SCULPTING THE LEGAL LANDSCAPE: EXPLORING THE COMPLEX INTERPLAY OF ARTIFICIAL INTELLIGENCE, HARDWARE, SOFTWARE, AND ROBOTICS

Massimo Farina[1]

Abstract
This paper provides a brief exploration into the undercurrents impacting the Fourth Industrial Revolution, which represents a significant convergence of four main technological components – hardware, software, artificial intelligence, and robotics. It dissects the unique characteristics and functionalities of each, showcasing their crucial, yet distinct roles, and underlines the synergies that result from their combined application. A significant part of the paper explores the evolving human-machine relationship, highlighting the increasing trust in intelligent robots and its implications for our technological future. The article further navigates the complex legal landscape at the nexus of these technologies, addressing the challenges and proposing potential avenues for effective solutions. This research attempts to add a comprehensive understanding of the dynamics of the Fourth Industrial Revolution and its implications on the legal space.

Keywords
Artificial Intelligence, Robotics, Hardware, Software, Privacy, Copyright, Liability, Trust.

Summary
1. The fourth industrial revolution: unprecedented technological acceleration and the synergy of hardware, software, artificial intelligence, and robotics. - 2. Defining the distinctions: hardware, robotics, software, and artificial intelligence. - 3. Hardware *vs.* robotics and software *vs.* artificial intelligence: their crucial yet separate roles. - 4. Trusting the technology: the evolving relationship between humans and intelligent robots. - 5. Navigating the legal challenges at the nexus of hardware, software, artificial intelligence, and robotics.

---

[1] Researcher in Legal Computer Science and Philosophy of Law, DIEE, University of Cagliari – Italy.

1. THE FOURTH INDUSTRIAL REVOLUTION: UNPRECEDENTED TECHNOLOGICAL ACCELERATION AND THE SYNERGY OF HARDWARE, SOFTWARE, ARTIFICIAL INTELLIGENCE, AND ROBOTICS

The Fourth Industrial Revolution[2] serves as a substantial upheaval, akin to a seismic wave that is sweeping across the global landscape. It isn't simply a mere extension or evolution of existing technological paradigms but fundamentally alters the very essence and fabric of how digital technologies become enmeshed in human life. This tidal wave of change is realizing the previously unimaginable vision – a thoroughly digitized world where technology is not merely an external tool but is increasingly a part of our own identity, impacting our interaction with the self, others, and the world at large[3].

Historically, the First Industrial Revolution was marked by the mechanized production enabled by water and steam power which fundamentally restructured manual labor. Following that, a subsequent era (the Second Industrial Revolution) featured the emergence of assembly lines and the harnessing of electricity as a viable power source, leading to the dawn of mass production. Later, another pivotal period (The Third Industrial Revolution) saw the introduction of automation, powered by electronics and information technology, accompanied by a transition from analog to digital systems. These events dramatically transformed the socio-economic-political landscapes of their respective eras. Following in this lineage but with an impactful differential, the Fourth Industrial Revolution, stands as a radical shift in human engagement with technology, provoking a genesis of monumental proportion in our socio-cultural, economic, and political structures.

---

[2] LEE 2018.
[3] SCHWAB 2016; FLORIDI 2014.

The current age is marked by an unprecedented acceleration in technology, with the velocity and the trajectory of change reshaping societies, economies, and individuals. The pivot of this radical evolution is the synergistic integration of hardware, software, Artificial Intelligence (in short AI), and robotics, forming an amalgam that magnifies their individual impacts into a transformative force[4].

Hardware and software[5] are not just components but the foundational pillars of the current digital era. The physical components that we visually identify with technology such as computer systems, servers, routers, and networks are the 'hardware'. These devices enable efficient data processing and communication, forming a complex physical network that spans the globe. In contrast, software forms the invisible, 'virtual' element of this network. It encapsulates the programs, operating systems, and protocols that guide the functionality of the hardware. Without the software, the hardware stands as stationary, lifeless machinery. The software breathes life into the hardware, transforming it from a static tool into a dynamic instrument capable of an array of functions – from simple data entry to complex computational tasks[6].

AI is the game-changer that infuses this world of hardware and software with 'intent'. It consists of the algorithms[7] and the capacity to learn in a machine-like manner – processing vast amounts of data, recognizing patterns, predicting outcomes, and making decisions based on those predictions. AI, in essence, gives technology its 'brain', empowering it to be not merely a functional instrument but an evolving, reacting, and learning

[4] AMATO MANGIAMELI 2020; AMATO MANGIAMELI, SARACENI 2023; BRYNJOLFSSON, MCAFEE 2016.

[5] FARINA 2023, 248-252; BORRUSO 1999; RISTUCCIA, ZENO-ZENCOVICH 1993; CURTIN, FOLEY *et al.* 2005.

[6] TANENBAUM, WOODHULL 1997.

[7] AMATO MANGIAMELI, 2019, 107-124; 2022, 93-101.

entity – a seemingly living entity capable of learning from its past, understanding its present and predicting its future[8].

Meanwhile, robotics serves as the bridge that connects the intangible digital world with the tangible physical world. Robotics technologies range from manufacturing robots that assemble cars in our factories, to autonomous vehicles[9] that may someday become our main mode of transportation. In doing so, robotics allows our digital tools to leave the confines of the circuitry and wiring, becoming actors in our physical reality. This enables the hardware-software-AI trinity to escape the cold abyss of binary codes, to engage in real-life, open-ended, unstructured, and dynamic scenarios[10].

The coalescence of these four entities – hardware, software, AI, and robotics – brings forth a renewed and reimagined narrative of the human-technology relationship[11]. As the driving force behind the transformation emanating from the Fourth Industrial Revolution, they are dramatically upending the ways we live, communicate, work, and recreate. In doing so, they are signaling the beginning of a significant paradigm shift for the entire fabric of our social, political, and economic systems.

Unlike its predecessors, the Fourth Industrial Revolution actively shatters the orthodox technological operation frame, prompting a pivot in our perspective from isolated, individual innovations to a new lens of integrated, interactive, and reciprocally influencing systems of technology. The technological and chronological linearity that characterized the previous revolutions is rendered redundant as multiple synergistically linked technologies leap forward simultaneously. This cyborg of technology is thus poised to deliver a lasting and profound influence on our world, reshaping

[8] RUSSELL, NORVIG 2016; LASCHI, MAZZOLAI, CIANCHETTI 2016, 3-18.
[9] QUARTA, TREZZA 2021.
[10] SICILIANO, KHATIB 2016.
[11] CAMPAGNOLI 2021, 40-84; CAMPAGNOLI, AMATO 2022, 309-322.

our future in ways that we are still grappling to fully understand and explore[12].

2. DEFINING THE DISTINCTIONS: HARDWARE, ROBOTICS, SOFTWARE, AND ARTIFICIAL INTELLIGENCE

We live in an era of unparalleled technological progress, marking a crucial turning point where the tangible reality steadily merges with the virtual realm. At its core, this revolution thrives on the orchestrated harmony of four key components: hardware, software, robotics, and artificial intelligence. Each intertwined strand contributes its unique character, shaping a multifaceted technological tapestry that profoundly reshapes contemporary society. Simultaneously, each element gives rise to significant legal considerations[13].

Hardware, often thought of as the physical infrastructure of technology, underpins all digital operations. It includes everything we can touch – the screens, microchips, hard drives, circuits, wires, and support peripherals. These complex technocentric monuments play an indispensable role in transforming binary data into comprehensible information, enabling us to interact with the digital world[14]. But beneath the sheen of efficient hardware systems lay mazes of legal challenges.

From an individual possession standpoint, right-to-repair[15] debates question the extent to which consumers can intervene with their devices. Overtly protective manufacturer warranties often limit hardware modifications, sometimes even problem-solving repairs, spurring serious implications for consumer rights. A surge in hardware production casts an ominous shadow

[12] SCHWAB 2016; FLORIDI 2014.
[13] KAGERMANN, WAHLSTER, HELBIG 2013.
[14] MORRIS MANO 2017.
[15] GONZALES, KIM, WANG 2023, 162-177; JIN, YANG, ZHU 2023, 1017-1036.

over environmental legislation, raising crucial questions about responsible e-waste management and unchecked depletion of critical raw materials.

The "Proposal for a Directive on common rules promoting the repair of goods"[16] represents a significant step in addressing these concerns related to hardware. This proposal, put forth by the European Union, aims to promote the repairability of various goods, including electronic devices. It advocates for rules that encourage manufacturers to design products with repairability in mind, ensuring that consumers have access to replacement parts, repair manuals, and support for independent repairs.

Moreover, the proposal seeks to extend the lifespan of products, reducing the need for frequent hardware replacements and thus mitigating the environmental impact associated with e-waste. It protects consumer rights by enabling individuals to have their devices repaired by third parties without voiding manufacturer warranties. Equally paramount are legal concerns related to unchecked surveillance capabilities offered by sophisticated hardware, pushing modern privacy norms to their limits. In today's digital landscape, the rapid advancement of surveillance technology has ushered in a new era of potential privacy infringements. These sophisticated tools, including high-resolution cameras, facial recognition systems, and pervasive data tracking, empower various entities to collect, analyze, and store vast amounts of personal information.

This technological prowess, while offering benefits in terms of security and efficiency, has also raised red flags from a legal and ethical standpoint. The unchecked use of such surveillance capabilities can lead to a significant erosion of individual privacy rights. Legal frameworks, such as the General

[16] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of March 22nd 2023, on common rules promoting the repair of goods and amending Regulation (EU) 2017/2394, Directives (EU) 2019/771 and (EU) 2020/1828 – COM/2023/155 final.

Data Protection Regulation (GDPR)[17] in the European Union, have been established to mitigate these concerns. GDPR, for instance, places stringent requirements on data processing and ensures transparency and individual consent.

Nonetheless, the tension between the potential for misuse of surveillance technology and the imperative to maintain privacy norms remains a pressing issue[18]. Striking the right balance between security, individual liberties, and legal compliance is a complex challenge that societies worldwide are grappling with.

Furthermore, the unchecked surveillance capabilities can have far-reaching implications, extending beyond legal boundaries to affect social trust, civil liberties, and the potential for abuse of power. The need for comprehensive legal frameworks and robust ethical considerations to govern the use of surveillance hardware is more evident than ever.

Advanced surveillance hardware has ushered in a new era of capabilities and possibilities, it has also underscored the vital importance of upholding modern privacy norms within the bounds of legal frameworks. The responsible and ethical utilization of surveillance technology remains a crucial focal point in the ongoing discourse on privacy in the digital age.

Software, the intangible mental force of technology, infuses life into these corporeal entities. It is the architect that commands the tangible hardware to perform desired tasks, representing the bridge connecting human intent and machine action. As software's complexity heightens, however, it simultaneously steers us into a labyrinth of legal predicaments.

---

[17] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of April 27th 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[18] LYON, ZUREIK 1996, 1-18; MANCARELLA 2019, 155-178; FRIEDEWALD *et al.* 2017; HELZEL 2023, 146-150; BLENGINO 2015, 41-56.

Evolving software innovation increasingly grapples with convoluted intellectual property rights. For instance, whether or not algorithms – the lifeblood of software – can be patented, remains an intensively debated issue. Unregulated code plagiarism and ownership disputes can occur, often leading to litigious deadlocks. Furthermore, user-centric software often necessitates collecting bulk personal data[19], opening the Pandora's box of data protection, user privacy, and consent exploitation[20].

Robotics, where hardware and software confluence to command real-world actions, has thrust us into uncharted legislative waters. As physical extensions of digital instructions, robots blur the boundaries between the human and mechanized worlds[21]. Robots invite an array of legal complexities; as autonomous or semi-autonomous objects functioning in real-life situations, they complicate our understanding of accountability. From an industrial accident with a manufacturing robot to a self-driving car[22] mishap, identifying liability becomes a confounding task. Is the user responsible, the creator of the robot, or the writer of the software code?[23] As robots become more autonomous and sophisticated, the question of who should be held responsible when things go wrong becomes increasingly complex. The legal status of robots has become a focal point in the broader debate surrounding their practical and applicative aspects, particularly in relation to civil and criminal liability arising from the actions of autonomous machines.

One of the primary legal issues is the determination of liability. Traditional legal frameworks are based on the premise that only humans can be held accountable for their actions. However, with robots, the lines of

[19] CERRINA FERONI *et al.* 2022, 23-46; ZICCARDI 2016, 469-497.
[20] BESSEN, MEURER 2008.
[21] SICILIANO, KHATIB 2016.
[22] BECK 2017, 227-251.
[23] RUFFOLO 2018; COPPINI 2018, 713-740; ALBANESE 2019, 995-1044; FINOCCHIARO 2020, 713-731.

responsibility become blurred. If a robot causes harm, is the fault of the manufacturer, the programmer, the user, or the robot itself? Until now, the application of existing laws has allowed us to associate the actions of artificial agents with the owner, user, manufacturer, or programmer. However, the evolution and widespread use of these machines have led to increasingly complex scenarios in the human-machine relationship, necessitating a comprehensive and precise legal framework regarding the duties and responsibilities of artificial agents and other actors involved in the innovation process.

The concept of product liability, where manufacturers are held responsible for defects that cause harm, may seem applicable. However, this becomes complicated when dealing with AI robots that learn and evolve over time. In such cases, the robot's actions may not be a direct result of the manufacturer's programming, making it difficult to hold the manufacturer liable.

Another legal issue is the lack of a legal personality[24] for robots. In law, only persons (natural or legal) can bear rights and duties. If a robot, particularly an autonomous one, causes harm, it cannot be sued or held legally responsible because it is not a legal person.

The European Parliament, with its Resolution of February 16, 2017, has taken a concrete step towards a harmonized and unified discipline in all Member States on civil liability for possible damages caused by robots and artificial intelligence. Specifically, points 51-55 of the Resolution highlight the need for the Commission to present a legislative proposal "on legal issues related to the development and use of robotics and artificial intelligence" without "in any way limiting the type or extent of damages that can be compensated, nor [...] limit the forms of compensation that can be offered to the injured party simply because the damage is caused by a non-human subject".

[24] FARINA, CAMPAGNOLI 2022.

Regarding criminal liability[25], two different approaches can be envisaged. The first frames the robot as a mere object and therefore not criminally liable. The investigation here focuses on the responsibility of the person who programmed or used the tool intentionally, with direct attribution of the action, or negligently, if errors are found in programming, construction, maintenance, or use. On the other hand, the robot could be framed as a new (non-human) subject of criminal law and therefore criminally liable. This approach, not immediately practicable, would only be feasible through a redefinition of the constitutional principle of personal criminal responsibility and, consequently, also of subjective capacity, action, and guilt.

At the European level, there has also been a proposal to introduce mandatory civil liability insurance for those who produce the goods that caused the damage. This solution could potentially discourage the development of new intelligent products. The future legislative instrument, according to the European Parliament, should be based on "a thorough assessment by the Commission to determine whether to apply the approach of strict liability or risk management". This highlights the complexity and urgency of the legal issues surrounding the liability of robots.

Artificial Intelligence, the 'brain' of this revolution, stands as a testament to human ingenuity[26]. AI's monumental capacity to process colossal data sets, learn novel issues autonomously, and make predictive decisions, however, also expose glaring legal gaps. From a privacy lens, AI's data appetites can dwarf any contemporary system, necessitating stricter data-handling regulations. Another stark challenge is AI's capability to generate original content. AI algorithms producing art or music currently exist in a gray area of intellectual property law and legal updates have struggled to keep pace.

It is clear from the above that this accelerated transition into the Fourth Industrial Revolution, propelled by the convergence of hardware, software,

[25] KING *et al.* 2020, 89-120.
[26] RUSSELL, NORVIG 2016.

AI, and robotics, stands as an emblem of our innovative spirit. However, nested within the promise of this exciting reality lie significant, complex challenges in legal understanding and institutional regulation[27]. It is essential to develop a comprehensive, adaptable, and robust legal framework, capable of navigating these challenges. Only then can we fully realize the potential of this technological renaissance while safeguarding societal norms, rights, and protections[28].

3. HARDWARE *VS.* ROBOTICS AND SOFTWARE *VS.* ARTIFICIAL INTELLIGENCE: THEIR CRUCIAL YET SEPARATE ROLES

Moving now to a deeper level of analysis it becomes evident that the nodal elements of this seismic shift – hardware, software, robotics, and artificial intelligence – hold separate yet supremely crucial roles. These underpin the revolution's vibrant core, driving the integration of our physical and digital worlds. However, the convergence of these discrete technological domains also interlinks independent legal territories, spawning a complex web of legal challenges[29].

Consider hardware, the physical embodiment of digital technology, the nerves, and sinews of the revolution. Hardware provides the tangible infrastructure on and around which all digital activities revolve. Ranging from microchips to fiber optic cables, screens to satellites, these devices facilitate human interaction with the virtual arena, translating obscure binary code into meaningful information[30].

---

[27] AMATO MANGIAMELI 2017, 87-112; MOBILIO 2020, 401-424.
[28] SCHWAB 2016.
[29] PYLE, SAN JOSÉ 2015, 44-53.
[30] TANENBAUM, WOODHULL 1997.

Robotics symbolizes an engineering narrative where hardware synchronizes with software to conduct physical tasks[31]. Positioned at the confluence of digital instructions and real-world actions, robots establish a dynamic interface that blurs the line between human and machine agency. This interaction generates a plethora of legal perplexities[32].

As mentioned in the previous paragraph, as robots assume more active roles in our everyday lives, debates around accountability become more complex. Who is to be held responsible when an autonomous vehicle causes a collision or a manufacturing robot malfunctions, leading to a factory shutdown or even worker injuries? Identifying the fault line among the end-user, the hardware manufacturer, the software programmer, or the entity that integrated the components into a functional machine is non-trivial. Clearly, our existing legal frameworks face an uphill task adjusting to this new technological narrative dominated by autonomous or semi-autonomous cyber-physical systems.

On the other side of the digital spectrum exists software. Envisioned as the invisible mind of digital technology, software drafts the command sequences that instruct hardware. It forms a dynamic bridge that channels and implements human intent into machine actions[33]. However, as software sophistication escalates, so does the complexity of associated legal predicaments.

Evolving software innovation has intricately tangled itself with intellectual property laws. Legal conundrums such as the patentability of software algorithms, the foundation stones of software, have led to an ongoing debate amongst lawmakers, innovators, and corporations.

[31] FARINA, SARACENI 2022, 329-341.
[32] SICILIANO, KHATIB 2016.
[33] TANENBAUM, WOODHULL 1997.

Historically, legal doctrine has tirelessly tackled various issues concerning the legal protection of software[34]. As technology rapidly evolves, these problems are being reproposed for the algorithms. Artificial intelligence is, fundamentally, an evolution of software, which revitalizes already faced discussions and previously provided solutions in a new scenario.

The tangible nature of the AI further complicates the application of intellectual property rights: patenting and copyrighting not only software but also algorithms[35] – a category considered as abstract ideas – are themes that come up again.[36]

Artificial intelligence represents the next step in the evolution of software, the section of the brain capable of learning and making decisions: this is one of its most complex aspects[37]. Consequently, the question arises: who holds the rights to innovations produced autonomously by AI?[38] Current laws offer little clarity on this front, hinting at another crucial area for reform.

It is apparent that the pivotal legal issues traditionally encountered in software protection are re-emerging in the sphere of AI. Given the pervasive influence of AI across diverse sectors, it is imperative that effective legal safeguards are instituted to ensure responsible AI utilization, while maintaining the principle of fair use for the progression of innovation.

By its very nature, artificial intelligence stands apart from its natural (human) counterpart, given its residence within an electronic device. However, this alone does not encapsulate its essence. Embodied AI is a rapidly evolving research frontier, often taking center stage in debates due to its tangible and captivating nature for the general public. As we gaze upon the current state of AI and ponder its potential future trajectories, we can identify three main

---

[34] ALPA, ZENO-ZENCOVICH 1987; BORRUSO 1999; CHIMIENTI 2018; DE SANCTIS 2000; FARINA 2018; RISTUCCIA, ZENO-ZENCOVICH 1993; UBERTAZZI 1994.

[35] MARMO 2020.

[36] BIAGIOLI, BUNING 2019, 3-17.

[37] SARTOR 2003, 23-52.

[38] TREVISANELLO 2019.

categories: Artificial Narrow Intelligence (ANI); Artificial General Intelligence (AGI); and Artificial Super Intelligence (ASI)[39].

The first type, ANI, also known as 'limited intelligence', is the only one currently available. These AI systems possess the computational ability to efficiently perform specific tasks, such as page tracking, chess playing, or handwritten number recognition, but lack versatility.

The second type, AGI, echoes the original concept of intelligence, translating it into algorithms with human-equivalent performance, intentionally programmed to excel in a single, narrow domain. To simplify, these are AI systems capable of performing any task at a human level.

The third type, ASI, surpasses – or rather, will surpass – human cognitive performance in virtually every field of interest. In the current technological landscape, only ANI-type intelligences are present. While it is claimed that AGI and ASI are under development through machine learning and deep learning techniques, an optimistic segment of scientific literature predicts the first AGI will only be available by 2029, and ASI by 2045. This forecast is tempered by a more prevalent view that pegs the arrival of AGI and ASI at 2100 and 2130 respectively.

Among the authoritative voices advocating for the imminent arrival of strong AI, Raymond Kurzweil[40] believes that the "singularity is near", and that the exponential growth of technology will soon surpass human intelligence and reasoning. Indeed, the technological progress witnessed in recent years is quite remarkable, and the various sciences involved are not only concerned with whether machines are (or can be) intelligent, but also whether they are (or can be) moral (and emotional). It is against this backdrop that we question whether machines can be deemed trustworthy[41].

---

[39] SIGNORELLI 2019; BOSTROM 2006, 66-73; BOSTROM 2018; BOSTROM, YUDKOWSKY 2011, 316-334.

[40] KURZWEIL 2005.

[41] FARINA 2022.

Trust in this context can be defined as the belief or confidence that the robot will act predictably, reliably, and according to its intended purpose. This trust is built over time, through repeated interactions and experiences where the robot proves its reliability and effectiveness.

However, this trust can be fragile. If a robot malfunctions or behaves unpredictably, it can quickly erode the trust that has been built. This is why it's crucial for robots to be designed and programmed with reliability and predictability in mind.

Moreover, trust can also be influenced by a robot's appearance and behavior. Robots that look and behave more human-like tend to be trusted more, as humans can more easily relate to them. This is known as the "uncanny valley" phenomenon, where robots that are almost, but not quite, human-like can be unsettling and less trustworthy.

In addition, ethical considerations also play a role in the trust relationship. As robots become more autonomous, questions arise about their decision-making capabilities and the implications of their actions.[42].

4. TRUSTING THE TECHNOLOGY: THE EVOLVING RELATIONSHIP BETWEEN HUMANS AND INTELLIGENT ROBOTS

Trust is often recognized as a crucial factor in the broader acceptance of technological systems[43] and, particularly, robotics. The matter of assessing this trust within human-robot interaction[44] has been approached in two

[42] SCHWAB 2016.

[43] PARASURAMAN 1997, 230-253.

[44] SCHAEFER 2013; BILLINGS *et al.* 2012; YAGODA, GILLAN 2012, 235-248; HANCOCK *et al.* 2011, 517-527; HEERINK *et al.* 2009, 1909, 1923; HOFFMAN *et al.* 2009, 5-11; BURKE *et al.* 2007, 606-632; BIROS *et al.* 2004, 173-189; LEE, SEE 2004, 50-80; MAYER *et al.* 1995, 709-734; ROTTER 1971, 443-452.

major ways. Objective[45] or implicit methods focus on analyzing people's uncontrolled behavioral responses, like response times. In contrast, subjective[46] or explicit measures employ consciously supplied verbal data such as survey responses or opinions.

A clear understanding of these methods' benefits and limitations is necessary for evaluating our trust in robots and AI. Though objective measures can yield insights into humans' raw, unmediated reactions to robots, revealing underlying beliefs, these methods are less popular than their subjective counterparts. And yet, both contribute valuable information about perceived security – a critical parameter in accepting physical or social interactions with robots.

To better explore the intricacies of trust from a psychological perspective, a useful tool can be the media equation theory. It posits that people subconsciously treat computer systems as social actors during cooperative tasks, providing an assessment of the user's faith in the system's reliability and capability.

Recent studies have examined human-robot trust through such interactive settings, revealing a preference for robots with human-like resemblance – both physical and vocal – since such robots evoke emotions and sense of connection like human interactions. The principle being, the more we understand the other, the more likely we are to trust them. This trust develops through a progressive and dynamic process, informed by past experiences and subject to constant change.

Although there seems to be a shift in our understanding of trust as the AI sector develops, it's important to differentiate between trust and accountability. Trust, in essence, means delegating a specific action to someone or something. But ensuring that the substance or entity being trusted could fulfill that task is crucial.

---

[45] HOFMANN *et al.* 2005, 1369-1385.

[46] DESTENO *et al.* 2012, 1549-1556; LEE *et al.* 2013, 1-14; HEERINK *et al.* 2009, 1909-1923; STEINFELD *et al.* 2006, 33-40.

Unlike humans, robots and AI do not meet the specific requirements of trust, however, they can contribute to creating a form of "virtual trust" or "almost-trust"[47]. This type of trust could mislead individuals about AI's abilities and only pertains to the rational aspect of trust. Analyzing AI through the three dominant aspects of trust (affective, rational, and normative) might help assess if AI is indeed trustworthy.

Affective value implies that the trustor trusts in the goodwill of the trustee, but as AI lacks emotional capacities, it's impossible for their responses to be guided by feelings. Similarly, the normative value assumes moral responsibility which AI cannot inherently possess. It's only within the rational aspect of trust, where past experience, cultural background, and related psychological factors, does AI possess an element of trustworthiness. However, this alone isn't sufficient to build complete trust, especially the type observed in human relationships.

By recognizing and understanding these distinctions, developers, implementers, and users can apply a more informed and nuanced approach to trust in AI and robotics. The capacity for robots and artificial intelligence to prove their reliability in a task doesn't automatically translate to the ability to foster authentic trust. A vital aspect of this understanding lies in realizing that AI can't inherently uphold moral responsibility or display genuine emotional reactivity, both key components of human trust dynamics.

As we move forward in the artificial intelligence era and as robots increasingly integrate into various human sectors, it's imperative to maintain a clear and realistic perspective on trust in AI technology. Trust has an affective, normative, and rational aspect, and while AI can satisfy some aspects under the right circumstances, it's still a long way from fulfilling the criteria for genuine trust that play out in human-human interactions.

[47] COECKELBERGH 2012.

5. ADAPTING LEGAL FRAMEWORKS TO EMBRACE THE INTEGRATED FUTURE OF HARDWARE, SOFTWARE, AI, AND ROBOTICS

Navigating the legal challenges in the domain of hardware, software, artificial intelligence, and robotics necessitates an in-depth understanding of these technologies, their interaction, and implications. To begin, legal distinctions are inherently complex due to the evolving nature of these tech entities. This complexity extends beyond just defining these technologies but also incorporates their synthesis and the development of novel legal frameworks to adapt to their synergy[48].

One approach is to push for technology-neutral laws[49]. This approach emphasizes on the functionality and consequences of technological advancements rather than their form. It posits, therefore, the need to ensure that the applicable law remains consistent despite the technological advancements, thereby minimizing legal uncertainty and promoting innovation.

However, even technology-neutral laws may fail to cover all scenarios, particularly with the ceaseless innovations in AI and robotics[50]. Navigating this landscape requires flexible and adaptable legal mechanisms. Recently, part of the legal doctrine[51] proposes 'Regulatory Sandboxes': controlled environments which allow testing innovative solutions under the watchful eyes of regulators, enabling swift identification and mitigation of potential risks without stifling innovation. This legal-sandbox approach facilitates experimentation while ensuring accountability, thereby neatly addressing the innovation-regulation dilemma.

---

[48] HILDEBRANDT 2016.
[49] CASAROSA 2022.
[50] BROWN 2013.
[51] ZETZSCHE *et al.* 2017, 31-103.

Another key principle to consider, according to Solum and Chung[52], is the 'Layers Principle', which posits the necessity of tailoring legal regulations to match the specificities of each layer of the complex Internet architecture. By extension, as AI and robotics become increasingly embedded in this architecture, a comparable approach would involve crafting regulations that consider the specific challenges and possibilities associated with each technological layer.

The legal landscape at the intersection of hardware, software, AI, and robotics is an intricate terrain requiring ongoing stakeholder dialogue, flexible and adaptable mechanisms, regulatory innovation, and judicious application of legal principles for successful navigation. Therefore, future research should focus on continuous engagement between regulators, legal scholars, technologists, and industry practitioners to explore the untapped potential in these technologies while effectively managing the risks. Cooperative efforts between such a diverse pool of specialists can undoubtedly lead to comprehensive legislation that supports innovation, promotes fairness, and ensures legal and ethical compliance.

To ensure that the legal framework keeps pace with technological progress and challenges, the regulatory bodies should be open to constant learning, adapting, and evolving, and consider working collaboratively with technologists. This cooperative and proactive approach is crucial to leveraging the benefits of the Fourth Industrial Revolution while mitigating its possible negative impacts, thus resulting in a positive outcome for society at large.

In essence, navigating the legal challenges, while complex, is not insurmountable when there is an interdisciplinary dialogue, flexibility in legal interpretation, and commitment to regulatory innovation. A precedent-based approach, though useful, may not always be sufficient, given the unprecedented nature of challenges posed by these technologies. Therefore, legal scholars, regulators and technologists must foster a shared

[52] SOLUM, CHUNG 2004, 815-878.

understanding and work collaboratively to develop principles that are both technology-neutral and flexible enough to accommodate future advancements.

The law-participant-technology interplay involves an intricate dynamic alignment process that also necessitates an appreciation of the socio-technical contingencies that these technologies involve. Hence the importance of continuously updating regulatory frameworks in response to the insights gained from their application.

Any legal framework developed must be guided by the principles of good governance, and must address challenges to privacy, copyright, and liability to ensure that the transitions catalyzed by the new Revolution era are legally sound and ethically guided. The ultimate goal is to ensure that inclusive, sustainable, and human-centric laws govern the Fourth Industrial Revolution, promoting its benefits while minimizing potential harms.

The complexity lies not just in the technical aspects of these technologies but also in their ethical, legal, and social implications, making this an extremely challenging yet necessary field of study for a better future society. Acknowledging this complexity is the first step towards crafting nuanced and effective legislation. A committed and collaborative approach towards understanding these challenges can not only help navigate the legal landscape but also engage in proactive lawmaking, thereby shaping a future where technology serves humanity's best interests[53].

It is incumbent upon the legal community to deliver judicious decisions that set meaningful precedents and provide clarity around the deployment and implications of Fourth Industrial Revolution technologies. To complement this, scholars and policymakers must work in tandem to synthesize multi-disciplinary research findings into actionable policies, with a constant focus on balancing technological advancement with ethical considerations[54].

---

[53] HILDEBRANDT 2016.

[54] MORO 2015, 525-544.

In closing, navigating the legal challenges at the nexus of hardware, software, artificial intelligence, and robotics during the Fourth Industrial Revolution presents a complex but not insurmountable task. The openness for interdisciplinary dialogue, recognition of boundaryless technologies, and the need for adaptable regulatory frameworks need to be at the forefront of these discussions. These strategies would indeed help guide the proper integration of these technologies into society and harness their immense potential safely and responsibly.

REFERENCES

ALBANESE, Antonio, *La responsabilità civile per i danni da circolazione di veicoli ad elevata automazione*, 995-1044, in *Europa e Diritto Privato*, 4/2019.

ALPA, Guido, ZENO-ZENCOVICH, Vincenzo, *I contratti di informatica*, Milan, 1987.

AMATO MANGIAMELI, Agata C., *Tecno-diritto e tecno-regolazione. Spunti di riflessione*, 87-112, in *Rivista di filosofia del diritto*, special edition, 2017.

– *Algoritmi e big data. Dalla carta sulla robotica*, 107-124, in *Rivista di filosofia del diritto,* 1, 2019.

– *Intelligenza artificiale, big data e nuovi diritti*, 93-101, in *Rivista italiana di informatica e diritto*, 1/2022.

AMATO MANGIAMELI, Agata C., CAMPAGNOLI, Maria Novella, *Strategie digitali. #diritto_educazione_tecnologie*, Turin, 2020.

AMATO MANGIAMELI, Agata C., SARACENI, Guido (eds.), *Cento e una voce di informatica giuridica*, Turin, 2023.

BECK, Susanne, *Google cars, software agents, autonomous weapons systems. New challenges for criminal law?*, 227-251, in HILGENDORF, Eric, SEIDEL, Uwe (eds.), *Robotics, Autonomics, and the Law*, Baden-Baden, 2017.

BESSEN, James, MEURER, Michael J., *Patent Failure: How judges, bureaucrats, and lawyers put innovators at risk*, Princeton, 2009.

BIAGIOLI, Mario, BUNING, Marius, *Technologies of the law/law as a technology*, 3-17, in *History of Science*, 57, 1/2019.

BILLINGS, Deborah R., SCHAEFER, Kristin E., HANCOCK, Peter A., *What is Trust? Defining the construct across domains*, Orlando, 2012.

BIROS, David P., DALY, Mark, GUNSCH, Gregg, *The influence of task load and automation trust on deception detection*, 173-189, in *Group Decision and Negotiation*, 13/2004.

BLENGINO, Cecilia Piera *et al.*, *Smart cities e smart citizens: trasformazioni e rappresentazioni della sicurezza nell'era della dataveglianza*, 41-56, in Raffaella BRIGHI, Raffaella, ZULLO Silvia (eds.), *Filosofia del diritto e nuove tecnologie Prospettive di ricerca tra teoria e pratica*, Rome, 2015.

BORRUSO, Renato, *La tutela giuridica del software, diritto d'autore e brevettabilità*, Milan, 1999.

BOSTROM, Nick, *Ethical Issues in Advanced Artificial Intelligence*, 66-73, in *Review of Contemporary Philosophy*, 5, 1-2/2006.

– *Superintelligenza. Tendenze, pericoli, strategie*, trad. it., Turin, 2018.

BOSTROM, Nick, YUDKOWSKY, Elizer, *The ethics of artificial intelligence*, 316-334, in RAMSEY, William, FRANKISH, Keith (eds.), *Cambridge Handbook of Artificial Intelligence*, Cambridge, 2011.

BROWN, Ivan, MARSDEN, Christopher T., *Regulating Code: Good Governance and Better Regulation in the Information Age*, Cambridge, 2013.

BRYNJOLFSSON, Eric, McAFEE, Andrew, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*, New York-London, 2016.

BURKE, Shawn C., SIMS, Dana E. *et al.*, *Trust in Leadership: A multi-level review and integration*, 606-632, in *The Leadership Quarterly*, 18/2007.

CALO, Ryan, *Artificial Intelligence Policy: A Primer and Roadmap*, 404-429, *University of Washington School of Law Research Paper*, 2017.

CAMPAGNOLI, Maria Novella, *Funzionare o essere? Appunti e spunti in tema di potenziamento umano*, 40-84, in Ircocervo, 20, 2/2021.

CASAROSA, Federica, *Technology-Neutral Legislation: Are Judges Able to Keep Pace with Technological Innovation?*, in *SSRN*, 2023.

CERRINA FERONI, Ginevra *et al.*, *Intelligenza artificiale e protezione dei dati personali: percorsi di analisi*, 23-46, in CERRINA FERONI, Ginevra *et al.* (eds.), *AI Anthology. Profili giuridici, economici e sociali dell'intelligenza artificiale*, Bologna, 2022.

CHIMIENTI, Laura, *La tutela del software nel diritto d'autore*, Milan, 2000.

COECKELBERGH, Mark, *How I Learned to Love the Robot: Capabilities, Information Technologies, and Elderly Care*, in OOSTERLAKEN, Ilse, HOVEN, Joroen (eds), *The Capability Approach, technology and design*, New York-London, 2012.

COPPINI, Laura, *Robotica e intelligenza artificiale: questioni di responsabilità civile*, 713-740, in *Politica del diritto*, 49, 4/2018.

CURTIN, Dennis P., FOLEY, Kim *et al.*, *Informatica di base*, Milan, 2005.

DE SANCTIS, Giovanni, *La tutela giuridica del software tra brevetto e diritto d'autore*, Milan, 2000.

DESTENO, David, BREAZEAL, Cynthia *et. al.*, *Detecting the trustworthiness of novel partners in economic exchange*, 1549-1556, in *Psychological Science*, 23/2012.

FARINA, Massimo, *I contratti informatici*, Milan, 2018.

– *Ridefinizione del perimetro fiduciario del rapporto uomo-macchina*, 391-401, in Cristiano CICERO (ed.), *Studi Economico-Giuridici*, Napoli, 2022.

– *Hardware/Software*, 248-252, in AMATO MANGIAMELI, Agata C., SARACENI, Guido (eds.), *Cento e una voce di informatica giuridica*, Turin, 2023.

FARINA, Massimo, CAMPAGNOLI, Maria Novella, T*ec-no-identità?: percorsi, provocazioni e istanze delle nuove s/oggettività*, Milan, 2022.

FARINA, Massimo, SARACENI, Guido, *Robotica*, 329-341, in Paola B. HELZEL, Paola B, PISANÒ, Attilio, TARANTINO, Giovanni (eds.), *Enciclopedia di bioetica e scienza giuridica*, Naples, 2022.

FINOCCHIARO, Giusella, *Intelligenza artificiale e responsabilità*, 713-731, in *Contratto e impr*esa, 36, 2/2020.

FLORIDI, Luciano, *The Fourth Revolution: How the infosphere is reshaping human reality*, Oxford, 2014.

FRIEDEWALD, Michael *et al.*, *Surveillance, privacy and security*, Milton Park, 2017.

GONZALES, Amy L., KIM, Yeweon *et al.*, *Multisolving innovations: How digital equity, e-waste, and right-to-repair policies can increase the supply of affordable computers*, 162-177, in *Policy & Internet*, 15, 2/2023.

GOODMAN, Bryce, FLAXMAN, Seth, *EU regulations on algorithmic decision-making and a "right to explanation"*, 50-57, in *AI Magazine*, 38, 3/2017.

HANCOCK, Peter A., BILLINGS, Deborah R. *et al.*, *A meta-analysis of factors affecting trust in human-robot interaction*, 517-527, in *Human Factors*, 53, 5/2011.

HEERINK, Marcel, KROSE, Ben *et al.*, *Influence of social presence on acceptance of an assistive social robot and screen agent by elderly users*, 1909-1923, in *Advanced Robotics*, 23/2009.

HELZEL, Paola B., *Dataveglianza*, 146-150, in AMATO MANGIAMELI, Agata C., SARACENI, Guido (eds.), *Cento e una voce di informatica giuridica*, Turin, 2023.

HILDEBRANDT, Mireille, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology*, Cheltenham, 2015.

HOFFMAN, Robert R. *et al.*, *The Dynamics of Trust in Cyberdomains*, 5-11, in *IEEE Intelligent Systems*, 24, 6/2009.

HOFMANN, Wilhelm, GAWRONSKI, Bertram *et al.*, *A meta-analysis on the correlation between the implicit association test and explicit self-report measures*, 1369-1385, in *Personality and Social Psychology Bulletin*, 31, 10/2005.

JIN, Chen, YANG, Luyi *et al.*, *Right to repair: Pricing, welfare, and environmental implications*, 1017-1036, in *Management Science*, 69, 2/2023.

KAGERMANN, Henning, WAHLSTER, Wolfgang *et al.*, *Recommendations for implementing the strategic initiative Industrie 4.0: Securing the future of German manufacturing industry*, Forschungsunion, 2013.

KING, Thomas C., AGGARWAL, Nikita *et al.*, *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*, 89-120, in *Science and engineering ethics*, 26, 1/2020.

KURZWEIL, Raymond, *The Singularity Is Near: When Humans Transcend Biology*, New York, 2005.

LASCHI, Cecilia, MAZZOLAI, Barbara *et al.*, *Soft Robotics: Technologies and Systems Pushing the Boundaries of Robot Abilities*, eaah3690, in *Science Robotics*, 1, 1/2016.

LEE, Jin Joo, KNOX, Bradley W. *et al.*, *Computationally modeling interpersonal trust*, 1-14, in *Frontiers in Psychology*, 4/2013.

LEE, John D., SEE, Katrina A., *Trust in automation: Designing for appropriate reliance*, 50-80, in *Human Factors*, 46, 1/2004.

LEE, MinHwa, YUN, Jinhyo Joseph *et al.*, *How to Respond to the Fourth Industrial Revolution, or the Second Information Technology Revolution? Dynamic New Combinations between Technology, Market, and Society through Open Innovation*, 1-24, in *J. Open Innov. Technol. Mark. Complex.*, 4, 3/2018.

LYON, David, ZUREIK, Elia, *Surveillance, privacy, and the new technology*, 1-18, in LYON, David, ZUREIK, Elia (ed.), *Computers, surveillance, and privacy*, 1996.

MANCARELLA, Marco, *La società digitale nel contesto internazionale: tra controllo, libertà e nuovi diritti*, 155-178, in *Eunomia. Rivista di Studi su Pace e Diritti Umani*, 1/2019.

MARMO, Roberto, *Algoritmi per l'intelligenza artificiale. Progettazione dell'algoritmo, dati e machine learning, neural network, deep learning*, Milan, 2020.

MAYER, Roger C., DAVIS, James H. *et al.*, *An integrative model of organizational trust*, 709-734, in *Academy of Management Review*, 20/1995.

MENELL, Peter, LEMLEY, Mark *et al.*, *Intellectual property in the new technological age*, Clause 8 Publications, 2018.

MOBILIO, Giuseppe, *L'intelligenza artificiale e i rischi di una "disruption" della regolamentazione giuridica*, 401-424, in *BioLaw Journal-Rivista di BioDiritto*, 2/2020.

MORO, Paolo, *Libertà del robot? Sull'etica delle macchine intelligenti*, 525-544, in BRIGHI, Raffaella, ZULLO, Silvia (eds.), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, Rome, 2015.

MORRIS, Mano M., *Computer System Architecture*, London, 2017.

PARASURAMAN, Raja, RILEY, Victor, *Humans and automation: Use, misuse, disuse, abuse,* 230-253, in *Human Factors*, 39/1997.

PERZANOWSKI, Aaron, SCHULTZ, Jason, *The End of Ownership: Personal Property in the Digital Economy*, Cambridge, 2016.

PYLE, Dorian, SAN JOSE, Cristina, *An executive's guide to machine learning*, 44-53, in *McKinsey Quarterly*, 3/2015.

QUARTA, Elena, TREZZA, Remo, *Driverless car o driverless law: quale direzione prenderà il diritto per evitare "incidenti sistematici"?*, 1-18, in *Cultura giuridica e diritto vivente*, 8/2021.

RISTUCCIA, Renzo, ZENO-ZENCOVICH, Vincenzo, *Il software nella dottrina, nella giurisprudenza e nel d.lgs. 518/92*, Padua, 1993.

ROTTER, Julian B., *Generalized expectancies for interpersonal trust*, 443-452, in *American Psychologist*, 26/1971.

RUFFOLO, Ugo, *Per i fondamenti di un diritto della robotica self-learning; dalla machinery produttiva all'auto driverless: verso una 'responsabilità da algoritmo'?*, 1-28, in RUFFOLO, Ugo (ed.), *Intelligenza artificiale e responsabilità*, Milan, 2018.

RUSSELL, Stuart, NORVIG, Peter, *Artificial Intelligence: A Modern Approach*, London, 2016.

SARTOR, Giovanni, *L'intenzionalità dei sistemi informatici e il diritto*, 25-52, in *Rivista trimestrale di diritto e procedura civile*, 57, 1/2003.

SCHAEFER, Kristin, *The perception and measurement of Human-Robot trust*, PhD Dissertation, 2013.

SCHWAB, Klaus, *The Fourth Industrial Revolution*, London, 2016.

SICILIANO, Bruno, KHATIB, Oussama, *Handbook of Robotics*, Berlin, 2016.

SIGNORELLI, Andrea D., *Rivoluzione artificiale: l'uomo nell'epoca delle macchine intelligenti*, Milan, 2019.

SOLUM, Lawrence, CHUNG, Minn, *The Layers Principle: Internet Architecture and the Law*, 815-878, in *Notre Dame Law Review*, 79, 2/2004.

STAHL, Bernd C., *IT for a Better Future: How to Integrate Ethics, Politics and Innovation*, 140-156, in *Journal of Information, Communication and Ethics in Society*, 9, 3/2011.

STEINFELD, Aaron, FONG, Terrence, KABER, David, LEWIS, Michael, SCHOLTZ, Jean, SCHULTZ, Alan, GOODRICH, Michael, *Common metrics for human-robot interaction*, 33-40, in *Conference on Human-robot interaction*, 2006.

TANENBAUM, Andrew S., WOODHULL, Albert S., *Operating Systems Design and Implementation*, New Jersey, 1997.

TREVISANELLO, Laura, *Macchine intelligenti che creano ed inventano. Profili e rilievi critici del nuovo rapporto tra intelligenza artificiale e diritti di proprietà intellettuale*, in *Trento Law and Technology Research Group Student Papers Series*, 54/2019.

UBERTAZZI, Luigi C., *La legge sul software. Commentario sistematico*, Milan, 1994.

WEST, Darrel M., *The Future of Work: Robots, AI, and Automation*, Washington, 2019.

YAGODA, Rosemarie E., GILLAN, Douglas J., *You want me to trust a robot? The development of a human-robot interaction trust scale*, 235-248, in *International Journal of Social Robotics*, 4, 3/2012.

ZARSKY, Tal, *The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision-Making*, 118-132, in *Science, Technology, & Human Values*, 41, 1/2016.

ZETZSCHE, Dirk A., BUCKLEY, Ross P., ARNER, Douglas W., BARBERIS, Janos N., *Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation*, 31-103, in *Fordham Journal of Corporate and Financial Law*, 23, 1/2017.

ZICCARDI, Giovanni, *La protezione informatica dei dati in ambito professionale*, 469-497, in *Cyberspazio e Diritto*, 17/2016.