering a company, I don't see why people should turn to a lawyer a few years from now. Related to the situation of a robot judge, I have recently watched a very interesting discussion in an article in *The New Yorker* entitled *The Limits of Political Debate* and which considers a technology endowed with Artificial Intelligence that has the ability to debate any topic possible, called Project Debater. Although in the showdown between Harish Natarajan ("the man") and Project Debater ("the machine"), the audience overwhelmingly felt that the debate was won by the man, Benjamin Wallace-Wells' article convincingly explains why Project Debater won the debate given the connection to the classic facts vs. emotions. When the judge and her considerations change, so must the lawyer.

Perhaps because of these considerations, I don't think we should fear AI, either from the point of view of our integrity as a species, or from the point of view of the professional component. Yes, it is possible that some of the work performed by some lawyers will be replaced by robots, but I believe that, for the foreseeable future at least, a significant proportion of legal work will remain solely the purview of human beings. Related to the perspective of some robot judges, maybe here I would talk about a fear.

The act of justice, even if it is not carried out in equity, but based on the principle of legality, must always have a human component. Justice is blind, but I want to believe that it has a soul, within the limits provided by the law. However, I believe that judges could benefit from the support of robots, which would relieve them of some of the mechanical activities they carry out and which would allow them to focus more on the legal issues that are brought before them. From the perspective of what's left for the lawyer and where we rely on technology, I think the essential question is whether we're willing to let AI choose for us. It is quite clear that in the long term the research work of a lawyer will move to AI software in the context where cybercrime represents a serious threat to the basic values of society, clearly endangering human rights, democracy and the state justice.

3.3. Cybercrime

Almost any type of crime can be committed in cyberspace, currently including specific forms of organized cybercrime, extremely difficult to control and combat by judicial bodies. The use by criminals of information and communication technology in their antisocial actions has led to the emergence of a distinct branch of the criminal phenomenon - cyber or computer crime - which presents additional specific features compared to the classic criminal phenomenon.

A *modus operandi* through the use of servers, IP addresses, networks and systems spread over the entire geographic territory of the world map calls for a social reaction adapted to the new times that in turn uses new technologies, specialized training of investigators and

judicial bodies and a legal framework to match to meet these new realities. Apart from adapting the means and methods of criminal investigation, one of the biggest challenges is the interpretation and application of the principle of territoriality of the criminal law and, consequently, the definite determination of the criminal jurisdiction applicable to concrete cases of cybercrime [15]. International doctrine has already signaled that the increasing threats posed by the digitization of almost every human activity require new ways of approaching the problem of territoriality and that it is extremely important to distinguish between what is here and what is there in an electronic form [16].

The Internet is not a space of non-law, despite the expression of isolated contrary opinions [17]. However, it is difficult to define an Internet right or even a criminal Internet right at the present time. As a consequence, the Internet obeys existing legal norms and jurisprudential principles from objective reality, but the digital environment exerts a corrosive action on the law, and the legal system is now at a turning point. The term "cyberspace" was used for the first time by the writer SF William Gibson in the work *Neuromantul*, the author imagining a space populated by millions of users connected to a "consensual hallucination" [18].

Virtual reality becomes the "new reality", an alternative reality where the rules of objective reality undergo mutations. Cyberspace promised us a type of society that the space of our reality would never allow: freedom without anarchy, control without governance, consensus without power [19]. While the "world wide web" (www) network is global, transnational, law in general and criminal law in particular remain traditional and national, although there is more and more interference, an eloquent example being that of mutual cooperation in criminal matters. Therefore, the principles of law enforcement in space are no longer compatible with the parallel cyberspace dimension of virtual space that does not overlap physical space. For this reason, some authors talk about a "limitation of the territoriality of subjective jurisdiction" in the context of cybercrime.

Naturally, an introduction to the issue of the application of the law in space in the particular case of cyber crimes implies an incursion into the principles of the application of the criminal law in space as they are provided for in domestic law, but the correct and effective approach requires focusing the scientific approach on the transnational elements of the phenomenon cyber criminal. In other words, law enforcement in space in the case of cybercrimes must take into account the transnational nature of the "online" area. In this virtual space, the classic rule of territoriality established by international law cannot bring clear solutions.

At the same time, being a manifestation of national sovereignty, the rule of territoriality is not easily abandoned. The eventual solutions that sovereign states could reach in their fight to combat cybercrime cannot be limited to the European Union or the Council of Europe, but will have to have a global character. By far, the Budapest Convention of the Council of Europe on cybercrime, to which 65 states parties from all over the world, including the USA, have joined, currently remains the best framework to provide the emergency solutions necessary to achieve justice, while respecting time human rights and established

principles of state jurisdiction. In these conditions, the birth of a new profession appeared more than necessary: auditors of computer systems.

3.4. The birth of a new profession in the digital age: IT Systems Auditors from Romania

In the context of the adoption of the new law on cyber security, which transposes the NIS2 Directive of the European Union, Romania takes an important step in consolidating its expertise in the field of information security. The draft law introduces an innovative and potentially transformative element for the IT professional landscape: the Romanian Computer Systems Auditors Corps. This new entity, provided for in Article 56 of the draft law, is conceived as a professional organization of public utility, not for profit, with legal personality, under the coordination of the National Cyber Security Directorate (DNSC). Its main purpose is to regulate the standards and professional practice of cyber security auditing in Romania having an important role in regulating the standards for the professional practice of cyber security auditing.

He will also be responsible for developing and monitoring compliance with the Code of Ethics in the field. For companies and organizations that require security audits, the existence of a regulated professional body will provide more confidence and predictability in the services received. So, the establishment of the Body of Auditors by Computer Systems in Romania is not only a legislative requirement, but also an important step in the professionalization and maturation of the field of cyber security in the country. This initiative has the potential to create a new category of highly qualified professionals, contributing significantly to strengthening Romania's cyber resilience and aligning it with the best international practices in the field, while also taking into account the respect for fundamental human rights and freedoms in the digital age.

3.5. The relevance of cyber security from a human rights perspective

Are human rights universal? Human rights are equally individual and universal even in the conditions where cybercrime has become a reality of our days. Two millennia of moral and political reflection have gradually affirmed and consolidated this complementarity, but have not yet perfected it. First, the individual nature of these rights was affirmed; shored up in the space designated by the term polis, with its Athenian prototype, Greek philosophy of the classical period, including the works of Plato and Aristotle, could justify slavery, class hierarchy and the exclusion of barbarians.

This limited spatial perspective was overcome with Macedonian dominance over the Greek cities. The leap from polis to cosmopolis was amplified by Alexander the Macedon, who conquered the Persians militarily but was intellectually conquered by the imperial idea. Paradoxically, by denying the individualism of human rights, the imperial idea opened the horizon of universality. In this new political and geographical context, reaffirming the individualism of human rights, the skeptics added to them the feature of universalism. Natural law was, in the thinking of the Greek skeptics, the foundation of both features. Continued in the Roman Republic, and then in the empire, this type of reflection crossed the line between philosophy and legal thought. The subordination of this feature to the Roman imperial idea, however, compromised the universalism of human

rights, by both geographic and political limitation. To be truly universal, human rights must be both recognized and protected in this dimension [20].

Christianity reinforced the universality of human rights through the correspondence between natural reason and divine reason. On this basis, the recognition of the universalism of human rights was associated with a transcendent sanction, designed to ensure the effectiveness of these rules. Texts from the Gospels, patristic and scholastic literature, especially from Thomistic thought, grounded and refined the answers to these challenges. The theological development was overshadowed, however, both by religious confrontations, those within the Christian world and those between this world and other civilizations, as well as by the increasingly extensive and accelerated phenomenon of secularization. Beyond its challenges, modernity opened the way to a new type of reflection - philosophical, moral, political and economic, rationally establishing, through the appeal to natural law, the individualism and universalism of human rights. The results of this type of reflection were taken up both in the efforts to develop political declarations and legal regulations (national, regional, universal) for the recognition and identification of the content of human rights, as well as in the successive processes of building institutions able to ensure the protection effective of these rights.

International legal protection of human rights has a universal dimension, in the UN system, and a regional dimension in the European, Inter-American and African systems. Especially the UN system proved to be a failure, the right of veto in the Security Council being used first by the Soviet Union, then by Russia and China to prevent the application of the principles of the Universal Declaration of Human Rights and the Charter. The only international legal protection system with an effective character is the European one, based on the European Convention on Human Rights (ECHR), since this convention is directly applicable in domestic law, and the European Court of Human Rights in Strasbourg ensures its compliance, through binding decisions; the vulnerable point of this system is the way of enforced execution of the Court's decisions, in the hypothesis that the condemned state does not execute them voluntarily: the intergovernmental mechanism of the enforced execution procedure does not always ensure the exact and timely compliance of the decisions.

By adopting the Charter of Fundamental Rights of the European Union (CFREU), a supranational system of human rights protection was created, which is the most effective, as it also sanctions the violation of these rights by the Union bodies, and its effectiveness is ensured not only through direct application of European law in domestic law, but also through effective means of executing the judgments issued by the CJEU. But due to the multiplication of human rights, the last two legal protection systems risk compromising precisely the universal nature of these rights and thus losing their credibility. Individual rights, justifiably recognized to some persons from minority categories, have been elevated through various legal artifices to the rank of human rights, in the absence of universal character.

However, by their very name, human rights are not particular, dependent on circumstances, but are definitively linked to the idea of universalism, that is, they belong

to all human beings and can be exercised by any of them. If it has been known since the Roman jurists that majority does not mean universal, even more so it should be known today that minority cannot be equivalent to universal. The regionalization of human rights and their confinement in particular areas constitutes a syncope in the evolution of two and a half millennia for the recognition and legal protection on an ever wider scale, according to their universal character.

More seriously, the propaganda of authoritarian and totalitarian states is fed in this way, which masks the very violation of human rights through which truly universal values are defended, according to natural reason: life, physical and mental integrity, safety, freedom and dignity of the person. Two millennia of moral and political reflections and institutional building efforts were not enough to translate into political and legal practice the universalism of human rights, arising from their indissoluble connection with all human beings.

In his opening address to the United Nations General Assembly in 2017, Secretary-General Antonio Guterres pointed out that the growing number of threats to cyber security has made it one of the main threats to international security. In addition to the threat of cyberwarfare, cyberattacks have caused hospital shutdowns, shutdowns of high-power transformers, paralyzed cities, and even compromised the integrity of the democratic process.

As cyber threats become more common, more sophisticated and with increasingly serious consequences, it is no wonder that governments, industry and cyber security experts are stressing the need to strengthen cyber security. But these efforts often overlook the human rights dimension, or worse, perceive it as an obstacle to cybersecurity. This is a false presumption and it is high time it was seen as such. There is no universal definition of cybersecurity. But the definition given by the Freedom Online Coalition's "An Internet Free and Secure" working group is interesting and considers preserving - through policy, technology and education - the availability, privacy and integrity of information and basic infrastructure to make people safer online and offline.

Using the definition of cyber security, it is easy to understand that threats to cyber security - or cyber security - can also represent human rights violations. Denial of information and its basic infrastructure, in the form of network shutdowns, for example, violates a wide range of rights, notably by restricting access to information and the ability of individuals to express themselves, peacefully assemble and associate, but also to enjoy a series of economic, social and cultural rights. There are countless examples of situations where information security is compromised, whether through data leaks for financial gain, mass surveillance by governments, or targeted attacks on human rights defenders or journalists, violating the right to privacy, among many other rights. Violations of communications privacy lead to serious human rights violations, including detention, torture and extrajudicial killings.

While most people will experience some form of cyber insecurity in their lives, even those for whom accessing the internet is a significant challenge, not everyone experiences this

insecurity to the same extent. Human rights defenders, journalists and all those in a situation of marginalization or vulnerability, because of religion, ethnicity, sexual orientation or gender identity, for example, fall into groups sensitive to specific risks. They are more likely to be targeted by government or other surveillance, and the consequences of more general threats such as data breaches, internet shutdowns are often much worse for them because of their special position in society. The more people and things are connected, the greater the risks associated with cyber insecurity.

Unfortunately, governments do not put human rights at the center of the discussion or, even worse, use the excuse of cybersecurity to strengthen their control over the Internet. The development of cybersecurity laws, policies and standards tends to take place in "opaque places" or "safe places" and therefore does not benefit from the input of civil society or human rights experts. This runs counter to a multi-stakeholder approach to internet governance based on the full engagement of governments, the private sector and international organisations. This approach notably excludes the powers and monitoring necessary to protect human rights. Often, discussions of security take place within the confines of the intelligence services or other military or government agencies that are not subject to the scrutiny and scrutiny of the public and civil society.

Cybersecurity is sometimes equated with national security, a sacred sphere where governments can do anything away from prying eyes and, even more, away from public scrutiny. As a result, laws, customs and policies are not defined in a human rights framework and make abuse of power possible. It is becoming increasingly clear that international human rights texts also apply to digital technologies. However, when it comes to cybersecurity, human rights are never at the center of the discussion, and unfortunately, sometimes not even a part of it. This is partly due to the fact that international cyber security debates mainly address the issue of attacks between state actors and therefore fall under the rubric of international security and disarmament. But the content of these debates and the resulting standards have implications for how state actors approach cybersecurity at the national level.

And this is a fundamental problem when the private sector owns and/or operates most of the infrastructure, hardware and software on which the Internet depends. To promote and respect human rights in the digital age, the time has come for cyber security to be treated as a human rights issue. First, the idea that human rights are an obstacle to security must be rejected. Perhaps the most often cited example to demonstrate that human rights would stand in the way of security is represented by the thesis that codification, essential to the enforcement of the right to privacy, impedes the work of justice.

In other words, one cannot diminish cyber security for law enforcement without diminishing everyone's security and endangering human rights. And that's because cyber security is inexorably linked to the security of individuals, a fact that represents one of the foundations of human rights. Cyber security and human rights are complementary, interdependent and mutually reinforcing. In this way, a human rights-based approach to the development of legal norms, policies and practices in cyber security becomes imperative. Cybersecurity risks should never be used as a pretext for violating human

rights. On the contrary, the recognition that individual and collective security is at the very heart of cyber security implies that the protection of human rights should be at the heart of cyber security policy development.

Cybersecurity processes must be multi-stakeholder and inclusive, but also multidisciplinary, both in terms of human rights and technological expertise. This means positioning cybersecurity outside the confines of national security and intelligence agencies and challenging the idea that cybersecurity is primarily a national security issue. Given that citizens are so often asked to make sacrifices in the name of national security, it is essential that these sacrifices are carefully considered in order to maintain a balance of necessity and proportionality. There must be independent monitoring of responses to international security threats to check whether they are justified, there must be more transparency and public debate to ensure national security, which must not be confused with the security of the regime in power. Digital technologies represent a new and unforeseen challenge to human rights and security that will require much more study, research and analysis. As long as cybersecurity and human rights are not seen and treated as complementary, mutually reinforcing sides of the same coin, both cybersecurity and human rights will suffer as *Homo sapiens* becomes *Homo digitalis*.

3.6. From Homo sapiens, Homo digitalis?

After *Homo sapiens*, *Homo digitalis*?! Preparing to hand over the baton? There's been a lot of talk lately about AI. It's fashionable. He's a scumbag or the ace up the sleeve of the progressives. It's not a given, it's built. Eric Yuan, the founder of the Zoom platform and the current CEO of the company, revealed in an interview that they are working on a project to create "digital twins" that can take our place in video conferences and even make decisions on our behalf. This would complement other simpler and more repetitive tasks of the respective clone, such as making phone calls, reading emails, replying to most of them, and flagging those that the digital creature does not consider itself capable of responding to answer [21]. This would translate into a digital duplication, a numerically unlimited version, 3D variant of the natural person, but with the possibility to modify and enhance certain parameters, certain capacities (negotiation). These "digital twins" are controlled and trained by the human individual [22].

If man, the professional, is a whole composed of emotions, of feelings that determine his certain states and reactions, of intuition and creativity, his immaterial clone can only be a synthesis of pre-learned algorithms, so that the being, the man, will always be capable of interaction by empathizing with the client's needs, with his emotions, by creating a natural connection; unless there is an interaction of clones (the clone of the notary or the lawyer, with the digital clone of the client or with the clone of the opposing party's lawyer), in which case we can no longer speak of a professional-client relationship, but of a world parallel, with virtual characters.

Man is the supreme divine creation and no artificial mechanism will be able to substitute him in the interaction with his fellows. Just as AI has as its ideal the perfection of the human mind, the "digital twin" will be a set of algorithms unable to achieve the performance of the professional. For Man was created in the image and likeness of the

Supreme Creator, but he is not without sin and is subject to error, and what he creates in turn, the digital avatar, will only be able to reproduce repetitively predetermined mimicry according to induced mechanical automatisms.

The avatar does not interact with human energy, vibration, environment, has no intuition or presence of mind, no charisma, no grace, no spirit of gentleness or youthful determination, no emotional intelligence, even though one tries to "read" human faces. The avatar is linear, flat, often predictable. The association of the terms "intelligence" and "artificial" is inappropriate, because intelligence is also emotional and is by its essence natural, not artificial. Moreover, one author remarked that the term originated in English, but its translation should be different, that of "intelligent information", because we do not translate the phrase "artificial cleverness" [23].

Mutatis mutandis, what could be the benefits of "computer twins" in the case of liberal legal professions, such as notary or lawyer? Beyond replacing the secretary for performing repetitive and time-consuming tasks, let's think what would happen if the "virtual twin" gave the customer an inappropriate answer! Who would be liable for malpractice or damage to the customer? Obviously, the legal subject is the man, the professional who has assumed the delegation of competence to a machine.

Are we ready to abandon humanity and create parallel digital professions? Let's think about the judicial processes in the Anglo-Saxon system, where there is a lot of speculation about the human factor among the jurors! Will the lawyer clone be able to deliver the same professional performance in the defense of the client? But what if the jurors will be dirigible and predictable clones? How will the clone notary be able to exercise his role as a mediator, bringing peace in the negotiations between the parties, modulating the pride, the unleashed feelings, which often inflame the atmosphere more than in a non-graceful procedure?

The formalism gained over time and proven, in the spirit of the safety of the legal circuit, is a must-have in ensuring a quality legal service, and the trusted third party, to whom the state has outsourced the performance of the solemn act, can only be the notary, the man, the professional, who assumes this task and for the fulfillment of which he is responsible according to art. 1258 Civil Code and Law no. 36/1995.

In the era of technological hegemony, the augmented notary is not a digital clone, but the one who exploits the tools of emancipation and with the craft of the art of law puts them at the service of the litigant. Like any invention, Artificial Intelligence is a gift that must be put to the service of humans. A first step in this sense was made through the adoption at the level of the European Union of the Regulation known as the AI Act, with the role of "literacy in the field of AI". AI should not be rejected out of hand in the liberal professions, but harmonized with the interests of the professional and those of the beneficiaries of the service. Perhaps on a cultural level it will have the role that printing had, of disseminating information and culturalizing the masses, if we have the skill to channel it in this sense, or perhaps on a general level it will have a Promethean

significance, of the fire that creates prosperity or destructive fire, if not guided constructively.

It must be the autopilot, the personal assistant that supports the human factor, but does not remove it. It will be a helpful tool with a beneficial impact if we know how to put it to work under our control, through data and information collection and analysis, research, comparative studies, reports, summaries, controlled interaction, storage and guidance with consultative role, content generation including after dictation, visual content, social media posts, presentations, brainstorming and decision-making support, but never by us surrendering the trust with which we have been invested in the exercise of these noble professions in service people, to algorithms without sensitivity, without life, without fear of God! We have a divine mission, to preach the tilting of the scales of Justice in favor of the idea of just, to put into practice the definition of Law, which must remain "the art of good and equity", and this can only be achieved by the human mind, and not exclusively by a car, no matter how powerful it is!

The specificity of legal professions or, better said, of legal activity is given by the combination of axiological and legal content. Therefore, the jurist cannot limit his scope of knowledge exclusively to legal notions or concepts. This is precisely the reason why the jurist does not allow himself to be comfortable, because in order to avoid limiting the perspective, he must constantly research, in order to correctly apply or adapt the legal norm to a certain political, social and economic context.

Moving gradually to law, this profession can be characterized in various ways, but it is by no means comfortable. From the point of view of its purpose, advocacy is inconvenient and requires constant efforts. Advocacy is uncomfortable, because it searches, and it requires endurance, because searching is a permanent state of mind, regardless of the efforts made. Artificial intelligence is not a new thing, it has only gained momentum in recent years due to its accelerated evolution. Let's think about what a revelation the search function "control + lit. F". This was a pioneer of artificial intelligence, but it only facilitated the effort put into the search, by reducing the time dedicated to this activity. In no case, however, did it replace the research process. It is paradoxical that, used inappropriately or excessively, the function "control + lit. F" can become a limitation of the field of knowledge.

Artificial intelligence should be used with caution, only to facilitate the research and not to delegate this process. Such a transfer would be equivalent to the inhibition of the critical spirit and, implicitly, to the disappearance of the lawyer. Being inert, the lawyer will turn into a simple intermediary between the litigant and the artificial intelligence. This is why we have a duty to implement policies to clarify and make clear to anyone – litigant, judge, prosecutor, young or experienced lawyer – that artificial intelligence cannot replace the research process. Let's not forget that in the bundle of fundamental rights, in the bundle of fundamental human rights, the right to humanism and humanity must be the fundamental right of mankind! And let's remember that all this can only happen by using the principles of ethics and integrity in cyberspace.

4. Applying the principles of ethics and integrity in cyberspace

4.1. Introductory matters

Artificial intelligence has already infiltrated many aspects of people's daily lives. The recent rise of so-called machine learning algorithms has sparked a fundamental discussion about the role that technology should play in our societies and the ethical considerations that must be taken into account when it has an increasing impact on the lives of citizens. Almost 2500 years ago, in his *Nicomachean Ethics*, Aristotle (384–322 BC) conceived of ethics as an individual necessity, which allows the achievement of happiness through the prism of virtue, but also as a collective imperative, necessary to access to a fairer society. Let us imagine today the return of the Stagirite among us and put before artificial intelligence to ask the question of its ethics.

Without a doubt, AI is one of the greatest technical achievements ever achieved, affecting the entire economic and social world, but from the equation of which the notion of ethics is largely absent. Approaching the subject, we note, first, that artificial intelligence and ethics seem irreconcilable, the latter presupposing groping, approaching moral cases in their complex singularity, reluctant to absolute rules; on the contrary, the first one is based on formal and binary contours, rarely dealing with nuances. They are not opposites though; no doubt, an algorithm can be ethical, but for this it is necessary and sufficient, at the same time, to be built with a concern and in an ethical perspective! What then could be the cardinal principles of an ethical AI? In a pure but fatally approximate answer, an ethical artificial intelligence is one with a positive impact on the environment, society and the economy in general.

Still, it is a democratic one, that is, understood by and accessible to all and, last but not least, a humble one, in the conditions in which it gives us the most likely answer and one almost drawn by lot! It is a question of stripping her of *húris* – that immeasurable selfishness that the ancient Greeks rejected out of hand, or in this kind of cases the AI should admit that she does not know and therefore *aidos*, the virtue of disinterestedness and modesty, is preferable. The development of an AI will be the stake of the current century and, consequently, it is necessary to integrate as much ethics as possible into the design and auditing processes of the algorithms. For this, an absolute priority is the widespread dissemination of this culture of ethics, convincing all interested parties of its importance and meanings.

An ethical reflection in the field of AI is possible especially within the EU; in economic-technological competition mainly with the other two "major world empires", the US and China, it promotes an approach more focused on ethics than on investments. In addition, Europe also historically remains the first foyer of philosophical and moral reflection and must continue to be in the leading sector as well. However, the Union's "Ethical Guide to Artificial Intelligence", from 2017, is considered to be based on a conception of man and machine, largely disconnected from reality, which no longer differentiates the living from the mechanical [24].

Seven essential elements (security, privacy protection) for a so-called ethical AI have been defined in order to operationalize ethical applications of artificial intelligence. It is

considered that in order to have AI without prejudices the teams that create them must be multidisciplinary; they need to be composed both by computer scientists and by people active in the social or human sciences. It is also necessary to establish new communication channels between these teams, which usually do not communicate with each other or very little. The idea is to make computer researchers and developers aware of the ethical, legal, and legal implications of their research and writing.

They need to understand that not everything can be studied and analyzed, nor can it be in code. As it will not be possible to have an AI that either 100% ethical, which does not discriminate against anyone or any group. At some point, the enterprise will have to choose between the absolute efficiency of its tool versus its explainability, strike a balance between the two elements. By proclaiming itself neutral and refusing to impose moral norms on the individual, the EU circumscribes itself to the main problem of our age in the matter. Legislating on moral issues vis-à-vis AI has become almost impossible today due to the relativism of our society. There is no longer a common foundation, of universal principles on which to lean. When we no longer know what a man is, we no longer know what a car is either. The modern individual no longer supports any other moral and natural order than his own desire. "The self has become the measure of humanity. And the disconnection from the real, linked to the digital, reinforces this relativism. We are lost in an endless moral wandering. Philosophy and humanity must be reinvested in this field [25].

Three groups of ethical problems brought to attention with the emergence in society of generative artificial intelligences are considered as main ones in substance and more meaningful in the common perception. The first is about controlling and filtering generative AI biases, which come from the data used for learning. Next are the ethical issues that reside in the "emerging capabilities", respectively those developed in this way and were not foreseen *ab initio*, models that can "lie" or invent in certain cases manipulation and influencing strategies that were not intentionally foreseen ; this emerging capacity prepares us many more positive surprises, but, at the same time, it also generates concerns because in this way we can move on to the manipulation of human beings by machines. Finally, the third category of ethical considerations is related to the long-term effects of generative artificial intelligence on humans and society.

In this sense, adaptation to these radical and rapid transformations and their effects on the human condition is involved. Generative AI models are dual technologies that can be used for both good and bad. The main measures provided in the regulatory texts of the field reflect this dual orientation, with the preponderance of one or the other of the perspectives. This is how it happens that while the documents adopted in UNESCO and in that of the Council of Europe insist above all on aspects related to fundamental rights, those related to the OECD and the EU privilege the issues of securing the market and stimulating innovation. The situation is explained by the mission, the object of activity and the nature of the respective issuing structures, beyond which there is also a certain concern generated by the achievement of a balance and a compatibility of the two dimensions of concerns. AI development requires trust, and this is the result of the balance between market and protection.

Undoubtedly, human rights remain a common foundation of action by intergovernmental authorities for a "human-centric" artificial intelligence in the service of humans. At the same time, they are exposed to a double "risk of dilution" in the face of the use of new technologies, in the sense of "weakening" the form and substance of the right. Regarding the form, some soft normative instruments, such as recommendations, guidelines, etc., written in the logic of promoting self-regulation of the actors, propose an ethics of AI. It is thus considered that only soft law regulation would allow a harmonious regulation of this emerging technology.

Regarding the proposed contents, there is a slight mix of genres, in the sense that a significant number of commitments actually resume a series of fundamental rights. It is proper to an ethical norm to be a rule of conduct, free of state sanction, which the actors impose on themselves, or the observance of fundamental rights is not optional, it must not depend in any way on the will of those involved. And this without taking into account the fact that the respective actors are the most powerful of the existing ones, the only ones who impose a norm of behavior. Indisputably, "soft law" presents certain advantages: it is transnational, its rule is agile, unbound from any normative procedure and respected, being accepted by the interested parties. But the privatization of the norm with its corollary disengagement of states is not desirable. While the appeal to fundamental rights can be appreciated as a strengthening through confirmation, normative parasitism carries the risk of degrading fundamental rights, giving the impression that they would not enjoy imperativeness. So, in a more general plan, the ethical norm must articulate with the legal rule and not be substituted for it, and not by rivalry, but by complementarity. Basically, if fundamental rights appear indisputably as a shared objective, criticisms regarding the perception of the related requirements and their guarantee are mainly directed towards the approaches of legal regulation.

Artificial intelligence is a phenomenon of the post-industrial world, it is certain that it will have an increasing impact on our lives. We are told that AI will begin to replace doctors and lawyers, factory workers and managers. However, it seems to me an exaggeration of the phenomenon. Integrating AI into an organization's daily operations requires more subtlety than imagining robot lawyers or doctors. From one point of view, I think AI can help improve many things, and here I am thinking, for example, access to education, healthcare, etc. However, it is essential to ensure that AI is developed and used in an ethical and responsible way to avoid any unintended negative consequences. It is a challenge of modern man, of future generations.

I am optimistic that humanity will rise to the occasion and integrate this phenomenon to its benefit, as it has done with many other challenges throughout time. In this sense, information technology ethics is a discipline that has its roots in the ethical theories of moral philosophy. From its origins, starting with Wiener's works on cybernetics in the 1940s and up to the present day, it is generally accepted that ethical theories of moral philosophy are mobilized to understand and analyze the problems generated by cyberspace. Within moral philosophy, there is a great diversity of ethical theories. It can even be said that there are as many conceptions of ethics as there are recognized philosophers in the field of ethics.

Thus we have: Aristotelian virtue ethics, Kantian deontology, Bentham's hedonic utilitarianism, Levinas' ethics of responsibility/otherness, Jonas's technological responsibility, Morin's ethics of trust, etc. Also, there are as many ethical theories as there are disciplines from the point of view of applied ethics: for example medical ethics, business ethics, etc. On the other hand, we distinguish four major currents of ethical thought in Western moral philosophy: deontological ethics, consequentialist or utilitarian ethics, virtue ethics and pragmatic ethics. To these currents, other non-Western ethical traditions can be added, for example those of African and Asian origin, which may constitute a fifth major ethical current.

4.2. Deontological ethics

Deontological ethics is based on the observance of moral duties that function as absolute restrictions on all behavior. According to deontological theories, any act must comply with the standards, regardless of the consequences. Debt is thus analyzed as an "unconditional practical necessity of action". In other words, an action is moral only if it conforms to moral rules, that is, the action must obey the rules regardless of its consequences. The ethics of information technologies and systems, as a branch of professional ethics, is deeply rooted in the deontological perspective. As such, it promotes good practices and establishes a set of mandatory rules in formulating codes of conduct for IT professionals and, by extension, all users of information technologies and systems within the company. The ethics of responsibility is expressed in a "technological" responsibility and an ethics of alterity. Concretely, the ethics of responsibility is reflected in a renewal of the categorical Kantian imperative through the obligation to maintain the permanence of an authentic life on earth in the face of technological change. The ethics of alterity holds that there is a responsibility towards the other when one discovers the face of the Other.

This ethic is based on "religious transcendence", which means that encountering others is generative of responsibility towards them and requires the prohibition of violence. Discussion ethics is a theory developed within the Frankfurt School and is based on the idea of consensus for ethical-moral research and aims to establish a basic principle for moral deliberation and the evaluation of the validity of norms. Consensus is understood as the agreement of all participants in a discussion.

This theory starts from the postulate according to which neither the truth, nor the cogito, nor the divinity are accessible. Therefore, we are dealing with a transparent communication that refers to the informed choice of a certain set of individuals. At the same time, the ethics of discussion sets the rules for genuine, free and successful communication, that is, transparent communication that promotes mutual understanding in order to reach an agreement; is the communicative process organized around the values of transparency, impartiality, sincerity, truth and relevance.

4.3. Utilitarian ethics

Utilitarianism is a moral theory that is based on the principle of utility and emphasizes the consequence of actions. It is a form of consequentialism in the sense that, for utilitarians, what matters is not the intention of the action, but its effects, results, or consequences. A just moral action is an action whose consequences are good to the extent that it contributes

to maximizing the happiness of the greatest number of individuals. Fundamentally, utilitarianism rests on a hedonistic postulate that the purpose of life is the pursuit of pleasure and the maximization of happiness for all.

The ethics of trust is a form of 'ethics of complexity', in line with complex thinking, and can be broken down into three levels of ethics: an individual or 'self-ethic', a community or 'socio-ethic' and an 'anthropo-ethic'. -ethics". Norbert Wiener is considered the founding father of IT ethics in the late 1940s. Wiener was one of the first authors to explore the ethical and social implications of information technology, in a context that coincides with the first developments of these technologies. His work in ethics, on the other hand, did not resonate with scholars and practitioners of the time. It lasted until the 1980s, when the foundations of what has since been called Computer Ethics were laid, conceived as a branch of ethics applied to technology. Therefore, IT ethics is considered to be a branch of professional ethics (professional deontology) concerning good practices and codes of conduct for IT professionals. Ethics related to the impact of IT based on the four fundamental issues of IT, namely confidentiality, integrity, ownership and accessibility. Since then, new issues have been identified and debated by a relatively dense literature. These include, but are not limited to, protection of personal data, misuse of computer equipment, illegal downloading and computer crime, artificial intelligence, biotechnology and nanotechnology.

The dynamics of contemporary society dictates the need to transform educational processes according to the development of information technologies and their adaptation in order to guarantee fluency and ease of use and updating. The continuous development of information technologies and their widespread application in most human activities have radically changed the face of many industries and inevitably raise ethical questions about the use of these tools.

Indeed, if one considers ethics, conceptually, as a reflection and process that tends to direct behavior towards "right and good actions", it is considered important to understand what realities underlie the ethics of information technologies from the point of view of individual and organizational use, from the point of view of moral positioning, and from the point of view of the type of use, precisely adopted, of "a technology that can lead to socio-technological change". The ethical aspects of several phenomena specific to cyberspace must be taken into account, starting with the politicization of cyberspace, which also includes the ramifications of the "campaigning in cyberspace" phenomenon, followed by astroturfing, information dissemination and the phenomenon of fake news, which captures more and more the information space.

Regarding the politicization of cyberspace, the first high ethical problem lies in the difficulty of attributing a cyber attack, which can be exacerbated by the existence of so-called "false flags", that is, an attacker's manipulations of the technical traces of his attack, the so-called "artifacts" - to mislead investigators about the real origin of the cyberattack. Unfortunately, there are many techniques available to cyberattackers: modifying malware metadata, tools they create and use, falsifying event logs in the victim's infrastructure, which they control, reusing another group's malware or modus operandi cyberattackers

but also opportunism in choosing the target, taking advantage of the existence of a "service" suspect, given the geopolitical situation.

Political campaigns these days are especially easy targets. They are inherently temporary and transitory, lacking the time or money to develop long-term, well-tested security strategies. A large number of new staff are involved, with not much time for training, staff who may bring their own hardware from home as well as malware. Events are moving fast, the stakes are high, and people feel they don't have time to worry about cybersecurity. There are plenty of opportunities for something like this to go wrong. At the same time, campaigns increasingly rely on proprietary information about voters, donors and public opinion. It also stores sensitive documents such as opposition research, vulnerability studies, personnel vetting documents, political documents and emails on various servers.

The risks of a potential attack are increasing and so are the consequences of a cyberattack, and the ethical issues that such a situation can generate are many and thorny. If we analyze the ethical dimensions of astroturfing [26] we can consider that it was created in order to fulfill the agenda of a corporation, by manipulating public opinion and disregarding scientific research, representing a serious escape from ethical behavior. While from a legal or ethical point of view the phenomenon of "astroturfing" can be downright appalling, in business its use benefits the companies that use it. The potential for profit is huge, especially if astroturfing efforts can be used to train rivals of the company and bring them before commissions of inquiry, whether of a judicial or regulatory nature. It could even be said that astroturfing is simply part of the game in the corporate professional league. Political parties practice astroturfing, why not companies?

Also, almost all large companies donate to non-profit organizations, many of which have overtly aggressive agendas. In this case, astroturfing could be considered just an extension of this practice. The problem is that while astroturfing can help companies, it hurts the public's ability to understand complicated IT issues, shrouding them in a veil of mystery only a step away from the most imaginative conspiracy theories. Many people already do not trust the information technology sector, and soaking the news in disinformation, a completely unethical act, only deepens public suspicion. Digital technology encourages the dissemination of knowledge and know-how. Its ability to influence socio-economic structures also means that it gives power and a competitive advantage to those who design their applications over those who merely use them.

4.4. *Virtue ethics*

Ethics is a form of critical thinking about the social structures and traditions that shape the life of societies and aims to question the morality of the process of information dissemination and offer the possibility of making choices based on real information. Digital libraries belong to a new emerging digital culture. The existence of this informational plethora raises new questions regarding the production, collection, classification and dissemination of knowledge.

How can the integrity, validity and sustainability of these digital collections be guaranteed and, above all, is it ethical to disseminate information without regard to copyright and

proprietary data/information? Information technology is now ubiquitous in the lives of people around the globe. These technologies take many forms, such as personal computers, smart phones, the Internet, web and mobile applications, digital assistants, and cloud computing. In fact, the list is constantly growing and new forms of these technologies are working their way into every aspect of everyday life.

By letting the digital environment grow chaotic and unregulated, the level of cybersecurity has actually been reduced, resulting in a deterioration and pollution of our infosphere. This fact is the direct result of what was wanted - entertainment, cheaper goods, free news and juicy online gossip - and not the deeper understanding, dialogue or education that would have served much better and benefited the future. In the case of previous media for the dissemination of information (eg newspapers, physical media), there was a constant concern about maintaining standards, observing accuracy and the presence of the necessary informed public debate. Now we have the same problem with disinformation being practiced online. These types of digital, ethical issues represent a defining challenge of the 21st century and include violations of privacy, security and safety, property and intellectual property, trust, fundamental human rights, as well as the possibility of exploitation, discrimination, inequality, manipulation, propaganda, populism, racism, violence and hate speech. The lack of foresight of proactive ethics hinders decision-making as rapidly as the cybersphere develops, undermines real-time management practices and harms global digital innovation strategies. The near-instantaneous spread of digital information makes misinformation hard to track and nearly impossible to correct in real time, especially when trust is undermined.

4.5. *Pragmatic ethics*

How do we establish trust through credibility, transparency and accountability - and a high degree of patience, coordination and determination? Will this desired be achieved with the development of an ethical infosphere capable of saving the world and us from ourselves? Increasing attention is being paid to the impact of the fake news phenomenon on democracy and society in general. Researchers from many fields are trying to determine who is behind the fake news propaganda efforts, what are the effects and how to combat this phenomenon using technological means.

The studies conducted also analyze the ethical issues raised in the fight against fake news. Developing a scheme of a pragmatist media ethics, the tangled ethical complex of the problem is examined, which, like Ariadne's knot, can get us out of the fake news labyrinth. In addition, the pragmatist approach to fake news also allows us to highlight the discordant values and results at stake, in attempts to conceptualize and eradicate this new ethical challenge so present in social media.

Such an intuitive engagement with the phenomenon of fake news represents an essential first step in diagnosing ethical challenges and potential solutions. It can be assumed that the term "fake news" has a simple meaning or it can be interpreted as any term by analyzing the sum of the meanings of the words from which it is formed. This is because the term "news" means verifiable information in the public interest, and information that does not meet these standards does not deserve the label of news. In this sense, then, "fake

news" is an oxymoron that lends itself to undermining the credibility of information that does meet the threshold of verification and public interest-that is, real news.

To better understand cases involving manipulation in the sense of exploitative language and the conventions of news genres, one must treat these acts of fraud for what they are - a particular category of falsified information, cloaked in the cloak of disinformation, increasingly diverse and widespread, including in entertainment formats such as visual memes. One danger is that "fake news" is usually free - meaning that people who cannot afford to pay for quality journalism or who do not have access to independent public service media are particularly vulnerable both to disinformation as well as false information. The spread of disinformation and false information is largely possible through social media and social messaging, which raises the question of the need for and framework for regulation and self-regulation of companies providing these services. Due to their nature as intermediary platforms rather than content creators, these companies have so far been subject to only very loose regulation, except in the area of copyright.

However, in the context of increasing pressures on these information media, as well as the risks vis-à-vis free expression that over-regulation implies, important steps have been taken in the field of self-regulation. Development of journalistic strategies to combat disinformation they should, therefore, be undertaken in the conditions where the manipulation of information has been present in the life of society for millennia, while the evolution of journalistic professionalism represents a relatively recent phenomenon.

As journalism has evolved to fulfill a normative role in contemporary society, the media has largely managed to operate outside the universe of fabricated news and covert attacks, protecting and promoting journalism that aspires to high professional standards, that respects factual truth and source verification, verification methodologies, and public interest ethics.

Today, even considering the variety of types of "journalism", it is still possible to identify diversity narrative from real news that bears the distinct label of ethics in communication and attempts to be editorially independent of political and commercial interests. But before the evolution of such standards, there were few norms regarding the integrity of information in mass circulation. In this context, the time has come for the mass media to relate more closely to professional standards and ethics, to abandon the publication of unverified information and to distance itself from information that might interest only a certain category of public, but which is not in public interest. Therefore, the media must recall the time when all news outlets and journalists, regardless of their political orientations, avoided the spread of disinformation and false information.

One of the cybersecurity trends to consider is the constant need to see the ongoing evolution of relevant cybersecurity regulations. The dynamic and fast-moving nature of cybersecurity is becoming significant regulation that is far too slow to be considered a benefit and could restrict security by building a culture of compliance and a false sense of security against agile, motivated adversaries and intelligent. The ethical use of information technologies translates into the use in accordance with the intended purpose of the

technology, respecting the integrity and security of the system and is based on the implementation of general principles of good conduct such as responsibility, vigilance and respect for others in daily use of artificial intelligence.

The contextual nature of individual ethical use is also important to emphasize. Ethical judgment regarding certain habitual behaviors is greatly influenced by the "professional" or "private" context in which these behaviors take place. The perception of ethical use is much stricter in the professional context than in the general social context, where there is a certain elasticity or even laxity of the concept of ethical use. This is the case with illegal downloading which is considered morally wrong when done at work but acceptable in private life. In addition, we consider that the pragmatic view seems to be more representative, because, without denying the normative aspect of ethical use, users place a special emphasis on the practical consequences of acts that are expressed in the form of conduct adopted regarding the use of these tools. In conclusion, individual ethical use is not, as one might expect, a more or less rigorous application of moral prescriptions derived from ethical theories of philosophy or legal obligations. If we were to conclude about defining the ethical use of information technologies, it should take into account both user and organizational design, and also encompass the different dimensions of AI ethics. This would represent an intended use of the technology, respecting legal requirements, system integrity and security, which involves taking into account the interests of the parties involved and applying general principles of good conduct such as respect for others, responsibility in daily use of technology.

5. Regulation and liability of artificial intelligence

5.1. Further considerations on guilt and liability

With the development of AI, certain issues will arise, such as those of a legal, ethical and psychological nature. For a long time limited only to works of fiction, artificial intelligence is today developing exponentially and flooding all areas of socio-human life. Like any innovation, and even more so a revolutionary one, it also raises multiples and profound legal issues and require appropriate analysis and reflection. Both object and pretending to be a subject of law, speaking of the emergence of a "legal person of the third type", its impact calls for innovations on existing normativity and substantial, qualitative developments for the future, since law itself becomes an object of AI , witnessing the emergence of a "transjuridism".

The notion of fault and liability may struggle to find its place in this new environment, as an AI system can cause damage as a result of its autonomous actions driven by data and algorithms, without any fault in the traditional sense. In this regard, the issues of burden of proof, limited responsibility (liability) and defective product liability need to be re-examined to some extent. To avoid a liability gap, the most reasonable way forward in civil liability may be that limited liability (with reconsidered defenses and statutory exceptions) and fault-based liability should continue to coexist.

Are we heading towards the end of our civilization giving way to a new Middle Ages? At this moment I have no doubts that it is so. Because the end of this civilization will undoubtedly bring, after a period of medieval darkness, a new Renaissance. While her

salvation could resemble the resurrection of Lazarus, who will have lived for a while, after his resurrection, as a dead man among the living, with his body already disembodied by returning to the dust. The only thing that scares me, due to the smallness of my mind, is the speed with which degradation is sweeping us. Of course, we are a territory on the periphery of the great culture and civilization to which we belong, and decay is faster and more easily visible here.

However, during my adult life, extracurricular and school education, from the simplest level to the highest studies. suffered a drop in creepy quality. And starting from here, the competence and strength of the society registered a resounding collapse, I might say. Just 20 years ago, my students were competing for clear, logical, and organized notes taken while the teacher explained freely, without limiting or slowing down his presentation. About 10 years ago, students started asking to be dictated clearly, rarely and loudly, and even to be told when the dictation starts and ends, thus demarcating the minimum they "need" to learn from the rest of the explanations and ideas which "they don't need". This year, one student claimed he couldn't gather his ideas while using his concentration to write, an activity he's not very used to and which, of course, he doesn't "need" for anything. Just as no one needs to read the leaflet of a medicine they take or give to their child, because it is just a click away on the internet. And these are just random examples that cross my mind. You scare me because I liked it at school. And everything I am today is because of the school. For, even if the civilization will be reborn from the darkness in which it itself collapses with voluptuousness, it is woe and bitter for those who share in the collapse [27]. Can the law save us? We will try an answer.

5.2. The EU legal framework for artificial intelligence

The Regulation of the European Parliament and of the Council of 13 March 2024 establishing harmonized rules on artificial intelligence is the first binding regulation in the world adopted in this matter [28]. EU regulation adopts and promotes a "proactive" approach to the matter, recognizing the benefits of AI systems for citizens, businesses and the public interest, while also wanting to protect against security risks and the fundamental rights associated with them.

As pointed out in the related European Parliament debates, the regulation in question was intended to set the tone worldwide in terms of artificial intelligence development and governance, ensuring that this new technology, called to radically transform our societies thanks to the considerable advantages it can offer, to evolve and be used in compliance with the European values of democracy, fundamental rights and the rule of law.

According to the legislative act, an artificial intelligence system means "an automated system that is designed to operate at different levels of autonomy and that can, for explicit or implicit objectives, generate results such as predictions, recommendations or decisions that influence physical environments or virtual" (art. 3). Such a definition particularly encompasses systems that use symbolic or generative AI, machine learning, logic and knowledge, and even those that are not yet invented. Also, the same article specifies that the legal text applies to all natural or legal persons, public authorities, agencies or other

bodies that develop, put on the market, put into service, make available or use such systems in the EU market, for a fee or free of charge.

They are classified into four categories, namely those with unacceptable risk, high risk, limited risk and weak or minimal risk. Certain AI practices considered unacceptable are prohibited, in particular systems that allow: manipulating people through subliminal techniques acting on their unconscious, exploiting the vulnerabilities of specific groups, such as children or disabled people, remote biometric identification "in real time" in spaces accessible to the public, those for biometric identification using sensitive characteristics, such as gender, race, ethnic origin, citizenship status, religion, political orientation, those that allow determining the probability that a person will commit a crime or recidivism and based on profiling, location or past criminal behavior, leading emotions and uses in repressive services, border management, the workplace and educational institutions, the creation or development of facial recognition databases through the untargeted notification of facial images from the Internet or from video surveillance. Regarding high-risk AI systems - respectively those that present a high risk for health, security or the fundamental rights of natural persons, such as those used in biometric identification, access to education, workforce management, access to essential private services and to public services and benefits, law enforcement, justice and border control – stricter requirements are foreseen. They must be dealt with during development and before they are placed on the market in order to determine the measures that allow the generation and minimization of their risks.

In addition, a certain degree of transparency, traceability, accuracy, human control and cybersecurity is required, with the European Commission noting that "an artificial intelligence that we can trust should comply with all applicable rules, as well as a number of requirements such as:

- the specific evaluation lists that aim to contribute to the verification of the application of the key requirements;
- human involvement and oversight: AI systems should facilitate the existence of fair societies by supporting human involvement and respect for fundamental rights, without reducing, limiting or compromising human autonomy;
- robustness and safety: an AI we can trust requires algorithms to be safe, reliable and robust enough to deal with errors or inconsistencies throughout the AI systems lifecycle;
- privacy and data governance: citizens should have full control over their own data, which is not used for harmful or discriminatory purposes;
- transparency: traceability of AI systems should be ensured;
- diversity, non-discrimination and equity: AI systems should take into account the full range of human skills, competences and requirements and ensure accessibility;
- societal and environmental well-being: AI systems should be used to accelerate positive social change and foster sustainable development and environmental responsibility;

- accountability: mechanisms should be established to ensure accountability and responsibility for AI systems and their actions. Artificial intelligence must be developed exclusively in the interest of the common good, i.e. for the benefit of all mankind. Otherwise, it will become man's greatest enemy, bringing about his extinction."

Failure to comply with these rules is sanctioned by "fines ranging from 7.5 million euros or 1.5% of turnover to 35 million euros or 7% of worldwide turnover, depending on the offense and the size of the company". At the same time, a European office created within the European Commission will supervise the application of the respective legislative act. A relatively comprehensive AI legal framework has thus been established to ensure that artificial intelligence systems developed, designed, marketed and used in the European Union are human-centred, in such a way as to ensure a use of the technology safe and compliant with respect for fundamental rights.

In any case, the EU-European regulation is seen as a historic, pioneering legal regulation, which will play a role in the field and on the international scale, in the sense that it not only "created rules, but also exports them" especially by the exemplary character it induces, but also by the conditionalities it can impose. Integrated with the perspectives of international law, foreshadowed by the resolution of the UN General Assembly of March 21, 2024 and consolidated by the envisaged framework Convention of the Council of Europe, these regulations converge towards the crystallization of a "global right" of AI.

5.3. Towards a regulation of international law

The resolution of the UN General Assembly of March 21, 2024 regarding the promotion of safe, secure and reliable artificial intelligence systems for sustainable development creates the prerequisites for a global approach within the framework of UN multilateralism to the issue and paves the way for its international law regulation. Indeed, it extends the concerns and results already registered in the UN system, especially by the International Telecommunication Union, UNESCO and the Human Rights Committee, in the plan of the general policy of the world organization and amplifies the process of normative framing of the challenges of artificial intelligence.

The document adopted by consensus and having as its initiator the USA and 123 co-authors stands out and sets the tone in this regard, through the inclusive and constructive dialogue that characterized the approach for discussions, negotiations and future regulations in new sectors developed on this basis (such as peace and security international, responsible military use of AI autonomy). From a legal perspective, we are at the moment of expressing firm political intentions and initiating the defining milestones to be followed and reflected upon.

They circumscribe this perspective as true guidelines for reflection, regulation and action: the inclusion of AI as a component of efforts to promote the objectives of sustainable development 2030, the imperative respecting, protecting and promoting human rights in the use of new technologies, reducing the digital divide between states and within the same country, ensuring the same human rights in the Internet and offline.

Trying to predict future developments, one can consider, following the model offered by other world problems, the elaboration and adoption of a framework treaty in the field of AI, which will then be supplemented and developed equally in relation to the challenges of the stage and the demands, the particularities of the different fields of activity. The first benchmark would thus aim at advances in the levels of knowledge and technological applications of artificial intelligence, and the second, complementary and interdependent, would refer to horizontal diversity, by thematic excellence.

These expected normative-institutional developments continue with the adoption of a global pact on artificial intelligence and the creation of an international agency in the field according to the IAEA model. In the UN perception, the new chapter of public international law thus generated as the international law of artificial intelligence should be founded, as the UN Secretary-General stated at the November 2023 summit in Great Britain regarding related governance "on the Charter (of 1945) and the Universal Declaration of Human Rights (1948)" and to follow in the constitution and development of its normative substance the horizons presented in the resolution of the General Assembly of March 21, 2024. On such programmatic bases, to which other soft law instruments are added, we are witnessing the unfolding at the international level of an increasingly vigorous process of crystallization of AI regulation. In the same perspective of an interstate framework, with a global vocation, but as an initiative started from a regional context, the Council of Europe's Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law stands out. Considered as the first binding legal treaty in the field of AI, the document is also characterized by the fact that it is open to ratification by all the states of the world.

That is why this initiative belonging to a regional international organization, the Council of Europe, has the capacity to establish the general framework of the interstate regulation of the juridical-ethical regime of artificial intelligence. In addition, by virtue of its stated character as a framework convention the document is to be supplemented and developed by a series of sectoral regulations dealing with "specific issues related to the activities carried out within the life cycle of AI systems".

At the same time, its association with the AI Regulation of the European Union makes Europe "the world center of the legal regulation of artificial intelligence systems". The European Commission signed, on behalf of the EU, on 26.06.2024, in Brussels, the Framework Convention of the Council of Europe on artificial intelligence [29], which will certainly start an extensive process of change whose meaning we are trying to discern in the conclusive statements that will end our scientific research approach.

6. Instead of conclusions, about the need to understand the meaning of change

We look at the change and we don't understand it. Most of the time, as Toffler notes, we are dealing with dozens or even hundreds of currents of change in causal interactions, and not infrequently they gather in larger confluences, in tumultuous rivers. The speed of change, including social changes, also accelerated, which caused a compression of reaction times. Lacking the possibility of understanding the nature and essence of change, as well as adequate tools for knowledge and mastery of complexity, sometimes there is

also a fear of transformations or even resistance to them, which makes them more difficult and more expensive. The need for new on-board instruments is acutely felt. How it has often been said, not having these instruments in today's conditions is like trying to fly a jet plane with the on-board instruments of a classic plane. An excessive centralization of decisions is no longer possible when the reaction times have become so contradictory, and the elements involved so numerous" [30]. How to understand the essence, nature and directions of change?

This obviously also requires understanding the interdependencies, the connections and the complexity of the whole. We will not be able to understand the whole without knowing its component parts in depth, but neither will we be able to know its component parts without understanding the whole. These processes will probably involve a constant back and forth, from analysis to synthesis, from the particular to the general, from systems to subsystems and vice versa, from structures to values and concepts, from the anatomy of systems to their physiology, from parts to the whole and vice versa, as well as extensive dialogues between disciplines and numerous successive iterations. We are facing a revolutionary leap in knowledge processes.

The deepening of specialization, the "tunnel" vision of the specialist, who came to "know more and more things, about less and less" often erected impermeable walls between the different fields of knowledge. Focusing on increasingly narrow fields, in addition to the great obvious benefits it has brought to humanity, has also created numerous barriers in sensing connections, interdependencies and in understanding the whole. Paradoxically, but often with the progress of our specialized knowledge, our ignorance regarding the globality of the world increases. The rationalist, rectilinear, Cartesian thinking of the biunivocal cause-effect type links also led to the appearance of handicaps in the understanding of interdependencies and complexity. The existence of a series of interdependent causes and effects make the context constantly in motion. The equilibrium state of a system is also rather a particular case. The state of dynamic imbalance, in search of balance, is rather the state of affairs.

Sometimes it is enough to change the point from which we observe reality or the optics in order to notice new things, imperceptible before. The same observed fact or process will be noticed differently by a physicist, a jurist, an economist or a philosopher. For example, even man can be seen as a physical, biological or social being. He can be seen as homo faber or sapiens, as homo juridicus. But looking at him in each of these poses, we cannot perceive the unity of his being.

However, in reality, it does not exist and it only acts as a whole and in a specific social-economic context, which in turn is constantly changing. Without noticing the interdependencies and understanding the complexity, we will not be able to make the progress expected from scientific knowledge. We have paid and continue to pay a very high tribute to partial approaches, excessive simplifications. The solutions adopted in the case of sectoral approaches have often proven palliative, contradictory or even incompatible.

Understanding complexity requires the admission of paradoxes, the existence of the contradictory, the possibility of the existence of different paradigms. Changing some paradigms or axial principles can make us see realities with completely different eyes. In his epistemological research, the French sociologist Edgar Morin also advances the idea of the possibility of a new rationality that could revolutionize thinking [31]. Perhaps the most revolutionary change is precisely the modification of the thinking system, from the linear, Cartesian one - of the univocal cause-effect links - to the holistic one - of noticing the multiple and contradictory interdependencies - based on concepts of system, process, feed-back and on continuity-discontinuity, balance-imbalance, necessity and chance dichotomies.

In this new context, we will not be too surprised that apparently completely isolated facts are very closely related to each other. To understand what is happening around us, to understand the essence, nature and directions of change, we must try to coherently integrate and synthesize facts, events, realities and knowledge without any apparent connection between them. Especially since the new civilization is breaking into our midst. "This new civilization is so revolutionary that it defies all our previous assumptions. The old ways of thinking, the old formulas, dogmas and ideologies, no matter how beloved or useful they were in the past, no longer correspond to reality. The world that is rapidly emerging from the collision of new values and techniques, new geopolitical relations, new lifestyles and ways of communication, calls for ideas and analogies, completely new classifications. We cannot cram the embryonic world of tomorrow into the quiet spaces of yesterday. Even the conventional attitudes or states of mind are no longer appropriate" [30]. Currently we are witnessing the "great transition" from the industrial to the post-industrial civilization. We are still in the period of big questions where the answers can only be provisional and partial. This does not mean we stop looking for them. To not put them at all means to constrain the understanding" [30] as the author believes, to assert oneself without co-optation, exploitation, cheap resources and without the creation of an integrated world market.

And if I were to say, that after the end of corporate globalization that turned out to be a horror reset utopia, we are on the collision course with the fourth wave, of the civilization of the post-electronic society or cybercivilization, governed by cyberintelligence in the cyber age, I would say that we don't have to be afraid. And yet, there is an unknown: man himself, in his unpredictability. But he wants me to believe that if the current "war of the worlds" (Ukraine, Israel) after the bloody "cold war" does not reach a nuclear apocalyptic paroxysm, the fourth wave will mean the *modus ponens*, the second "rebirth" of humanity.

And if we add to all this the "sovereignist" trend, which recently appeared on the European political scene, which feeds the theme of patriotism, gaining momentum after three decades of the EU (1993-2023), prompts us to note the fact that love of country has never known such a popularity than before '89! Paradoxically, the term "sovereignist" does not even appear in the Romanian Explanatory Dictionary! The term "sovereign" instead reminds us of Article 1 of the Constitution: "Romania is a national state, sovereign and independent, unitary and indivisible." The notion of sovereignty is detailed in several branches of Law, from Constitutional Law to Administrative Law or European Law.

The theory is clear and logical. Sovereignty appears to us as a natural expression of goodness and equity. And yet, to some, the "sovereignist" option is presented rather as a fracture of elementary logic, stating that ignoring Article 148 denotes ignorance or populism. Moreover, for them there is also a covering motivation saying that the "sovereignist" rhetoric conveys the supremacy of the Constitution which it presents as being in opposition to the European Union. In the opinion of unionists, the speech of the sovereignists always revolves around the first article of the Constitution, ignoring precisely the part that deals with integration into the European Union: article 148 (2) "As a result of the accession, the provisions of the constitutive treaties of the European Union, as well as the other binding community regulations have priority over the contrary provisions of the internal laws, in compliance with the provisions of the act of accession."

There are arguments based on the text of the law, but the fact that Great Britain has left the damaged ship of the EU should not be overlooked. However, it is necessary, in my opinion, to look at law as a cultural phenomenon, revealing its interdependence with civilization and mentalities. Going in the depth of the subject, we will investigate the relationship between the legal phenomenon and the great trials of life, such as revenge, hatred or forgiveness. More or less abstract notions, such as happiness or absurdity, should be viewed through the legal filter, in order to reveal the answers provided by law to the great questions of existence revealed in the essential pages of legal literature, but also in classics of universal culture, such as Shakespeare, Dostoevsky or Kafka. At the same time, perspectives from the history of the state and Romanian law should not be missing. Last but not least, we will look to the future, towards a "technocratic" perspective, appreciating the impact of AI rather as a problem of general adaptation of human society and not so much a regulatory one whose response would be inadequate in itself, since reproaches the law for the inability to properly perceive the data of artificial intelligence, the low speed of reaction and the insufficiency of the judge's intervention in the resolution of related conflicts [32].

In another philosophical way, the protection against AI derivations offered by regulation "as long as what we mean by this notion and the measures taken in these areas are in no way up to the stakes" misses the point, it is a great illusion, being of a fiction [33]. Faced with an intellectual and creative turning point that affects our fundamental capabilities, the solution would be for the various professional bodies to mobilize to define what they are ready to yield and refuse to the digital industry, without which "we will find ourselves in a world in which we will be as strangers." [34].

In general, the field of artificial intelligence is a very promising one for any individual who wants to research socially relevant topics, as the impact of artificial intelligence in legal activity is increasingly visible. At the same time, we are discussing an area of research that is constantly changing, with spectacular and disruptive changes. Let's just remember the last few years. Probably, in 10 years, today's ideas will have to be substantially updated or will be contradicted by new discoveries or scientific leaps. New technologies and experiments reveal that soon the memory of every human brain will be able to be uploaded to the cloud and stored. Yes, all the data stored by the human brain will be able to be transferred before death to permanent storage media.

Today, more and more factories exist and are being built where products are printed and robots take care of almost the entire production process that requires physical labor. Weapons, bionic arms or organs, cars, robots and more can be 3D printed. There is much to say about what lies ahead. There are people who implant chips, in which they store personal information or about their various assets. Next we will outline the main ideas that could be considered for a large scientific research project in our homeland.

The first idea would be to not accept change just for the sake of newness, but only if it represents definite progress, because not everything that is new is automatic and good. Then, equally important is the need for antefactum regulation of the field of artificial intelligence. Taking into account the premise that the roller coaster of artificial intelligence is impossible to stop, with integrated efforts both public and private, a legal framework can be built to keep new IT technologies in a human-friendly womb. AI is the terrible child of postmodern society, which can and must be educated to serve the general long-term interests. In 2018, Elon Musk drew attention to the danger of the development of unsafe artificial intelligence, appreciating that it can become "an immortal dictator from which we will not be able to escape". The general interests of society presuppose the establishment of a set of rules to guarantee that AI is safe, useful to people and, at the same time, ethical (fair, non-discriminatory, moral, just). Among the scientists, highly skilled in field of AI, I will mention M. Tegmark, who makes the following pertinent recommendations: one strategy that will probably help us in all AI challenges is to act together to improve human society before AI takes off and we'd better modernize our laws before technology makes them obsolete, as well as agree on at least some basic ethical standards before having powerful machines learn those standards.

In a recent presentation in June 2024 [35], Ray Kurzweil, one of the world's leading futurologists and computer experts, maintained his 1999 prediction [36] that Artificial General Intelligence (AGI) would be reached in 2029, i.e. in 5 years. In essence, general AI could understand and learn any human task. In various robotic forms, they could do much better, faster, and cheaper everything humans currently do (and more), enabling total abundance. He announced at the time that many other experts already believe that that level is likely to be reached around 2035, even though, at the time of his original prediction, most believed that it was something that could only be reached around 2100. In other words, the other pundits in 1999 were dead wrong, moving forward 65 years in the meantime, and even so, Ray Kurzweil believed in June 2024 that he was likely to be right after all. "with everything" on the subject, that is, 2035 should also be pessimistic, the progress remaining to be made being achievable until 2029 [37].

He also mentioned in that presentation his way of estimating – he had basically assumed in 1999 that the annual rate of increase in computing power, versus cost, of previous decades would remain at least the same in the future. This meant that in 2029 calculations of 1 trillion bits per second should be reached at a very low cost, level of complexity and efficiency that general artificial intelligence would achieve. Currently, other recognized experts, such as Ben Goertzel, share his optimism [38], appreciating that we would be on the chart in this regard and that recent developments, such as ChatGPT, would confirm the relevance of his prediction.

In any case, that general artificial intelligence would be achieved in 2029 or in 2035 – would not fundamentally change the degree of success in analyzing and anticipating the future of the above prediction, nor the expected implications of the result itself. And regarding the implications of AGI, Ray Kurzweil effectively anticipates a kind of heaven on earth for humanity just after that point. From goods and services to discretion and ways to cover other needs/desires without having to work anymore - to the possibility of "freezing" age and even reversing it in step two [39]. That is, from robots that function as suppliers/providers of goods, services and emotions (produce food, walk the dog, offer friendship and even tenderness) – to youth without old age/immortality [40].

The current technological developments constitute, as a whole, a revolution, to the extent that they open completely new perspectives. They will have repercussions on the behavior of individuals, of public bodies, of the most diverse organizations and at the same time, they will have an increasingly strong impact on the security of societies and individuals. In other words, states and civil societies will develop through integration and even through submission to technological developments. They create opportunities in all areas of society and can be used to increase the efficiency and speed of processes. However, new technologies will create new challenges and new vulnerabilities. States will be threatened differently and will have to adapt to the new environment. New technologies will thus exert a direct and indirect influence on the challenges they will face the armed forces and implicitly on their evolution. They will replace the current expensive and complicated systems. The combination of emerging opportunities and the new vulnerabilities they will create anticipates the fact that current technological developments will influence relations between states in the field of security in a positive and a negative sense. The current discussion regarding the introduction of these new technologies focuses mainly on diametrically opposed aspects: on the one hand, the substantial savings possible in the long term and, on the other hand, the significant costs that could initially be a limiting factor, all the more so as it will be necessary to establish a new governance and control system that will bear additional costs.

On the other hand, the security aspects of this development are far too frequently absent from the debate. For example, what is in the machinery behind ChatGPT? This means that we are faced with a historical dilemma. First of all, we should understand the extraordinary processing capacity of natural language. There are extremely few cases where the AI does not correctly understand what it is about. And that should give us serious thought. Second, we will quickly see significant changes in the labor market. Until now, scenarios were made about what will happen when drivers are replaced by self-driving cars. Is such a thing possible? The answer is: "yes, but the world is not ready yet."

The impact of the introduction of this technology would be devastating as humans would collide in the most brutal way possible with technology. Imagine the emotion an accident caused by such a car would cause. You can bring statistical arguments, like those who say that "there are far fewer accidents involving self-driving cars", but this kind of argument will not hold. The inattentive man who discovers at the last moment that there is another man in front of his car, at least brakes, tries to avoid it, even if this can result in greater

damage. The car, if it has an error, runs over a man just as it would run over a log. It's just an aspect [41].

Scenarios have been made about how AI could replace basic jobs such as cleaning or preparing food in fast food restaurants. Is it possible? In the case of each it is debatable. In terms of cleanliness, not much progress has been made, despite quite a lot of effort, and in terms of jobs in restaurants or cafes, it is a major problem. Although you can robotize the entire flow, customers flee from areas where there is no human interaction. Including the preparation of food is an interaction with the person you can't see, but feel! So it's not really possible here either. But there are areas where the impact will be devastating. Areas from which you would expect the least, although from the very beginning there was the target. They are not entry-level jobs, but on the contrary, high-level jobs. The first victims will be the doctors in the field of medical imaging. I'm not an expert, but I think that even now the interpretations of imaging investigations given by AI algorithms will be better than those given by humans. Regardless of specialization or experience, humans will no longer be able to compete with AI in this field. Also, in terms of patient treatment management, AI will play an increasingly important role. Simply, based on the existing data in the patient file, the algorithms will accurately prescribe the prescription without any human intervention. Also, in the legal area. AI lawyers will really eat the bread of today's lawyers. Indeed, an AI lawyer will not be able to impress the judge, but who says there will be human judges? Quite quickly, the lower courts will switch to robotic judgment, and only the higher courts will have human judges. Probably, in a first phase the AI will help the human judges to process the documentation, but in a short time it will enter the front line!

But the biggest impact and, at the same time, the fastest, will be the one on the IT world. With today's technology, an AI algorithm can be taught extremely simply to program. In fact, this is already happening, but not with the impact I am talking about. "Systems that will write programs only based on specifications given in natural language will be a reality much faster than you think. Moreover, the roots of the phenomenon are already visible. We can say that we are lucky to live in an era of technology, where artificial intelligence intertwines with human reason, forming a duo destined to make our lives easier.

Today, people are surrounded by technology, giving rise to a synergy that was hard to imagine at the beginning of this millennium. Technology, which a few decades ago was only present in science-fiction films, today has reached everyone's reach, becoming an integral part of the everyday life of most people. Its emergence and rapid development led to the progress of society on multiple levels, but it also came with challenges and anxieties that began to sprout in our souls. As the process of technologization has expanded in countless directions, grabbing every bit of our lives, people have had to adapt to new trends and evolve with new technologies. We have reached the point where the Internet and smart devices have taken on the role of being our best friends and helping us to solve the problems we face in our daily life more easily.

We find digitization in everything that surrounds us, in all the fields and activities in which we take part. Thus, it was inevitable that the impact of new technologies would not spill

over into the judicial system, bringing with it a series of benefits and challenges that all participants in the justice act must face, including us, the lawyers. In what follows, I have proposed to initiate a journey in which the stations will be represented by the most important changes that reflect the impact of new technologies on the Romanian judicial system, analyzing at the same time how the legal profession must keep up with them [42]. Therefore, the importance and diversity of digital technologies places us in front of continuous questions: how to use the tools that the evolution of science and technology offers to humanity?

How to resolve the contradictions that appear every day in all areas of our lives, from politics to economy, from work to medicine, from education to social relations? Is the European citizen aware of the fact that the rights applicable in the "offline" environment must also be respected online? Does the European Union sufficiently protect individual rights online? How useful is a better information of the European citizen about his rights in the online environment? These are just a few questions whose answers we will analyze in the following by referring to the conclusions of a recent Eurobaroment survey on digital rights and principles [43].

A possible answer would consist in the fact that the virtual environment brings with it a series of challenges in terms of guaranteeing and protecting personality rights, challenges that are all the greater as the pace of technological progress, with which legislation must keep pace, is an extremely fast one alert "Personality rights are particularly vulnerable in the so-called digital age due to the use of new information technologies. Thus, the legislation must respond effectively to face the new challenges represented by the new methods by which personality rights are exposed to risk and violated. This fact led to the recognition of new forms of expression of these rights, including the right to self-informational determination [44]".

In this context, another natural question that arises is to what extent the individual is aware of the fact that he enjoys the protection of his rights including in the online environment and to what extent he is familiar with the tools that the legislation makes available to protect these rights. Although the legislation at the European level has seen significant improvements in the matter of protecting the rights of the individual, including in the online environment, given the complexity or the fast pace of development of the digital environment, it has become a real challenge for the legislation to keep up with all these pretense of order technological.

Vulnerabilities related to the protection of personality rights appear in a more obvious manner in the online environment, all the more so as the degree of information of the European citizen regarding the protection of his rights, including in the digital environment, is not in the highest parameters, varying according to by a series of factors such as age, education, socio-professional affiliation, financial resources, etc. Vulnerabilities are all the more obvious when those targeted are children or other people who need increased protection from the state.

From this point of view, it is extremely important that the legislative regulations in the matter follow the pace of development in the field of digital technologies. In addition, it is necessary to implement some policies to inform the citizens of the EU member states in the matter of protecting their rights to an equal extent in the "offline" and "online" environments. If we refer to the reality of our country, the need for citizens to be informed about the protection of rights in the digital environment is much more acute compared to other states, where the level of awareness in this regard is much higher [43].

As for me, I have lived under a communist regime for more than half of my life, and I can tell you that a society without objective legal reporting is absolutely awful. But a society based only on the letter of the law, without going a little further, fails by lacking the use for its own benefit of a much wider spectrum of human possibilities. The letter of the law is too cold and too formal to have a beneficial influence on society. When the whole life, as a whole, is interwoven with relationships in the spirit of the law, an atmosphere of spiritual mediocrity is released that paralyzes even the noblest impulses of man.

And it will be simply impossible to face the challenges of our threateningly armed century, only with the weapons of legalistic social structures. Today, Western society shows us that it reigns over an inequality between the freedom to do good and the freedom to do evil. A statesman who wants to do something effectively constructive for his country must act with a lot of precautions, even timidly (this is not the case in Romania today), we could say. From the very beginning, it collides head-on with thousands of hasty and irresponsible critics. It is constantly exposed to European Union directives and the press. They must justify their decisions step by step, how well they are founded and free from the slightest mistake. And an exceptional man, of great value, who has unusual and unexpected projects in mind, has no chance of establishing himself. From the beginning thousands of traps will be laid for him. The result is that mediocrity triumphs under the guise of democratic restrictions. It is easy to undermine administrative power anywhere, and in fact it has actually diminished considerably in all Western countries. The defense of individual rights has acquired such proportions that society as such is now completely defenseless against any initiative. In the West, it is time to defend not so much human rights, but rather its security.

In a world where legal systems interfere more and more, and legal experience is subject to constant evolutions, wanting to discover appropriate practice solutions that scientific research by bringing together the thoughts and creative energies of of the Romanian nation will generate them in a perpetual and necessary upgrading to respond to the purpose of our generation. We must be the generation of national and Christian revival, the generation of a healthy, strong and determined Romania.

The purpose of our generation is to scale towards the perfection of national ideals: unity in history and salvation in eternity. Our mission is to determine the rebirth of Romania: through reunification, regaining national dignity and a decent prosperity. Despite all obstacles and temptations, we are called to make history, not to be consumed by history. And Politics (political sciences), but also Law (legal sciences), together with related theories/constructs (Rights, Freedoms, Rules), have reached the stage where they have to

decide what they want to be: Science or Metaphysics (Philosophy) . The difference is that in Science the concepts evolve, and not necessarily towards something known in advance, while in Metaphysics (Philosophy) things are static, they cannot be proven to be falsifiable, they have a specific purpose.

Today we live in times when these Concepts are extremely static, infallible, beyond any possibility of combat (there are jurisprudential standards and that's all). We behaved like the drowning man clinging to the blade of grass, in the present case with these political-legal Concepts. The discussion should be about how we transform these concepts, from ideologies, into theories subject to falsifiability (subject to evolution), respectively how to accommodate the idea of evolution of these concepts with the lack of a specific purpose (I don't know if these Freedoms are for the good of man taken individually or for the good of the State, for example).

Science has as its objective benchmark nature, the surrounding world (Nature establishes the principle of falsifiability). Law and Politics have no objective benchmarks (on the contrary, they sufficiently generate their own benchmarks) and have remained at the stage of conventions. So does the State. If they remain at this stage of constructs superimposed on a certain spatio-temporal context, they will always be subject to opinion, and not to argument. I don't question these constructs (Freedoms, rights, etc.), but I think it's time to look for their objective benchmark, to help them evolve to move from the stage of ideology to the scientific stage. That's why I say it's time for questions rather than answers. It is not the rules, not the freedoms that are the problem, but the way we weigh and measure them. Each in his own way. This and because Politics and Law remained in the preparatory stage of the scientific paradigm, in the stage of ideology. Or maybe not everything has to become Science, and Man has to get used to the thought that ideology is also part of his life.

References

- [1] E. Albee, "Who's Afraid of Virginia Woolf?," 13 October 1962.
- [2] L. Papadima, Who is afraid of the computer?, Bucharest: Arthur Publishing House, 2013.
- [3] C. Vrabie, "The Promises of Artificial Intelligence to Public Administration and Smart Cities," pp. 9-46.
- [4] R. Coravu, "Technological Apocalypse," 2023. [Online]. Available: <https://anthropos.ro/robert-coravu-apocalipsa-tehnologica>.
- [5] G. Anders, "Cluj-Napoca," in *The obsolescence of man*, vol. I, Cluj-Napoca, Publisher Tact, 2013, pp. 289-292.
- [6] "Eternal Winter," [Online]. Available: <https://bit.ly/47kQm0p>.
- [7] W. J. Burns, "Transforming the CIA for an Age of Competition," [Online]. Available: <https://www.foreignaffairs.com/united-states/cia-spycraft-and-statecraft>.
- [8] G. Anders, Philosophical Transcripts, Cluj-Napoca: Tact Publishing House, 2013, p. 16.
- [9] V. Vinge, "Technological Singularity," January 2003. [Online]. Available: <http://cmm.cenart.gob.mx>.
- [10] C. Vrabie, AI - from idea to implementation, The winding path of Artificial Intelligence towards maturity, vol. 1, Bucharest: Pro Universitaria Publishing House, 2024, p. 15.
- [11] C. Vrabie , "The Promises of Artificial Intelligence to Public Administration and Smart Cities".

- [12] G. Tecuci, "Why artificial intelligence is not a threat to humanity, but a huge opportunity," 2023. [Online]. Available: <https://evidencedialogues.wordpress.com/>.
- [13] M. Tegmark, *Life 3.0. Man in the age of artificial intelligence*, Bucharest: Humanitas Publishing House, 2019.
- [14] R. Susskind, *Tomorrow's Lawyers: An Introduction to Your Future*, Oxford University Press, 2023.
- [15] L. M. Stanila, "Cyberspace and the territoriality of criminal law," *Premium Juridic Universe*, no. 7, 2021.
- [16] J. Kleijssen, "Cybercrime, Evidence and Territoriality," *Netherlands Yearbook of International Law*, 2016.
- [17] J. P. Barlow, "Cyberspace Declaration of Independence," 1996. [Online]. Available: <http://web.archive.org/web..>
- [18] W. Gibson, *Neuromantul*, Bucharest: Paladin Publishing House, 2017.
- [19] L. Lessig, *Code version 2.0.*, New York: Basic Books, 2006.
- [20] V. Stoica, "Are human rights universal?," *Old Dilemma*, no. 1034, 2024.
- [21] P. Nilay, "The CEO of Zoom wants AI clones in meetings," 3 June 2024. [Online]. Available: <https://www.theverge.com/2024/6/3/24168733/zoom-ceo-ai>.
- [22] D. Carmen, "Homo juridicus digitalis, the digital avatar for legal professionals," [Online]. Available: <https://www.juridice.ro/741>.
- [23] B. Barraud, *Humanisme et intelligence artificielle*, Paris: L'Harmattan Publishing House, 2022, p. 347.
- [24] European Parliament, "European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics," European Parliament, Brussels, 2017.
- [25] P. A. Michau, "Face à l'avènement de l'intelligence artificielle, nous manquons de philosophes," *Le Figaro*, 19 Janvier 2023.
- [26] Wikipedia, "Astroturfing," Wikipedia: The Free Encyclopedia, 2024. [Online]. Available: <https://en.wikipedia.org/wiki/Astroturfing>.
- [27] C. Popp, "The End Before the Beginning," *Anthropos. Philosophy magazine*, no. 12, 2023.
- [28] J. Sénéchal, "L'AI Act dans sa version finale – provisoire –, une hydre à trois têtes," *Dalloz- Actualité*, 11 March 2024.
- [29] European Commission, "Commission signed Council of Europe Convention on AI," Brussels, 2024.
- [30] A. Toffler, *The Third Wave*, Bucharest: Politica Publishing House, 1988.
- [31] E. Morin, *Lost Paradigm: Human Nature*, Bucharest: Romanian Educational Book Publishing House, 2022.
- [32] A. Grinbaum, "Régulation de l'IA: "La technologie va trop vite pour les lois"," *Le Point*, 5 March 2024.
- [33] E. Sadin, "Artificial intelligence: la grande illusion de la régulation," *Liberation*, 29 February 2024.
- [34] E. Sadin, "La vie spectrale: Penser l'ère du métavers et des IA génératives," 2023.
- [35] R. Kurzweil, "The Last 6 Decades of AI — and What Comes Next | TED," YouTube, 27 June 2024. [Online]. Available: <https://www.youtube.com/watch?v=uEzHu4NHrs>.
- [36] R. Kurzweil, *The Singularity is Near: When Humans Transcend Biology*, New York: Viking USA, 2005.
- [37] Stanford University - Human-Centered AI, "Artificial Intelligence Index Report," Stanford, 2024.
- [38] N. Lanese, "AI singularity may come in 2027 with artificial 'super intelligence' sooner than we think, says top scientist," 6 March 2024. [Online]. Available: <https://www.livescience.com/technology/artificial-intelligence/ai-agi-singularity-in-2027-artificial-super-intelligence-sooner-than-we-think-says-top-scientist>.
- [39] R. Kurzweil, "Ray Kurzweil on how AI will transform the physical world," *The Economist*, 17 June 2024.
- [40] L. Bondoc, "Coins-power, coins-vanity, coins-respect," 10 April 2024. [Online]. Available: <https://www.juridice.ro/essentials/8320>.

- [41] D. Diaconu, "Who will be the first victims of artificial intelligence?," 2023. [Online]. Available: <https://www.nationalisti.ro>.
- [42] T. Parolea-Moga, "Short considerations regarding the impact of digitization on the Romanian judicial system and the need to adapt the lawyer profession to new technologies," [Online]. Available: <https://www.unbr.ro/wp>.
- [43] R. Matefi, "Digital rights and their protection in the online environment, in the representation of EU citizens," *Revista Universul Juridic*, no. 5, pp. 52-55, May 2022.
- [44] I. Sarlet, "The Protection of Personality in the Digital Environment," in *Personality and Data Protection Rights on the Internet*, vol. 96, Cham, Springer, 2022.