Preface

Publication is a self-invasion of privacy

Marshall McLuhan (1911 – 1980)

Natural or man-made disasters are a good indicator for evaluating cybersecurity systems. These systems have been purchased or developed to operate efficiently 24/7 over many years. In both cases, whether purchased or developed, personnel training are necessary for their implementation, maintenance, and monitoring of proper functioning. These actions implicitly entail ongoing training of human capital, which can work autonomously or collaboratively, that is, receiving external support through outsourcing. Therefore, institutions of higher learning, such as universities, offer specialized curricula in the field of cybersecurity, ranging from continuing education courses and summer programs to engineering degrees, bachelor's degrees, master's degrees, doctorates, and postdoctoral programs. This is because modern societies practically cease to function without computer systems, telecommunications, electricity, and other infrastructure.

For this reason, societies invest the taxes collected from their citizens in specialized cybersecurity training, for example. Therefore, these teachers frequently attend international events to stay updated on the latest developments in the sector. However, this is not always the case, and it all depends on the geographical latitude and longitude from which these teachers and/or researchers originate. Many of them simply use these trips as free pleasure vacations, paid for by the citizens. Consequently, when natural disasters occur, such as intense rains that cause rivers to flood in cities, citizen alert mechanisms fail, even though the inter-university network contains hundreds of thousands of presentations related to civil protection in cases of natural disasters and the development of emergency models for such crises. When these systems fail, it means that corruption is deeply entrenched and perfectly camouflaged, not only in the political sphere but also in academia.

And it is precisely in the educational sphere where one of the constant sources of attacks within information networks is observed, attacks that have found in social media an ideal channel to promote discrediting not only of colleagues but also of the rest of the local, national, and international community. One way to detect this is through discourse analysis, as traditionally done in the studies of linguistics, semiotics, social communication, ethnography, etc., and which have been gaining so much momentum with natural language processing for the generation of virtual agents (e.g., Alexa, Google Assistant, Siri, among others) in communications since the end of the 20th century. In summary, those who theoretically dedicate themselves to resolving community crises in emergency situations with security systems have merely been out there presenting mirages and empty promises related to security.

The aggravating factor in this situation is not only financial, since these individuals travel at taxpayer expense, but also that, in the event of deaths resulting from shortcomings in public safety systems, no one from the academic sector is held accountable. One need only consult the databases of authors of papers presented at international events, where research supposedly focused on improving public safety has been conducted. Furthermore, it is important to remember that these academics are state employees whose privileges and salaries are guaranteed for life. Now, a rhetorical question arising from this distressing reality is: Why is no one holding these individuals accountable for security problems?

This is because these individuals constitute power structures that are above the highest authorities in the rest of the state. They not only remain in their positions for extended periods but also enjoy academic immunity and legal impunity. This latter situation is achieved through the exchange of favors between the academic sector and those holding degrees related to law enforcement. This is precisely where the other major Spanish dilemma lays, one that will be exacerbated by artificial intelligence and all its ramifications, such as the granting of technical academic qualifications in computer science to law graduates, for example. Many educators along the Mediterranean coast, at the end of the 20th century, pointed to this inclusion as the end of freedoms in interactive communication.

They had already detected a potential anomaly among computer science academics and students of new technologies (traditional computer science and all its specializations, ranging from artificial intelligence to quantum computing) who already hold law degrees. In other words, it represents the end of freedoms, not only for citizens' right to truthful and objective information, but also the rise of theocrats stemming from "narco-education", whose aim is to destroy the democratic system of communities, beginning with silencing journalists.

Besides, the connections between European and Latin American secular private, religious and public universities are striking, particularly their ability to promote and amplify corruption by exploiting opaque methods of international law to threaten citizens' security, such as silencing journalists who speak the truth. These are uncomfortable truths that expose deceitful, mocking, and dictatorial figures. In brief, mentally ill individuals who, by invoking terms like emotions, empathy, affectivity, and artificial intelligence, find amusement in misusing social media, since their destructive actions are supposedly invisible. Yet, it is they who carry out cyberattacks and constantly manipulate online information for their own gain. The aim of these schizophrenic and Machiavellian individuals is to distort new generations through fragmented knowledge, such as that disseminated through podcasting, to name just one example.

These are some of the conclusions reached when analyzing the intersection of elitist/private/religious education (these three terms are considered synonymous) from the developing world to the developed world, and vice versa. In other words, currently, there is no firewall that can eradicate this negative human and/or social factor that undermines network security and universal human rights, such as freedom of speech and access to truthful information. Therefore, many failures in security systems do not originate from external sources but rather from the people who comprise the human capital of companies, industries, businesses, municipalities, schools, universities, and so on, as can be observed in the studies conducted and the lessons learned over time, where the natural, formal, and empirical sciences converge. This is the main reason why many cyberattacks are orchestrated from within the educational sphere, because they know they can initially rely on legal loopholes for censorship until they are discovered and denounced, along with those who defend them. Consequently, the circle of corruption has extended into the legal realm, thanks to the promotion of narco-education between the developed and developing worlds, for example.

This link between narco-education and gardunians absolves the academic sector of its communicative responsibilities in the face of natural disasters such as tornadoes, droughts, floods, avalanches, pandemics, and so forth, where the dead are counted not just in the dozens but in the thousands or millions. In the case of natural phenomena, emergency telephone systems are not even activated in time to save human lives, since apparently no one wants to assume the responsibility of issuing the alert, for example. Vilely, even this basic social service is neglected by those who are attacking colleagues, journalists, democratic institutions, etc., every day from within the university.

One only needs to read and analyze the content they publish on social media, which ranges from an exaggerated narcissistic cult to the Machiavellian distortion of current social issues through the abusive use of photographs and videos. Many of these images allude to the free nature of their summer or winter vacations, presented as lectures, courses, seminars, and so forth, to name a few examples. In short, their communications on the surface web are banal, trivial, and self-referential, while they are blatantly attacking in the dark web. Now, we must add to this the legal corruption of some unscrupulous individuals who, in exchange not only for money but also for potential engineering degrees, master's degrees, doctorates, postdoctoral degrees, honorary doctorates, and so on, as an honorary reward for overseeing and protecting the illicit acts of their shady friends. There is still no hardware or security system that can detect and prevent these destructive phenomena.

The only way to expose them is through their abusive use of static and dynamic images, prepaid interviews, the role of lecturer, etc., the content of which circulates on the main social media applications. Cyber(il)legals engage in a myriad of illicit activities, such as censoring publications, deleting online content, protecting cybercriminals, promoting dubious online scams, obtaining academic qualifications without lifting a finger, and mocking their European colleagues (for example, when they have to pass exams to practice law in EU member states, while these individuals have other direct financial paths), and so forth. Their main strategy, which they periodically employ, consists of appropriating new terms in the IT sector and constantly presenting and promoting themselves as "expert" speakers or lecturers at seminars or other national events. These private or public contexts are governed by the religious institutions, and citizen participation is nonexistent. In synthesis, they must always be present on trendy topics ranging from artificial intelligence, quantum computing, and the metaverse to the afterlife (virtual or digital wills), and a very long etcetera.

This last point (the virtual will) is the only thing that connects them to that ecclesiastical context. These are corrupt contexts where they not only buy university degrees, thanks to the rampant underworld in their hometowns, but also have the help and ease of validating their qualifications in Spanish cities, without

needing to take additional exams. All of this is achieved thanks to religious connections in the vast, law-ridden territory that the equation interconnecting religion, law, new technologies, social media, and the Ibero-America dark web has become.

The danger of this equation lies not only in the creation of cyberterrorists within European borders, but also in the rewards that these individuals can receive from the corrupt environments of narco-education, such as the awarding of fake computer science degrees and transforming them into experts in the field, even if their technical knowledge is nonexistent. Here, too, there is no software or hardware capable of detecting and preventing the damage caused by these cybercriminals when they apply the laws to serve the dictatorial autocrats of the Omega generation. These are criminals driven by avarice and a thirst for destructive power. Readers interested in these profiles and their modus operandi over time can consult the following references [1-22]. Below is a resume of the chapters in the handbook:

With the title **"Scanning Ethical Barriers Influencing AI Robotics Security"** chosen by Aron Kumar, Oliver Janssens, Marc Dubois and Mohamed Alami, they aim to rigorously summarize and detail not only the origins of interaction from the beginnings of artificial intelligence and robotics, but also how robots with artificial intelligence are being incorporated into the daily lives of French and Belgians, whether at home, in the workplace, at school, or in recreational settings. The chapter begins with a technical examination of the main commercial robots in Europe used for domestic tasks, as well as humanoid robots manufactured and marketed in Asia that can replace human workers in bars (waiters) or receptionists (hotels, hospitals, tourism offices, trade fairs, etc.). It then presents the potential problems arising from robotic vulnerability to cyberattacks, for example. In this regard, the authors have conducted a comprehensive technical analysis, accompanied by graphs and tables, of the main weaknesses of the robot models they studied. This analysis allows them to quickly detect and prevent malfunctions in devices with artificial intelligence. Therefore, in this research work, the authors focus on the consequences of human-robot interaction, as well as the legal problems arising from damages caused by robot malfunctions. The examples presented have a dual nature, as they address both the cause (malfunctions intentionally caused by attackers in cyberspace) and the effect (damage to people, animals, property, services, and so on). These examples are accompanied by existing regulations in Belgian and French legislation. Furthermore, this research provides the reader with answers to several ethical questions, as well as a set of legal strategies for addressing potential harm to third parties when providing goods or services, whether inside or outside the home. Lastly, in their future research plans, the authors positively assess the growth of Human Resource Management (HRM), outlining new and original lines of inquiry for the short, medium, and long term.

"New AI Technologies and the Nondiscrimination Policy" this is a research work, authored by Jimmy Andeng, John Beale, Gillian Dempsey, Paul Maharg, and David Turton, a diverse group of professionals – computer scientists, educators, philosophers, psychologists, and lawyers– conducts an empirical and comparative study of the main associations, organizations, institutes, federations, and other entities dedicated to promoting the knowledge and use of new technologies based on artificial intelligence. The study takes as its starting point the non-discrimination policies these organizations publicly declare. It begins by analyzing the universal rights of individuals and the free access to digital information that has been implemented since the democratization of the internet, culminating in the rise of AI. The four main themes addressed are discrimination, hate, harassment, and marginalization. Subtopics include place of birth, skin color, age, race, religion, political affiliation, marital status, sex, and physical and/or intellectual disability. Each of these topics and subtopics has been analyzed from various social perspectives related to the authors' professions. In summary, the study reveals that discriminatory policies persist within the activities of groups (associations, organizations, institutes, federations, and so forth) whose ultimate goal is to promote new AI technologies among their national and/or international members. This data has been compiled in several lists and refers to courses, committees, events, publications, etc., primarily within the educational sphere.

"Learning Balance between Myrmecology, People and Algorithms" is the title chosen by its author: Junxia Ma. In her work, she identifies an initial convergence between ant colonies, ant colony optimization (ACO) algorithms, reinforcement learning, and human space allocation to improve traffic management in the Australian port of Perth, within the mining industry. The study begins with an analysis of stigmergy to evaluate the best alternatives for loading and unloading materials. This synergy of mathematical, computational, biological (entemology), and social (labor) knowledge aims to improve the port's maritime logistics, given its geographic location as Australia's main access route to the Indian Ocean. The author began her research with an empirical study of port activity. She then analyzed the existing port management software. Based on this data, the author and a team of collaborators developed a pilot system that simulates, in real time, the flow of ships entering and leaving the port. Although the system is in beta,

initial results indicate a positive benefit, with improvements ranging from 8% to 11% in the equation that considers variables such as reduced processing time, data reliability, and ease of use, among others listed in the chapter. The conclusions demonstrate how the author and her collaborators have sought, from the outset, to achieve a biological-technological balance to improve the management of natural and human resources. At first glance, the initial results obtained indicate success in their hypotheses and in the beta version of the simulator.

Andrea Chiaraluce and Albertas Gimbutas are the authors of the **"Human Surveillance Designed to Recollect Teachers Confidential Information: Annihilating the Right to Human Dignity."** This study present a novel perspective in which contracted CS (computer science) professors are controlled by students to secure their positions, making the rights to human dignity, privacy, and confidentiality a mere utopia in our time. The study begins with a detailed description of existing commercial and open-source software applications used to monitor user activity when interacting with computers connected to the educational or work network. Through this study, they reach their first conclusion: user privacy on networked computers no longer exist. The report highlights the importance of implementing and updating regulations to protect citizens, not only against the latest generation of spyware and surveillance applications, but also by simultaneously drawing on reports published by the OHCHR (Office of the High Commissioner for Human Rights). This latter approach is used to investigate the new challenges faced by teachers who, in their work environments, perform pedagogical tasks that inherently involve the right to information in the digital age. The study includes fifty European case studies analyzed within the academic sector, primarily concerning teachers specializing in new technologies (computer science, artificial intelligence, robotics, telecommunications, etc.) who are hired on a temporary basis. The study concludes that many of these institutions use students as veritable spies to obtain personal/confidential information from their teachers and/or tutors. The aim is to denigrate the work of teachers, thereby securing not only the jobs of their former teachers/tutors, but also the opportunity to obtain from their employers (who reduce hourly labor costs by employing a trainee teacher) a series of personal and/or financial benefits. These benefits range from the allocation of research projects, funded stays abroad, and academic degrees from prestigious institutions, to subsidies for starting private businesses or holding political office. The data and information obtained have been masterfully presented in a collection of infographics that accompany the text.

"Nerds in Knurdland." The authors of the chapter –José Correa, Felipe Ruíz, Manuela Hidalgo and David Miller– analyze the psychological profile of those who not only threaten cybersecurity but also harm people in their family, work, and educational environments, presenting themselves socially as nerds. This latter trait is the first symptom detected by the authors when speaking to a real (physical) or virtual (social media) audience. The study reveals how these self-proclaimed nerds exhibit physical and psychological characteristics, when communicating technical data, digital humanism trends, etc., typical of an intoxicated person. Therefore, the authors point out that these individuals have a need to gradually create a scenario or space for their actions, starting in the family environment and extending to the educational and/or work setting. In the chapter, José Correa, Felipe Ruíz, Manuela Hidalgo and David Miller details how, in this territory called "Knurdland" (a term derived from the inversion of the word "drunk," combined with the suffix "land"), nerds transform themselves, adopting behavioral techniques that seriously affect their temperament, character, and mental health (both their own and that of the environment they influence). In another extensive section, the authors explain how, in this space, the behavior of these nerds is reprehensible from both an educational (virtual community) and operational (social media platforms) perspective. They also describe the deception they frequently employ to transcend the boundaries of Knurdland, relying on legal stratagems such as "victimizing the perpetrator," for example, presenting themselves on social media as tormented by anonymous attacks. The main theoretical aspects addressed in this research can be summarized as follows: Psychopathology of affect, psychopathology of language, study and application of the DSM-5-TR (Diagnostic and Statistical Manual of Mental Disorders –Revised Edition), gender dysphoria (sex-related health and disorders), and schizophrenia (delusional beliefs and confused thinking). An extensive appendix with examples from social media and bibliographic references completes this research.

The authors of this research: **"Voice Biometrics Techniques: Dilemmas in the Age of Artificial Intelligence"** are Kristin Persson, Hao Tan, Eric Wallin, Richard Olsen, Lars Gustafsson, Anne Saum, and Peter Berg. They highlight the main problems with the right to privacy arising from biometric techniques in the context of citizen cybersecurity in so-called smart cities. The research begins by statistically describing

the rates of criminal acts of voice spoofing in the following European countries: Poland, Romania, and Slovenia, when voice parameters are altered. It demonstrates the need to increase citizen security across the European continent. In their work, the authors focus on the biological and legal aspects, employing various artificial intelligence tools, such as Deep Neural Network (DNN) techniques, including CNNs, MLPs, RNNs, and Transformers. They analyze diverse Soft Computing strategies to tolerate imprecision and uncertainty in order to solve highly complex problems, such as identity theft through the human voice. In this sense, they broaden the study to include the characteristics of human beings when interacting with others through oral communication. That is, pronunciation, tone, volume, and modulation of words, basically. The vocal factor, combined with certain biological aspects that cannot be altered, such as facial features, iris patterns, fingerprints, voice tones, and body language, among others, can generate a unique pattern, as is the case with fingerprints, and reduce spoofing. In the end, the authors examine the current legislation in these countries regarding the right to privacy and the use of artificial intelligence in capturing conversations in public spaces (streets, parks, theaters, cinemas, airports, educational centers, etc.) and private spaces (homes, workplaces, and so on).

The chapter **"The Generative Artificial Intelligence: Inspecting Inter-generational Relationships"** has been developed in a didactic and easily understandable manner in each of its sections. The authors –Chang Lim, Tao Bao, and Rui Yang– of this work reflect on the psychological barriers faced by different generations in the everyday use of GAI or GenAI (Generative Artificial Intelligence). This study is based on considering users who work individually or autonomously to resolve problems related to computer data protection (firewall configuration, server installation, configuration and maintenance, security password assignment, remote monitoring and troubleshooting, etc.) in their work environments, as well as those who work in teams and require constant communication among team members to perform daily tasks in the context of cybersecurity. The chapter describes, with interesting examples, the positive aspects and new challenges for professionals in the field of cybersecurity. Simultaneously, and with regard to GAI use, it emphasizes the creation of a new digital divide between different generations of users. To delve deeper into these psychological barriers, a study population was established based on small companies (fewer than 49 employees) that provide outsourcing services in the field of cybersecurity. In their initial findings, the authors highlight the urgent need to implement AI literacy courses for individuals working in groups. Many of these workers lack a fundamental understanding of AI, distrust decisions made using AI, and are uncertain about the effectiveness of those decisions. This research includes numerous questionnaires that can serve as models. The responses to these questionnaires have been quantified in tables presented at the end of the study as appendices. The extensive bibliography accompanying the research work is also noteworthy.

The researchers –Yuan Li and Lei Yan– began their research work **"Applications of Cryptology: An Efficient Quantum Study"** by focusing on the increasing number of quantum computer installations and the new security challenges arising from the cryptography of public access keys. They then investigated the main advantages and disadvantages of the three primary quantum computer models: Fault Tolerant, NISQ (Noisy Intermediate-Scale Quantum), and Analog, excluding other models being developed in university laboratories and/or multinational IT companies. Their initial findings highlight the advantages of doubling the length of public keys, after considering the Grover and Shor algorithms. Through a historical analysis of the rapid evolution of quantum computers, they demonstrated an increased risk associated with traditional encryption methods such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic-Curve Cryptography). These are some of the motivations behind a novel QKD (Quantum Key Distribution) methodology for quantum key distribution to strengthen communication channels. They also consider it beneficial to direct future research toward the implications of new cyberattacks and post-quantum security. A comprehensive set of references accompanies this chapter, which can guide future algorithm developments in the context of quantum computing.

"Mapping the Impact of AI Endogamies on Supercomputing, Bioethics and Cyber Society: A Systematic Review and Meta-Analysis in Mare Nostrum." The authors of the extensive research are and Joaquín Medina, Marcos Aguilar-Cabrera, Carolina Ramírez-García, Rosa Castañeda-López, María Chávez, Antonia Herrera-Ibarra, Ramona Valdez, Ángela Rojas, Enrique Soto, and Pedro Ledesma. Based on a novel methodology, they have carried out a systematic and updated review of the Thurstone and Likert scales. They then reviewed the structure of scientific citation indexes and, finally, geographically located centers that distort the information provided, using online artificial intelligence. The ultimate goal was broad and multifaceted from the outset. First, to gather the opinions of science students in the European Mediterranean region regarding the intergenerational impact between parents and children within

the dynamic context of a digital society focused on bioethics and supercomputing, with the unique characteristic that parents and children share the same educational and professional spaces. In this sense, the research begins with a comprehensive review of the state of the art in supercomputing and bioethics research. Subsequently, they have added other components that were present in reality but function as illusions of that reality. Some of these components include: machine learning, autonomous intelligent agents, STEM, gender equality, assistive medical technology, assistive vehicles for the elderly and/or disabled, IoT, among others stemming primarily from CSE –Computer Science and Engineering, ICTs and AI. They then measured the scope or coverage of these areas of study. They observed that this broad scope is negatively impacting professional ethics, as there is a disproportionate increase in the indices measuring scientific citations between parents and children in short periods, compared to other colleagues. They argue that this is the origin of the social marginalization of scientists, particularly in R&D –Research and Development, fields. They also measured transparency regarding achievements attained through personal merit, rather than through family connections, in contrast to AI inbreeding. This refers to information published on freely accessible digital platforms such as Wikipedia and similar encyclopedias. The examples are accompanied by numerous graphs. These studies already highlight the gap and high degree of disparity existing between intergenerational relationships between parents and children, compared to the meritocracy of students, teachers, researchers, etc., in obtaining scholarships, research grants, funding for professional development courses, and so on. The conclusions show how the authors argue that these social biases are being incorporated into autonomous intelligent agents when they collect data online, and they have established some geographical points in this regard. Therefore, AI endogamy facilitates the dissemination of false data and information to end users. This work concludes with a comprehensive set of research directions and bibliographic references.

"AI Carnival of Doctoris Philosophiae Honoris Causa: Addressing a New Toxic Pollution in Iberian Environments" is a long and original title given by the authors: Carolina Ramírez-García, Patricia Wilson, Melisa López, Alejandro Contreras, Ramona Valdez-Bautista, Marcos Aguilar-Cabrera, Fernanda Durán, José Iglesias, and Alberto Espinosa. This extensive research work begin with a psychological, sociological, literary, and statistical study to analyze the career paths of computer science professors and researchers at public universities. The study period encompasses the beginning of their careers and work experiences, drawing on literature and psychology. The initial starting point was the compilation and selection of famous quotes from the literary thought of Latin American authors, combined with the evolutionary chronology of these professionals within the Latin-American computer science sector. This point is linked to the type of contracts they held as professors and researchers. Furthermore, they investigate the human makeup of early computer science disciplines and their interrelationships with other technical and/or theoretical areas, such as physics, mathematics, artificial intelligence, industrial engineering, telecommunications, systems engineering, software engineering, usability, automation, robotics, quantum mechanics, and so on. Using statistics and historical data, the authors identified abnormal or aggressive behaviors aimed at career advancement. The average age of these individuals ranged from 24 to 46 years. The main abnormalities detected, listed chronologically, are: the ease with which secondary topics in teaching and/or research are shifted in scientific publications; self-promotion in social media; the accumulation of awards; roles in various associations, foundations, etc.; and a lack of collaborative continuity with the working groups through which they have accessed national and international funding. In short, they exhibit disproportionate growth over time compared to their colleagues, examining the initial periods of their educational careers. These and other abnormal variables of human behavior converge in a novel evaluative matrix, which its authors call "*AI Carnival*." Another aspect of this study has been the literary corpus. The authors have chosen the literary phrase *"the perfect dictatorship*," referring to their Mexican and Chilean compatriots residing in Spain. The initial results have shown that over 78% of those receiving these academic degrees (among other significant awards) indirectly engage in the marginalization of other colleagues to hinder their growth and/or competitiveness. This phenomenon has been observed in departments where they began their teaching and/or research work, related to the "AI Carnival." The authors have compiled all the results into a database using SQL –Structured Query Language. This data indicates the existence of toxic work environments in the field of computer science and/or ICTs, dating back to the last century. Today, this toxicity remains hidden beneath a variety of guises within the Spanish educational carnival. The corpus examined comes from social media, specifically from the awarding of the title of "Doctoris Philosophiae Honoris Causa," which in this study relates to artificial intelligence and all its ramifications. The candidates are from Mexico and Chile. In the lessons learned section, they demonstrate and quantify how these professionals have exponentially expanded their influence toward what could now be erroneously termed "humanistic engineering." This involves adding artificial intelligence to every social aspect related to human beings and their context (environment, natural

resources, health, sports, ethics, legality, feminism, disabilities, and so forth) without a minimum of theoretical knowledge of each of the disciplines that comprise the formal, natural, and empirical sciences. As a final point, the authors argue that "AI Carnaval" is a Latin American trend designed to distract attention from other issues related to the quality of public services (health, education, citizen security, etc.). Furthermore, this trend currently serves to reinforce "a toxic academic structure."

"The Paradigm of Complexity: A Valid Instrument for Promoting STEAM Globalization and Racial Bias" presents a philosophical and sociological investigation based on the notions of Edgar Morin's complexity theory. The research begins by responding to a critique of the phenomenon of globalization, whose origin lies in the use of new technologies and the new paradigms presented by Morin. The authors – Laura Ricci, Veronica Grosso and Anne Boyer– demonstrate how these new paradigms of complex social interrelations have exacerbated racial discrimination among adolescents, led to a decline in local STEAM (Science, Technology, Engineering, Arts, and Math) fields, and resulted in the emigration of new professionals in the exact and formal sciences. Their study focuses primarily on the complexity of selecting university studies in the sciences (mainly computer science, physics, chemistry, and mathematics) among young French people upon completing their secondary education. In it, the authors present the complex reality of the data and information that prospective university students must manage. The study establishes psychological analysis mechanisms (primarily questionnaires and surveys) to address the disorientation, confusion, uncertainty, disorder, and ambiguity of concepts found on vocational guidance websites, both those belonging to secondary schools and universities. They also demonstrate how virtual agents, artificial intelligence applications, university portals, etc., fail to fully address students' doubts or questions. As a concluding remark, there is a wide range of graphs showing how the tenets of complexity theory have contributed to the decline in academic performance, professional development, and the inclusion of civic values, tolerance among human beings, and the acceptance of ChatGPT, Gemini, DeepL, Matomo, Zapier, and other instruments/applications of the artificial intelligence as an assistance tool in daily activities.

"The New Educational Dictators under the Banner of Tech Apolitical Progressivism." This is an extensive theoretical and historical chapter that analyzes the endogenous and exogenous factors of various educational models in the Latin American region. It brings together the history of social and student movements, beginning in the 1970s, through the inclusion of the burgeoning sectors of the so-called "upper-middle class," for the advancement of science, society and technology. The authors –Salvador Soto, Lucía Vargas, Ana Ferreira, Luis Ferreira, Ernestina Lara, and Susana Torres– have stratified society into four main zones: "lunatic", upper, middle, and lower. The lunatic zone is described as authoritarian and repressive. It is within this zone that they locate the educational dictators of a supposed progressivism based on the use of computers and/or intelligent agents. These profiles, as well as their functions, are very well summarized by the authors. Furthermore, they detail the main characteristic of that lunatic class that authoritatively operates above all the norms that regulate society and how they have become radicalized in the present day through social movements, alienated from the neutrality that an educational ecosystem should be. Simultaneously, they take stock of the educational setbacks resulting from the hypothetical progress that the inclusion of new technologies should bring as a democratizing element in major urban areas. The study continues with current educational models, which hypothetically seek to address the imbalances arising from power as a tool for service and not for privilege. These imbalances are analyzed primarily in relation to the free communication of social networks. The state-of-the-art section of this work includes a comprehensive, schematic historical overview, from the introduction of the first computers in primary, secondary, and university classrooms, following UNESCO guidelines in that geographic region. Consequently, the failure to integrate educational models from North America and Europe into the Latin American context is analyzed. The authors conclude the work with a set of hypotheses about the damage that this lunatic elite is causing and will cause, through artificial intelligence, within Latin American educational ecosystems.

"The Leaning Tower of Pisa and Its New Deviation in the Art of AI Education: Transforming Human-technological Machiavellianism into a Positive Value." Loredana Chieti, Antônio do Prado, Felipe Coutinho, Leonardo Rocha, and André Gonçalves are the author of this chapter. It begins with a summary of the deviations observed in pedagogical models, lines of research, the formation of working groups, the organization of conferences, and the development of prototypes related to the engineering of new information and communication technologies, all centered in the Tuscan region, specifically in the city of Pisa. Since 2017, they have been refining a novel framework for the interrelationships of educational and scientific activities, one that transcends the boundaries of Tuscany and extends to the four corners of the globe. These activities, within the realm of new information technologies, allow for the development of

proposals for new pedagogical models or technological prototypes, for instance, which originate in art and move toward cutting-edge technological fields. Through concepts derived from psychoanalysis, she demonstrates the presence of Freudo-Marxism. Furthermore, the research argues that the art of education is not only governed by deception and manipulation, but is also promoting a negative value through artificial intelligence, presenting it as a resource for creativity and originality. It includes extensive references to psychological studies related to psychoanalysis and its applications in the new millennium, as well as a comprehensive list of unfinished and/or non-widely applied R&D projects, based on the premises outlined in those studies.

"Narcotizing Machine Learning and Autonomous Intelligent Agents." This research introduces a critique of European reason in the face of the pre-Columbian-Mexican narcotization of artificial intelligence. The research work begins with an examination of curricula and human capital in artificial intelligence –related fields of study, in Catalonia during the 1990s, in both public and private schools and universities. Subsequently, the study analyzes the career shifts of these overseas professionals towards sectors such as audiovisual media, computer science and engineering, usability, user experience, human-computer interaction, IDC (Interaction Design and Children), UCD (User Centered Design), ICTs, AI, VR, AR, and so on, culminating in their current work in bioethics, law, feminism, and many other fields. Simultaneously, it explores how this broad divergence poses serious risks to the future of science, especially when professional inbreeding is present within the same centers of study, research, technology transfer, and so forth. Emphasis is placed on the phenomenon of generational inbreeding (parents and/or children), which opens up an infinite range of topics of interest among members of the same family and acts as an epistemologically destructive factor not only for new scientific frontiers but also for their traditional and precise spaces defined by domains, fields, and specializations. The various Catalan/Spanish schemes used to justify these anomalies are also examined. These range from obtaining European funding, signing collaboration agreements with universities, and producing collective scientific output to receiving rigged awards, including honorary doctorates, both within and outside the same autonomous region, all aimed at creating structures and ecosystems that remain unchanged over time. As a concluding remark, the author –Francisco V. C. Ficarra– predictions are made about the loss of local competitiveness in the international context of artificial intelligence due to the inbreeding of the Omega generation, Gardunia factor and education narcotized.

Finally, a selection of these chapters have been presented orally or virtually at the following international conferences, workshops and symposiums (Belmapan, Belize –Central America, December 2024). Besides, these contributions have been expanded from their long or short papers, posters, demos, and so on: ADNTIIC (13th International Conference on Advances in New Technologies, Interactive Interfaces and Communicability), CCGIDIS (13th International Symposium on Communicability, Computer Graphics and Innovative Design For Interactive Systems), ESIHISE (7th International Conference on Evolution of the Sciences, Informatics, Human Integration and Scientific Education), HCIHEART (7th International Conference on Human-Computer Interaction, High Education, Augmented Reality and Technologies), HCITISI (11th Argentine Conference on Human-Computer Interaction, Telecommunications, Informatics and Scientific Information), HCITOCH (13th International Workshop on Human-Computer Interaction, Tourism and Cultural Heritage), HIASCIT (9th International Conference on Horizons for Information Architecture, Security and Cloud Intelligent Technology), ITSIGUI (4th International Conference on Innovation in Tourism Systems, Intelligent Gamification and User Interaction), MSIVISM (10th International Conference on Multimedia, Scientific Information and Visualization for Information Systems and Metrics), QUITANS (6th International Conference on Quantum Information Technologies Applied to Nature and Society), RDINIDR (International Conference on Research and Development in Imaging, Nanotechnology, Industrial Design and Robotics), and SETECEC (12th International Conference on Software and Emerging Technologies for Education, Culture, Entertainment, and Commerce).

Francisco V. C. Ficarra
(main editor and compiler)

Riomaggiore, Italy (December, 2024)

Acknowledgment

Maria Ficarra, Mary, Amélie, Luisa, Carlos, Anna, Giulia, Sara, Donald, Jim, Miguel, Giselda, Riccardo, and Roberta, I would like to take a moment to express my sincere gratitude for all that you've done for this handbook. Your help and encouragement have been invaluable.