LIVING WITH THE ALGORITHM

Toward a New Social Contract in the Age of AI

$$A \wedge B \to A$$
$$A \wedge B \to B$$
$$A \to (B \to A \wedge B)$$
$$A \to A \vee B$$
$$B \to A \vee B$$
$$(A \to C) \to ((B \to C) \to (A \vee B \to C))$$

$$A \wedge B \to A$$
$$A \wedge B \to B$$
$$A \to (B \to A \wedge B)$$
$$A \to A \vee B$$
$$B \to A \vee B$$
$$(A \to C) \to ((B \to C) \to (A \vee B \to C))$$

$$A \wedge B \to A$$
$$A \wedge B \to B$$
$$A \to (B \to A \wedge B)$$
$$A \to A \vee B$$
$$B \to A \vee B$$
$$(A \to C) \to ((B \to C) \to (A \vee B \to C))$$

LIVING WITH THE ALGORITHM
Toward a New Social Contract in the Age of AI

PROLOGUE: THE IMPORTANCE OF CIVIL SOCIETY IN RAISING AWARENESS

Nowadays, algorithms are constantly used in different areas of life to improve the quality of services, enhance user experience, and optimize efficiency. Their use is very diverse: from advertising and selecting prospective students in university admissions processes to detecting issues in tax declarations. However, challenges surrounding privacy, security, autonomy, and many other areas go hand-in-hand with opportunities.

One particularly clear issue that arises from this widespread use of algorithms is **a lack of awareness**. This is true of not only the side legislators who struggle to regulate emerging technologies, but also citizens that are uninformed about the ever-increasing infiltration of algorithms in various contexts. Thus, **algo-awareness** is of critical importance these days. As defined by the European Commission, the term "algo-awareness" refers to the spreading of an evidence-informed understanding of algorithms, with regard to their role in online platforms as well as emerging issues and opportunities surrounding them.[i]

The timing is critical both for European citizens as well as citizens all over the globe. The European Union, which has been forming a strategy for artificial intelligence (AI) since 2018,[ii] most recently (on February 19th 2020) published a White Paper on AI titled "A European approach to excellence and trust."[iii] Indeed, the discussion of algorithms is central to any discussion about AI which has been simply defined as "a collection of technologies that combine data, algorithms, and computing power".[iv]

In a nutshell, the Commission seems to be taking a two-fold regulatory and investment-oriented approach to AI "with a twin objective to promote the uptake of AI and of addressing the risks associated with certain uses of this new technology".[v] The White Paper, which is aimed at listing and evaluating

---

[i] European Commission's Directorate-General for Communications Networks, Content and Technology, *Algo:aware: Raising awareness on algorithms* (n.p:n.p, 2018), 120. There is indeed an algo-aware project launched by the European Commission that seeks to solve both of these information gaps. The purpose of the project has been to come up with a variety of policy options, technical solutions and private sector and civil society-driven actions, to inform EU policy-making in order to maximise the effectiveness of future algorithm regulations, as well as building general knowledge of algorithms.

[ii] European Commission, *Artificial Intelligence for Europe,* COM/2018/237 (Brussels, 2018).

[iii] European Commission, *On Artificial Intelligence – A European approach to excellence and trust*, COM/2020/65 (Brussels, 2020).

[iv] Ibid., p.2.

[v] Ibid, p.1.

different policy options to achieve the two-fold sets of objectives (regulation and investment), expressly invites for the reactions of public and private stakeholders; namely the Member States, other European institutions, industry, social partners, civil society organizations, researchers, the public in general and any interested party.[vi] This guide, which was drafted by a Legal Clinic team of IE Law School participating in a project for a Spanish civil society association, *Foro de la Sociedad Civil*, has been addressing a large number of the issues that the White Paper presents.[vii]

The purpose of the guide is to provide information to digital technology users in today's "algorithmic society". It wishes to provide citizens with a broad yet useful understanding of how algorithms work, when they are used, and how they impact our jobs, privacy, and relationships with others. We hope that this straightforward yet reliable guide succeeds in raising awareness of the important and yet sometimes disruptive role algorithms have played in our everyday lives. This will allow individuals to take a more critical stance towards the phenomenon and ensure that their use is properly understood and regulated. For those that are already aware of the importance of algorithms, we hope that this guide will deepen and widen their knowledge of relevant debates from authoritative sources.

Beyond its aim to inform, this guide strives to enlighten **citizens** about the **value they provide** with their data use in our rapidly advancing "digital society". Citizens can hold multiple roles separately or at the same time: they are consumers, employees and employers, entrepreneurs, participants and speakers in the public or their private spheres. In all of these and other roles, citizens share data that fuel—or can fuel—algorithms. The centrality of the citizens' role is the starting point of this guide.

[vi] Ibid.

[vii] IE Law School, Legal Clinic Program (Spring/Fall 2019). Members of the student team that drafted the guide: or assisted in the drafting of the guide: Tugce Altunalan, Aurora Dell' Elce (co-author), Luis Ignacio Gil Palacios, Jimena López-Navarro (co-author), Amanda Matesanz, Ellie Sande, Aleksandra Smajevic (co-author), and Adam Wilson-Barnes. Faculty supervisor: Argyri Panezi (co-author), Assistant Professor of Law and Technology, IE Law School. The project was commissioned to the Legal Clinic by the Foro de la Sociedad Civil Association, represented by Pablo García Mexía, J.D., Ph.D. (co-author), project supervisor and author of the original table of contents for the guide.
The project initiated before the Commission's recent White Paper was released (supra note 3), but after the 2018 communication of a European strategy (supra note 2). The authors have focused both the EU and on global debates.
This Guide was drafted in 2019, and reflects updates until December 2019. Few edits reflect recent developments until the 24th of February 2020.

CONTENTS

I. INTRODUCTION

1. *ALGO-AWARENESS* AS A SOCIAL NECESSITY

The use of algorithms in our everyday lives is ever-increasing amidst a hype of media focus on the so-called "life under the algorithm."[1]

As algorithms become more popular, the importance for civil society's awareness, reflection, and engagement also increases.

What is an algorithm? As our society becomes evermore data-driven, what challenges do ***big data*** pose? What are algorithmic biases and how do they link to ***machine learning*** and ***artificial intelligence*** (AI)? What does the term ***predictive analytics*** refer to? Also, why are ***transparency and accountability*** so important? These are all notions that citizens need to be familiar with in order to be algo-aware; well informed and well-equipped citizens who can participate in and benefit from the ongoing tech revolution. It is not enough to merely be aware of the technological uses, benefits, and risks associated with the spread of algorithms in the marketplace, workplace, and household. We need to form a better understanding of how these technologies work, how they serve us, what challenges they pose, and the ways in which our data is collected and processed. We must reflect on the impact of algorithms, big data, and AI on our daily lives to develop an informed opinion on what role we would like new disruptive technologies to play.

As members of civil society, it is our data that is used fuel the digital economy and drive digital transformation. In other words, our digital footprint is critical to the evolution of technological tools. This is both challenging and empowering. This guide aims to identify the challenges and facilitate the participation and empowerment of our algorithmic society.

INFORMED CITIZENS ARE EMPOWERED CITIZENS

Civil society needs to be cautious yet aware in order to benefit from algorithms. In many cases they are very useful and improve our day-to-day lives and help with our work. Why assume, for instance, that algorithms (and robots powered by algorithms) threaten to replace humans when they are mainly channeled into jobs that require repetitiveness? Why shy away from other beneficial uses of algorithms? Using awareness to make informed decisions empowers us as citizens and allows us to take advantage of the benefits of technological developments. Most of us are aware of the importance

of technology in today's society, although we do not fully understand exactly how it works or what it does for us. We also use new technologies without actually realizing it. This guide seeks to close information gaps by explaining how algorithms work, when they are used, and most importantly, their advantages and disadvantages. This will allow citizens to become more conscious of technology given its growing role in society. It will answer questions such as: What does it mean to live in an era where algorithms are embedded in both simple and in disruptive everyday technologies? How are algorithms, blockchain technology, big data, machine learning and artificial intelligence changing our reality as citizens, consumers, and entrepreneurs?

In the following pages, you will find extensive information designed to guide you through the changes that algorithms are bringing in our daily lives. First of all, we will look at what algorithms are and how they are relevant to AI. Following this, we will explore useful applications of algorithms along with their threats and challenges We will focus on how these changes affect us, the value of our data in algorithmic-driven markets, and, more importantly, the significance of our behavior within an algorithmic society. We will conclude with various reactions to these challenges and investigate important opportunities for user empowerment.

II. WHAT IS AN ALGORITHM?

1. ALGORITHMS AND DATA: WHAT ARE WE TALKING ABOUT?

1.1 Algorithms, data, and big data

The term algorithm was coined by Mohammed Ibn Musa-al-Khawarzimi who, at the end of the eighth century, developed the mathematical approach which formed the basis of the digital development of AI.[2] An algorithm is a method designed to solve problems. In its mathematical sense it is a set of information (data) ordered and arranged around an operation which, when followed, solves a problem. To use a common metaphor, algorithms resemble recipes in a cookbook—they provide a flowchart of instructions that must be followed in order to complete a specific task.[3] For an algorithm to work it must have an input (data) and an output (again, data) to a question or set of questions (a result to the problem asked to solve).

The data input is essential for algorithms. In fact, the algorithm itself is entirely neutral – the input is the critical determining factor for all potential results, be they desired or not. The data used can be understood as an ensemble of various pieces of information, presented in a way that can be read by a machine (else: can be machine-readable). When processed by algorithms, the data (input) is used to check given assumptions and, ultimately, produce results or come to conclusions (output).

The usefulness and success of AI relies on the effective management of large volumes of data, in other words, big data.[4] Big data is basically large sets of data that can be collected and processed by technology. Big data can be analyzed in order to find patterns in human and other activity. The use of big data will aid the process of automation and machine learning.[5] Furthermore, a process called data mining, where vast amounts of information is collected from many different sources, can be used to find patterns and relationships about a garden-variety of subjects, ranging from specific human behavior to a company's business strategy.[6] Data mining strives to find a correlation between many variables that may seem invisible to the human eye. Thus, this method can provide a unique insight into specific fields of research. In order to sort the data various techniques are used, such as classifying or clustering all the information into different datasets. Essentially, data mining pulls together data based on the information it mines from various data sources. The detection of behavioral patterns, through the use of big data and data mining, will contribute to the implementation of AI in everyday activities. Ideally, this will lead to improvements in decision processes, business models, and customer experiences.[7]

There are various different types of algorithms that can be described based on their computing processes: randomness, recursive or iterative logic, backtracking, etc. The computing method is basically the technique that each algorithm uses to solve a problem. Problems can be solved by using any of these techniques, either alone or together.[8]

THE OUTPUT OF AN ALGORITHM DEPENDS ON THE INPUT OF DATA

1.2 Input and Output

The output of an algorithm is very much dependent upon and determined by the input of data. As the old saying goes, when garbage comes in, garbage comes out (Garbage In=Garbage Out is the GIGO principle in computer science, mostly relevant to machine learning as defined below). We may expect that when the data input is of high quality, the output is also of high quality—in other words "Diamonds In=Diamonds Out". Indeed, scientists talk about clean, (as opposed to dirty) data, biased and unbiased data, and so forth.

From a policy perspective, not all data that can be used as algorithmic input is treated the same. For example, sensitive personal data enjoy special protection under the General Data Protection Regulation in Europe. These include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; data concerning a person's sex life or sexual orientation.[9] Furthermore, certain uses of data might be, again from a policy perspective, treated differently. For example, regulation allows for the regulated use of sensitive data, such as health data, for scientific or research purposes. The same does not always apply to commercial uses of data. This guide further includes separate sections on data protection, security and privacy.

THE PRINCIPLE IS SIMPLE:
GARBAGE IN GARBAGE OUT
OR,
MORE IMPORTANTLY:
DIAMONDS IN DIAMONDS OUT

1.3 Artificial Intelligence (AI)

AI, as opposed to natural or human intelligence, refers to machine "intelligence." Of course, machines are not intelligent in the way humans are, but they can demonstrate human-like cognitive functions when "fed" with the appropriate data and technologically "trained" to do so. Again, algorithms are crucial here as they are the fuel that enables machines to "learn how to learn".[10] A contemporary definition of AI is attributed to computer scientist John McCarthy, who defined AI as "the science and engineering of making intelligent machines."[11]

We should note the difference between weak (narrow) and strong (general) AI. Weak AI is used to describe AI systems with narrow or limited capacities to perform tasks that they are programmed for, as for example to recognize images or speech.[12] The threshold for strong AI is much higher, and arguably not fully reached yet, and includes the ability to generalize knowledge, make future predictions and plans based on knowledge and experiences, and adapt to environmental changes.[13] Strong (or general) AI systems should be ultimately capable of independent thinking. One of the biggest challenges to achieving strong AI was explained by John McCarthy in his 1971 Turing award lecture as follows: "In my opinion, getting a language for expressing general common-sense knowledge for inclusion in a general database is the key problem of generality of AI."[14]

Alan Turing has famously developed the "Turing Test" which is meant to measure the level of machine intelligence with a model he called "Imitation Game" whereby a machine would pass the test if it were able to interact with a human, understand the context of the conversation, and fool the human into believing that they interact with another human. [15] If we wonder whether machines can think then this test can, according to Turing, provide a relevant answer. The passing of the test was sufficient for him to believe that machines are capable of thinking and perhaps learning.[16]

Machines are apparently doing a fantastic job at learning how to perform complicated tasks, as the capabilities of AI are constantly increasing. We are already living in an era when concepts traditionally associated with humans, such as ethics, will have to be adapted to the new reality of intelligent machines.[17] In the most dystopian of scenarios, AI may call into question not only humans' intellectual superiority but also our essence and role in life.[18] Indeed, with the incredible capability of AI, there is little doubt that these new intelligent machines might surpass us in many ways. It is, therefore, crucial to ensure that AI develops in a way that aligns with human ethics. In other words, the methods and processes of machine learning (see below) should be subject to human ethical values.[19] Given that AI systems have the ability to learn independently, the key is to program machines with the

right instructions the first time around, so that we can trust that they will continue to learn responsibly (or "ethically") on their own.[20]

1.4 Machine learning

Machine learning, a subset of AI, is the scientific study of algorithms that machines use to perform specific tasks. Machine learning algorithms build models based on data. When the algorithms need training, those are "training data." The machine then "studies" this data, meaning that the machine undergoes a certain training itself, and "learns" how to make decisions and/or predictions. What's more, machine learning often uses datasets collected usually from data mining processes to learn patterns and predict outcomes. Unlike data mining, however, algorithms continuously improve their ability to recognize these patterns as they learn from experience. The machine automatically digests the parameters collected of data and uses this information to inform actions to be taken by artificially intelligent systems. This process repeats itself in order to achieve more accurate results.

Machine learning is a central element of AI, as it seeks to create algorithms and devices that recreate the human being's cognitive functions, turning unintelligent or "brainless" machines into "smart" devices able to interact with humans.[21] Eventually, through machine learning, machines might be able to perfectly mimic human interactions, at which point we will have no choice but to accept that humans are intellectually expendable.[22] As mentioned above, strong AI systems should be able to pass the aforementioned Turing proving that they are capable of independent thinking.[23]

1.5 Predictive analytics

Predictive analytics or predictive data mining is a type of "intuition" that identifies meaningful patterns in data. By gathering the patterns and analyzing them together with other relevant data, it creates informed predictions. The relevant information can be gathered from government and other public authorities and/or from businesses and private individuals. For example, tax authorities receive and gather information from the taxpayers—including demographic information, income, and more—that when combined may help to predict who will and who will not pay their taxes in the future.[24] In the marketplace, different types of shops—grocery stores, online shops, retail shops, and many others—may gather consumer information, habits, and behaviors. This data has become a powerful tool for marketing and has helped to create a number of prosperous businesses, mostly in the advertising and data brokerage spheres.[25] Algorithms have promised the improvement of various other fields, including legal services with the development of legal technology (and judicial analytics in particular) and even the administration of justice. More clear examples of valuable uses of predictive analytics include their use in science to predict and preempt environmental and other catastrophes, or in preventive medicine.

2. ALGORITHMS AND AI: WHAT LIES AHEAD

The role of artificial intelligence has increased exponentially over the last few years, to the point that it has been referred to as "the new electricity", drawing parallels with the Second Industrial Revolution's impact on society.[26] It is debatable whether "the new electricity" or is indeed AI and not the Internet, which can perhaps be marked as *the* breakthrough of our century. Nevertheless, nowadays, while we are technically experiencing the Fourth Industrial Revolution, algorithms, artificial intelligence, but also human-machine interfaces, virtual and augmented reality, as well as the Internet of Things and blockchain are all developments that push us further into the future.

What other challenges may lie ahead in the future?

2.1 Surveillance and other ethical and legal dilemmas

Algorithms can "amplify large-scale surveillance through techniques that analyze video, audio, images, and social media content across entire populations and identify and target individuals and groups".[27] For example, in the case of facial recognition, once a specific person is recognized, the algorithm links the face to other personal records and identifiable data, such as a photograph or a criminal record. Other examples include AI Research and Development (R&D) within big corporate companies such as Microsoft, Google, and Amazon which are all developing AI systems in specific sectors as for example healthcare, transportation, manufacturing, and even retail. Major technology companies have also acknowledged that AI technology could create ethical and legal challenges for their respective businesses. In its official Securities and Exchange Commission (SEC) Report, Microsoft recognized that "AI algorithms may be flawed".[28] Datasets may be insufficient or contain biased information. Finally, it has been observed that inappropriate or controversial data practices could "impair the acceptance of AI solutions, undermine decisions, and ultimately cause harm and legal liabilities - for example in the forms of brand or reputational harm".[29]

As such, these challenges may also increase abuse of social and civil rights. In the absence of targeted laws and regulations, "artificial intelligence technologies like facial recognition systems fundamentally change the balance of power between the people and the government."[30] Also governments need to be aware of potential scenarios whereby AI systems may cause real harm due to their biases, inaccuracy, and the current lack of transparency and accountability. Furthermore, we might need to also consider extreme scenarios whereby industries creating these systems are willing to "conduct early releases of experimental tools on human populations."[31]

Advanced AI creates legal and ethical issues that require the collaboration of society as a whole to be solved, taking various perspectives into account. In other words, specialists in every field—

science, humanities, economics, law, art, etc.—are needed to collaborate to correct the imbalance that is often created through the use of AI.[32]

2.2 Exceeding human capabilities

AI is also capable of producing results and answers that go far beyond human capabilities. By using incredible amounts of human data, AI is able to understand, analyze, and predict human behavior. For instance, "affect recognition" is a subcategory of traditional facial recognition which "aims to interpret faces to automatically detect inner emotional states or even hidden intentions."[33] Essentially, AI can tell what a citizen, a consumer, or a criminal is really feeling—it produces "a direct window to the soul."[34]

2.3 Human enhancement

While algorithms are integrated into more aspects of our lives, scientific research and its applications spread into more domains such as healthcare and also neuroscience. Such developments bring both opportunities and challenges from an ethical standpoint. For example, should there be an algorithmic for human or even love enhancement?[35]

At a time when many domains in life are being taken over by metrics and medical enhancement there are plausible fears over a future of artificial human enhancement. What would that mean in practical terms? Let us explore the metaphor further. By taking medical enhancements, people are dealing with medical issues surrounding the body and the mind. Medical and human enhancement are not identical terms. In theory the first leads to the second. But could any kind of medical or human enhancement be permissible? Again, ethical considerations arise together with practical and legal considerations for malpractice frameworks and accountability. Yet, scientific research is leading to technological and specifically algorithmic solutions, including cyborgs, artificial agents, and androids, that might provide the next breakthroughs in human enhancement.[36] Whether this is realistic or not, only future will tell. Ultimately, society will decide whether this is a desirable future or one to be worried about.

2.4 Personal identity in the algorithmic society

Finally, we must reflect upon the vast amount of time we are spending using technology might be affecting not only how we relate to others but also how we relate to ourselves. It is necessary to identify and reflect on these changes in order to not lose our human capacity for self-reflection, which would make it difficult for us to retain a stable sense of self. Let us start then with a thought-provoking question: Is it possible to retain our human identity in an algorithmic society?

Algorithms play an important role in this redefinition of human identity. Algorithms can create a frictionless reality very different from what humans are built for: a reality where time, space, friction, and gravity are all present. It might be wise to assess the consequences of such developments and rethink the creation of superhuman, seamless realities.[37] This does not mean that we need to strive for a society of luddites, but a society of algo-aware citizens who are able to embrace the potential of technological advancements while avoiding the risks.[38]

Scholars have noted how people might be losing a clear sense of identity primarily because they have been drawn by the fantasies that technology incites.[39] For example, we are under the impression that technology allows us to customize human relations. We might prefer emailing, texting, and posting online to engaging in real conversation because technology allows us to edit and delete what we say, ultimately controlling how we want to present ourselves to others. While we may prefer these platforms because they make us feel less vulnerable, such modes of communication can never provide us with empathy or understanding. Human interaction, conversation and reflection are still key for experiencing human emotions and getting to know others. Essentially, they are vital to the development of human identity within society.

Furthermore, and perhaps most importantly, technology has created a world in which we are supposedly never be bored and never alone. However, being bored and being alone, far from being problems from which we must escape, are actually vital conditions for the development of an identity.[40] Thus, it is critical to understand to what extent technology introduces false ideas of identity, community and togetherness. Finally, it is important to point out that technology is not only affecting the development of human identity, but is in fact *redefining* it. Online, on social media platforms, and in other virtual environments, we are provided with the freedom to remain anonymous and engage in different relationships and communities that we would never be part of in real life.[41] As a result, we can take on new identities and even more than one at a time. These parallel identities have allowed people to perceive identity as multilayered, introducing distance between person and *persona* (between the body and who we think we are).[42] Preserving both identity and privacy proves to be extremely difficult in the digital era. Does our digital identity match our real and physical one? Or is it others' interpretation of our personality?[43]

III. ADVANTAGES AND OPPORTUNITIES WITHIN THE ALGORITHMIC SOCIETY

1. USEFUL APPLICATIONS

Algorithms power both simple and complex technological applications that we use in our everyday lives, from the search engines and social networks to online purchases, to smart objects, and automation and robotics.

1.1 Algorithms in our everyday lives

1.1.1 Search engines

Today's web search engines of today are descendants of information retrieval (IR) systems. These systems use different methods to find relevant documents for given queries. One of the better-known IR methods is the Boolean search method which was developed over thirty years ago.[44] The Boolean search method allows for the use of search keywords and elements of our syntax— "and", "or", "not"— as "operators" or "modifiers".[45]

While the Boolean method did a good job of retrieving documents for librarians it was too complex for other users. The ranking algorithm was developed to help fix these flaws.[46] It has allowed amateur users to find what they desire in a large pool of documents. The user inputs a word, sentence, or a phrase and the algorithm retrieves documents that are listed in the order of their relevance. Moreover, the words do not need to be spelled correctly. Ranking algorithms are used today by many web search engines, including Google, the pioneer of online search.[47] To this day, the Google algorithm, one of the most profitable algorithms in the world, remains a secret. Meanwhile, Google continues to be the single most wide-spread search tool around the world.

1.1.2 Social networks

One of the main functions of social networks is the formation of online communities by way of community detection. These online communities are created by taking a variety of different factors such as common interests into account.[48] How are algorithms involved? These factors are processed by community detection algorithms.

Community detection (CD) algorithms can be divided into two main groups regarding how they view relationships between communities in a network: disjoint and overlapping CD algorithms. Most CD algorithms are disjoint and assume that communities within a network do not overlap. However, there are some that are overlapping and recognize that an individual can appear in more than one community. Finally, there are algorithms that detect hierarchies between and within communities,

such as research communities divided into research groups. Due to the wide variety of CD algorithms that exist, the operators of these social networks must decide which algorithms best suit their network.[49]

1.1.3 Online marketplace

As commerce has moved online, companies have started to use algorithms to experiment with different pricing strategies in the hope of maximizing revenue. Among the companies that rely on algorithms are two major online businesses, Uber and Amazon. The on-demand driving service Uber uses surge pricing algorithms to vary prices dynamically in order to balance supply with demand. Amazon Marketplace uses two types of algorithms: the Buy Box Algorithm and the dynamic pricing strategy. The Buy Box algorithm determines which seller's offer price will be shown to customers, increasing the likelihood that that seller's product will be sold. The Buy Box is hence a type of matching service that balances customers' interests (price and quality), as well as the interests of sellers interest and Amazon (both of which are revenue). Finally, the dynamic pricing algorithm enables sellers on Amazon to track their competitors' prices and vary their prices in response. In a way, this allows sellers to compete for the Buy Box. [50]

1.1.4 An app for everything

The variety of algorithms used in mobile apps have greatly facilitated their development and maintenance. As a result, there is an app for everything nowadays. Machine learning algorithms play a particularly important role in mobile apps. As seen also above, machine learning consists of designing efficient and accurate prediction algorithms by analyzing electronic data that has been collected.[51] The main advantage of machine learning tools is that they have reduced the burden for programmers, who no longer have to anticipate every possible eventuality that may arise from the use of an app. Instead the algorithms can recognize trends and needs and develop appropriate coding in response. Machine learning algorithms can help address bugs and other flaws in a fast and efficient manner.[52]

1.1.5 Sensor society

As people search for information on search engines, talk on the phone, like a post on social media, or send an email, the sensors of their technological devices are costantly gathering and processing information.[53] Thus, every movement of every individual contributes to the continuously developing sensor society. Some sensors might be coordinated with others and can therefore share information with one another—in a way they can "speak." Tech companies exploit the sensor society to create customized products for consumers.[54] Sensor technology is present in many devices that people use in their daily lives, consciously or not. For instance, sensors exist in smartphones, cameras, drones, and so on. Cars are even installed with numerous sensors through which the car can detect when its driver is fatigued or distracted.

Sensor technology has significantly changed forms of information collection as well as our understanding of information processing. Most sensors, such as those providing facial recognition, depend on the user's physical proximity.[55] There are also sensors that collect other data "like the movement of the user from light to dark."[56] It can generally be said that the understanding of a sensor society "goes hand-in-hand with the rise of networked, interactive, digital devices, and directs attention towards the "datalinks" that make possible emerging and transformative forms of data collection, processing, and the use."[57] Companies or any other entities (such as governments) then use the data collected by sensors in marketing or for other purposes. For example, companies "reportedly use smart cameras to target marketing messages tailored to the customer's gender, age and mood, measured by facial recognition."[58]

1.2 Useful applications in the household

1.2.1 Smart objects and the Internet of Things

Smart objects have entered the household in many ways: from smart TVs and smart fridges to smart cleaning devices. Another crucial development is the widespread use of wearable technologies, such as arm watches that measure your heartbeat, that track the distance you have walked, and record the calories you have consumed. Smart objects entering the household, or even indeed attached to our bodies, are the product of a disruptive technology: the Internet of Things. This technology relies on user needs and algorithms to generate data.

What does the term Internet of Things refer to? The Internet of Things is a vision of the world in which physical objects that humans interact are embedded with internet connectivity, intelligence, and processing power (thanks to sensors). They will therefore be able to connect with each other via Internet Protocol networks.[59] As a result, objects will become more useful and able to adapt to the developing needs of people. They are inter-moderating and can also be used remotely or directly through the web. The definition of the Internet of Things is constantly evolving due to the leaps and bounds of technology and its platforms.[60] We commonly associate the Internet of Things with "smart technologies", all of which can be accessed through smart devices and AI-powered personal assistants such as Amazon's Alexa and Google Home.

When the Internet burst onto the scene it was astonishing how it was able to connect people in an unprecedented way, through networks all over the world. With the Internet of Things this revolution has been taken to another level—people communicate not only through their screens and posts but also in their physical environment regardless of their location. Access to information has been truly revolutionized. Nowadays, information can be accessed anytime, anywhere, and by almost any device. Thus, communication has also been revolutionized—it is now quicker, more efficient, and globalized.

This ease of communication can be linked to many other important efficiency gains in objects all around us. As communication improves, data packaging allows more efficient work to be done and reduces waste. Finally, developments in the Internet of Things arena go hand-in-hand with developments in automation.

1.2.2 Robots and robocalls

Robots have transformed many aspects of life like, including finance, hospitality, medicine, marketing, communications, and finance. This, among other changes, seems to be a defining part of the Fourth Industrial Revolution. A preliminary question to ask is: What exactly is a robot? According to Neil Richardson and William Smart, a robot is "a constructed system that displays both physical and mental agency, but is not alive in the biological sense."[61]

As robots become part of the consumer market, they are simply seen as a products. They have more potential, however, than most products we have ever seen. For example, there is potential for them to have functionalities or tools that allow them to search and select products on behalf of their owners. This raises a dilemma—is it the consumer or the robot who makes the decision to purchase? For example, Amazon's Echo can order pizza, get an Uber, play music, etc. Moreover, while the regulatory future of self-driving cars is unclear, it is speculated that they may also act as consumers. They could monitor when the car needs maintenance, check the owner's schedule and book an appointment at the nearest authorized car maintenance center, decide on the price and service required, and pay for the service. This would change the way products are marketed and the laws that come with the purchase.[62]

Finally, another way in which robots have already entered consumer's lives is through the telephone. The so-called "robocalls" are pre-recorded computerized calls, essentially created by a robot. They are an increasingly common occurrence. According to the Federal Communications Commission in the US, there has been a 57% increase in the amount of robocalls the average person receives, meaning that nearly half of the calls people receive are spam.[63] Most people have received robocalls from big businesses (your telephone/internet company, your bank, and many others), but due to the cost efficiency of robocalls, small businesses use them as well. However, multiple jurisdictions are starting to regulate robocalls. For instance, the UK's Information Commissioner's Office (ICO) penalized Keurboom Communications with a fine of $517,000 after it made 100 million robocalls, which led to 1,000 complaints.[64]

Generally speaking, automation, robotics, and the increasingly foolproof smart objects in our households, are all developments that mean we can stay constantly connected. This is expected to have revolutionary effects on consumerism as it presents the second wave of invasion of marketing to

households (after the TV and radio). This allows companies to use collected information to automatically order replacement items for products (such as dishwasher liquid) and even order modifications and house improvement products. A notable example would be the IBM/Samsung washing machine which deploys "a smart contract to order and pay for detergent when required"[65] and detects when the washing machine needs maintenance or a repair.[66]

1.3 Useful applications in the workplace

1.3.1 The use of algorithms in the recruitment process

Algorithmic tools have an increasingly active power in the recruitment process, for example, t qualify the high quantities of applicants that employers must assess.

Algorithms facilitate the enormous collection of data on "worker's skills, knowledge, aptitudes, attitudes, etc."[67] And "even [allow] technology itself to replace human resources supervisors and managers, and to make decisions that have legal effects on the employees."[68] Moreover, they do this at a speed that is not humanly possible, therefore allowing for "monitoring to be carried out at a lower cost."[69] With this in mind, the role of algorithms in creating a more competent labor market is highly valuable. Finally, at the same time the use of algorithms by employers in their search for job applicants is also rising. These developments, however, make for only part of the entire picture. There are further algorithmic uses in the workplace that are challenging from the perspective of privacy and data protection, as well as the well-being of the workforce more generally.

1.3.2 Algorithmically mediated work: the rise of the gig-economy

The gig-economy started to emerge over a decade ago in the United States. It revolutionized the labor market as it offered a completely new hiring model known as gig-work.[70] The gig-economy centers around platforms which have a unique business model.[71]

In the gig-economy, traditional firms have been replaced by platforms that create digital work intermediation. Their role is twofold. Firstly, they act as matchmakers, pairing consumers with entrepreneurs. The matchmaking is done via algorithms—they consider a variety of factors such as previous work quality, availability and geographic location, in order to find the person best suited for the job. Secondly, these platforms provide a digital framework in which transactions can be made.[72]

Gig-economy platforms make their money by creating a surplus in the economy, reducing transaction costs, and by way of regulatory arbitrage. Surplus is created by removing search frictions (obstacles that impede matching supply to demand, such as geographic obstacles). Platforms remove these obstacles by providing superior matching opportunities via the use of algorithms and the internet. These platforms also provide an infrastructure in which these transactions can take place, thereby reducing transaction costs and making them faster and easier. Finally, regulatory arbitrage and other

speculative activities create shareholder value in these gig-economy platforms. Usually this is done by portraying employees as independent entrepreneurs.[73] The costs that these entrepreneurs generate for the firm are far less than those of employees, as the firm does not need to pay their insurance, pays fewer taxes, and is not responsible for their resources. For instance, Uber is not responsible for the cars used by drivers as these drivers' personal assets. Due to the smaller costs that these firms need to cover, they are able to generate more profit.[74]

While profitable for these platforms, presenting employees as self-employed can greatly undermine their labor rights. The European Union has taken many steps to ensure that these workers have fair working conditions and adequate legal and social protection. Firstly, they have clarified the conditions required for an employment contract in order for it to fall under the jurisdiction of EU labor laws. Although the existence of an employment relationship can only be assessed on a case-by-case basis, the EU has stated that the essential feature of an employment relationship is that "for a certain period of time a person performs services for and under the direction of another person in return for which he receives remuneration," [75] a feature that exists in most relationships between workers and gig-economy platforms.

The EU has also taken two important legislative measures in the context of the European Pillar on Social Rights. Firstly, it has developed an Access to Social Security initiative, which could lead to new EU directive ensuring "similar social protection rights for similar work regardless of employment status."[76] Secondly, the EU is revising the Written Statement Directive to ensure more protection for atypical forms of employment.[77] This document will contain some general labor standards for all workers, such as the right to reference hours, the right to request a new form of employment, and the right to a reasonable notice period in the case of dismissal.[78]

Despite these challenges, there are many advantages that the rise of the gig-economy platforms has brought about: they create work opportunities in weaker economies, protect against discrimination in hiring and in the working place (due to race, gender, physical conditions, health etc); they offer flexible (not fixed) working hours;[79] and also allow workers ("gigers") to work in other paid-jobs.[80] The gig-work that algorithms support in today's economy seems to provide more freedom to both the customer and the employee.[81]

1.4 Useful applications in the marketplace

1.4.1 Blockchain, cryptocurrencies, and the empowerment of small/medium-sized businesses and start-ups

Algorithms seem to have the potential to transform the business sector, in which distributed ledger technologies and specifically blockchain technology allow for the empowerment of small- and medium-sized businesses as well as start-ups. Notably, algorithms power technologies such as

blockchain which require a high level of encryption. Below, we will define what blockchain technology is, and how it is relevant to algorithms.

Using consensus algorithms, blockchain is a list of records maintained by a decentralized web of computers linked in a peer-to-peer network. Each blockchain exhibits unique characteristics, but there are some features common to a blockchain. For example, each blockchain keeps a record (ledger) and changes to this record can be made by a network of parties (either a limited group or anyone in the world). In order to strengthen the security of the information in this record, cryptographic algorithms are used, which allow the authentication of the information in the record, thus creating a "paper-trail." This "paper-trail" consists of a chain of data blocks (hence the name "blockchain"), which are joined in a decentralized and public manner. In turn, these are stored on a wide network of computers (nodes) to prevent the system from collapsing.[82] The nodes work collaboratively to store, share, and preserve the data, using a "consensus algorithm" to guarantee the integrity of each block.[83] Once published, nobody, not even the administrator, can modify the existing block— they can only add information.[84]

Depending on the platform architectures of the blockchain, we differentiate between public and private blockchains. Anyone can join as a server to the public, which is typical of cryptocurrencies. The private or licensed, in contrast, requires an invitation to join as a server to the network, for which one can use a certificate or a key.[85] In both the public and private blockchain, communications are distributed among equals (peer-to-peer) and there is a form of consensus to decide the specific blocks that can belong to the chain.[86]

Although uses are increasing, blockchain technologies are still primarily utilized for payments or to automatize "smart contracts." A smart contract allows two parties to draft certain aspects of a legal agreement. The smart contract in the blockchain will then implement these terms, which ensures that neither party can break the agreement and no third party is involved. Blockchain enjoys incredible momentum and is tightly linked to the various algorithmic typologies we have looked at here. Indeed, blockchain is commonly identified as one of the key disruptive technologies of our times together with AI, big data and the Internet of Things. Finally, according to the World Economic Forum, 10% of the world's GDP could be stored in blockchains by 2027.[87]

Finally, we should mention the proliferation of cryptocurrencies which also use decentralized control to introduce and sustain cryptographically strong digital currencies new mediums of exchange, as opposed to traditional methods (printing of national currencies and the central banking systems).[88]

2. COMMERCIAL AND CONSUMER CHOICE AND THE EXPANSION OF RIGHTS AND FREEDOMS

The examples given above demonstrate how algorithms have drastically changed many aspects of our lives. Most of these aspects are related to our lives as consumers and participants of a (digital) marketplace that is becoming increasingly global and borderless. With this kind of technological progress, our rights as consumers are necessarily expanding. At the very minimum, consumer choice and commercial availability has widened.

Besides the widespread use and, indeed, usefulness of algorithms, we can also recognize their contribution to expanding citizens' rights and freedoms, such as the right to work and to provide work, to participate in a free and healthy market and make informed choices as consumers, as well as the right to be informed in general. More importantly, it is a citizen's right to participate in all economic, social, and political dimensions of an ever-growing "digital civil society."[89]

IV. THE THREATS OF ALGORITHMS

1. ALGORITHMIC OPACITY: KEY POINTS

One of the biggest flaws of algorithms is that they can be biased. This becomes especially dangerous in cases of automated decision making, as biases can then result in discrimination. However, things become even more problematic when we do not even recognize that algorithms are being biased or erroneous and therefore cannot address these flaws. Indeed, most of us do not understand algorithmic systems due to a lack of transparency. Often, we cannot see how analytics, the basis of algorithmic decision making, is being conducted (how patterns in data are being discovered and interpreted) nor what data is being analyzed.[90]

Algorithmic opacity has several causes, including technical ones. For instance that, an algorithm may be too complex to be explained and made transparent. There are also important economic causes, such as cost, business practices (as, for example, trade secrets), as well as social causes, such as data privacy. Sometimes these causes are so difficult to address that even well-engineered computer systems can remain opaque.[91]

However, due to a variety of factors, transparency alone is not sufficient to tackle these flaws. Firstly, transparency does not always entail change. People aim to implement transparency in algorithmic systems in order to achieve accountability. However, if there is no system with which to implement the necessary changes, then transparency does not really help improve things.[92] Moreover, transparency can actually be harmful on occasion. For instance, the revelation of certain data can threaten privacy. Actors bound by transparency regulation can even purposefully make vast quantities of information visible to distract receivers from a piece or pieces of information they wish to conceal (so called resistant transparency).[93] In other words, there is a delicate balance to strike.

There are also the technical and temporal limitations of transparency. Due to the scale and speed of the creation of these systems, when malfunctions occur, it is often difficult even for the creators themselves to detect a problem (the technical limitation).[94] Additionally, depending on when the information is revealed, accountability varies. In order to understand how the system works, and be able to adequately hold the system accountable, one cannot only observe current information, but they must look at how components have interacted previously and how their interaction has changed over time. However, this is difficult to achieve if there was no ongoing surveillance of the system.[95]

Finally, transparency is not only about revealing and concealing data. It is achieved through the constant configuration and deployment of platforms, algorithms, and machine learning protocols. It is therefore an ongoing process. An algorithmic system does not simply consist of codes and data but of an *assemblage* of human and non-human actors. Hence algorithmic systems need to be

approached as assemblages. Their components cannot be addressed separately. In other words, in order to discipline and regulate algorithmic systems, it is not enough to be able to "see into" the system; one must understand how the entire system works.[96]

2. THE MANIFESTATIONS OF ALGORITHMIC RISK

Besides algorithmic opacity and the risks it entails, there are many other manifestations of algorithmic risks that we need to be aware of. The effects on equity, privacy, security, our physical integrity, and on competition are all worth mentioning. There are also specific threats related to automation and to extreme levels of algorithmic control (algocracy).

2.1 Equity - The inherent problem of algorithmic bias

There are various examples that demonstrate AI biases, which is the (re)generation of *social* bias via AI systems.[97] An example from the labor sector is the fact that certain online advertising patterns end up suggesting higher-paying jobs to men than to women. In addition, facial recognition systems have been proven to work inaccurately for people of color. The famous Google Arts scandal at the beginning of 2018 is highly illustrative of this issue; people of color were "whitewashed" out of an algorithmic system that matched contemporary human faces with faces in famous art paintings.[98] This was a reflection of (i.) biased data—faces portrayed in the art displayed in the most prominent museums are predominantly Caucasian—and (ii) a failure of the technical (programming) teams that developed the application to identify the bias in the input, or at least the output. In another case, as part of an employee selection process, Google's AdSense algorithm assigned lower scores to African-American-associated surnames "like DeShawn" and "[un]like Jill".[99] Indeed, the general fear is that AI replicates and amplifies deeply embedded inequalities in our society. More constructively, there is now a rising number of voices that focus on eliminating AI bias and exploring methods to achieve computational fairness.

Large technology companies such as Google, Amazon, Facebook, Apple, and Microsoft (also known as GAFAM), and China's Baidu, AliBaba and Tencent (known as BAT), are all continuously involved in AI development. The widespread use of AI in such companies has brought about not only a general discussion of the power and promise that comes with the development of AI, but also a very targeted discussion of the bias that AI may generate, and how to deal with this issue at both the industry and societal levels. For example, diversity algorithms[100] are discussed as a potential solution for dealing with the issue at the industrial level.

However, this recent focus on bias arguably implies certain challenges. Addressing bias as a computational problem reduces the power of its root cause, which stems from society. AI, data used to train algorithms, and the embedded societal power-structures are all interwoven. As this is not only a

logical problem, but also a social and emotional one, it is not enough to approach it strictly from a logical perspective. Additionally, the lure of AI bias may distract from other issues.[101]

In conclusion, it is arguable that the proliferating AI bias debate distracts our communities from the bigger picture: long-term biases embedded in society and in human thinking that, firstly, cannot be solely attributed to algorithms and, secondly, cannot be solely addressed computationally. The existence of algorithmically generated biases and the resulting AI biases cannot be understood as detached from reality. Needless to say, the existence of algorithmic and AI biases does not suggest that we should not be using algorithms or create AI systems. Both algorithms and AI systems are simply an unavoidable but also highly desirable result of technological evolution. Finally, it is worth considering how technology can be improved in more efficient and perhaps more drastic ways in comparison to the ways in which human predispositions change and human and societal "behavior" improves. In the end, it might prove easier to face the challenge of algorithmically generated biases than it is to face complicated, multifaceted, and deeply embedded human and social biases.

2.2 Privacy

A crucial challenge is data privacy and security. On one hand, as data is stored on many devices, there is a constant risk that it may be leaked or hacked. Moreover, the internet has rapidly become the best way for advertisers to market their products to consumers via unavoidable pop-up ads or background wallpaper adverts. With the advent of big data, companies are now able to research and tailor advertisements to each individual person through online searches.

A vast amount of the world's data has been generated only in the past decades and this speed is constantly increasing as technology advances. This makes it very difficult for people to track which data they share and with whom they share it. It is just algorithms (thus machines) who "read" the data and detect patterns in people's behaviors—the search engine collects metadata that helps predict what people might do next or what they may be might be interested in and so on. That said, predictive analytics as a tool has greatly developed over the years. Machines interpreting changes in online users' communication or search behavior patterns can now detect very personal information, including human condition and symptoms such as depression.[102]

What creates concern for consumers nowadays is not only the data collection, but also any predictive analysis based on that data. For instance, in media there are uses of electroencephalography to determine when viewers' brains have detected an item of interest before the viewers themselves have consciously registered it.[103]

Finally, we must pose the question: Is the constant gathering of consumer information surveillance? Surveillance is defined as "purposeful, routine, systematic, and focused attention paid to

personal details, for the sake of control, entitlement, management, influence, or protection."[104] In the digital era we face what is called "dataveillance" and has been defined in simple terms as " the systematic monitoring of people or groups, by means of personal data systems, in order to regulate or govern their behavior".[105] Although dataveillance is a form of mass surveillance, it can also be personal, for example, in the case of web browser cookies.

In sum, one might say that the very nature of our digital era challenges privacy: algorithms can deep search the deep web for data available online. Finally, with regard to other disruptive technologies—such as the Internet of Things and robotics, which are intrinsically linked to AI—there are heightened privacy concerns due to the mass amount of personal and sensitive data that can be gathered via camera (facial recognition), voice (voice recognition), and other identifiers (footprints etc.).

2.3 Security

Security threats manifest in many ways, from the leaking of sensitive or inaccurate information, to hacking, which has real physical effects upon people.[106] Furthermore, hackers have proved able to invade and breach firewalls that protect users and are therefore able to steal information from our digital devices—from smartphones to wearable smart technology. For example, it was estimated that there will be 780 million pieces of wearable technology by the end of 2019, meaning that roughly 780 million people could also be at risk of data security threats to technologies that are on their bodies. This has given governments and legislative bodies incentive to develop laws and rights with regards to wearable objects.[107]

Security risks include risks from malicious cyberattacks and also from system vulnerabilities. Cybercrimes include offences against the confidentiality, integrity and availability of computer data and systems, illegal interception, data interference, system interference and other misuse of devices .[108] Offences can be computer-related, such as forgery and fraud, but also content-related—from copyright infringment to child pornography.[109] There is also another layer of the web, the so-called "dark web", usually facilitating such illegal activities.[110] As technology advances, in some of these cases security risks can stem from malpractice and malicious use of algorithms and also be linked with abilities inherent in AI. The impacts are broad: a security breach can jeopardize privacy, dignity, safety and physical integrity of individuals. All of this should inspire a preventive response from cybersecurity regulation. Indeed, under most jurisdictions, the breaches mentioned above are also criminal activities. States try to combat cybercrime in both the domestic and international level with cooperation of various competent authorities.[111] Finally, security breaches pose a threat to democracies, economic activity, and innovation. Indeed, one must not underestimate the use of algorithmic tools by malicious actors and/or totalitarian political regimes with various motives including to pose threats to elections and

democratic dialogue on and offline. There are various such algorithmic tools, as for example, the spreading of fake news and the more pervasive deepfake technologies.[112]

Overall, discussions of data security are proliferating and also becoming more critical as more and more objects get connected to the internet—from cars and drones to smart glasses and smart watches. Arguably both the data privacy and security debates are heightened as we are moving towards an era trending vast and seamless digital infrastructure and the proliferation of algorithmic uses; the era of the Internet of Things (cars, drones etc.) and also the Internet of Bodies (smart wearables but also implants).

2.4 Threats related to automation

Automation and the entry of robotics into our everyday lives has likewise raised a number of challenges. Bots and robots are capable of violating consumer protection regulations in the same way as humans are. They can be deceptive and also have biases, associated with algorithmic bias, as discussed above. This raises serious concerns about consumer vulnerability to possible malpractices. It is a legitimate fear, for example, that consumers could be falsely comforted by the seemingly human characteristics (compassion, empathy, etc.) of some robots and thus, disclose information that they assume is confidential.[113]

Another example is the proliferation of social media accounts associated with bots whose online activity can also deceive consumers. For instance, bots can manipulate the ratings of a product or service. Such practices, when targeted to manipulate consumers, are considered abusive, as they interfere with the consumer's ability to understand the conditions or quality of a product or a service.[114] Some major corporations have already been accused of unfair trade practices for downloading spyware on computers. Indeed, according to the US Federal Trade Commission, spyware and spybots lie under the category of deceptive and unfair trade practices.[115]

2.5 Physical integrity

There are also real threats to physical integrity. Mistakes and malfunctions are always possible with technologies and are not easily dealt with by people with low or average technical capabilities. For example, as the Internet of Things creates interconnected systems, one mistake can cause a large malfunction affecting entire systems. More importantly, people's health or even lives could be put at risk if heartbeat or insulin-providing device having been hacked. Finally, with the rise of smart devices, we might also see certain professions affected, integrity affecting our physical integrity. For example, automation reduces the need for human physical labor. This raises another important challenge: technological dependency and algocracy.

There are novel discussions about ways to (re-)integrate human decision-making in mechanical decision-making processes—introducing the "human in the loop." As Ge Wang, Stanford University computer scientist, puts it:

> Essentially, the human-in-the-loop approach reframes an automation problem as a Human-Computer Interaction (HCI) design problem. In turn, we've broadened the question of "how do we build a smarter system?" to "how do we incorporate useful, meaningful human interaction into the system?"[116]

2.6 Algocracy

The inevitable growth in the use of algorithms carries a crucial risk for the users, as they are slowly becoming passive spectators by giving up control. They are therefore becoming less entitled to feeling guilty or proud for society's shortcomings or accomplishments.[117] Giving up our tasks and delegating them to machines might end up affecting the way in which we express our desires and even desires themselves. This could result in detachment, alienation, and dependence.[118] A simple example is navigation skills—the more we depend on algorithmic navigation, in and outside of our cars, the worse our sense of direction and map-reading skills become. As a result, we become more dependent on navigation tools. In addition, there are concerns about the lack of transparency in the ways that new technologies may nudge us to affect our decisions, mostly as consumers, and ultimately our individual autonomy. For example, Facebook has experimented by intentionally controlling the news posts on users' feeds in order to analyze how they influence the emotions of users.[119]

2.7 Competition

Algorithmic management, using platform-based rating and reputation systems, monitors the users and the providers of the platforms in ways that might affect competition. The system ultimately awards winners based on network effects and can also assist monopolies.

Data is becoming a commodity which can be traded by some businesses in exchange for money. The concentration of critical masses of data in the hands of certain companies results in bottlenecks. For example, telecom companies are organizing aggregate data in packages and selling them anonymously to other businesses, allegedly in the aggregate level, which then these data packages for marketing purposes. The reason companies purchase these data packages is to be able to target specific audiences they believe would be interested in buying their products. Thus, the consumer might think that the advertisements are competitive when in reality, they are targeted.

Finally, the effective oversight over companies that hold massive data monopolies is currently a central concern of both the EU competition and the US antitrust authorities.[120] In spite of the many efforts to regulate global data markets, it is difficult to identify common standards. Standards might be

structuring around different data fields (for example, different for health data or other sectors of sensitive data). We will conclude this brief mention in markets and market regulation with an emphasis on the notion of data sovereignty.[121] Indeed, while novel data markets and markets for data brokers are constantly emerging, some have started even started discussing the possibility of monetizing consumer data and creating new markets.[122]

V. TOWARDS USER'S EMPOWERMENT. THE POLICY, ETHICAL AND LEGAL REACTION TO EXCESSES FROM THE ALGORITHM

1. OVERVIEW OF POLITICAL, SOCIAL, AND LEGAL INITIATIVES

1.1 The Declarations on "Good AI"

The growing importance of AI has led multiple international organizations, namely the European Union (EU), the United Nations (UN) and the Organization for Economic Co-operation and Development (OECD) to make declarations on its ethics.

The European Commission has led two key initiatives. The High-Level Expert Group published the "Ethics Guidelines for Trustworthy Artificial Intelligence"[123] in April 2019, focusing on the characteristics that "trustworthy" AI should have. The Guidelines establish seven requirements all AI systems need to have to be deemed trustworthy: data governance, transparency, non-discrimination, sustainability, accountability, robustness, and human empowerment. In summary, trustworthy AI must be robust, ethical, and lawful.[124] The EU's second initiative is the Commission's communication entitled "Artificial Intelligence for Europe,"[125] which establishes Europe's approach to AI and its initiatives for the future, so that it can "become a leader in the AI revolution in its own way and based on its own values."[126]

Similarly to the EU, the OECD's "Council Recommendation on Artificial Intelligence"[127] focuses on the importance of AI systems being transparent, safe, sustainable, respectful of the rule of law, and allowing for a system of accountability. The OECD's principles on AI were the foundation of the G20's AI principles which can be found in its Ministerial Statement on Trade and Digital Economy.[128]

The UN has also been working on generating AI strategies. Since 2017, their International Telecommunication Union (ITU) organizes a yearly "AI for Good Global Summit." This summit focuses on finding ways to take advantage of AI to help achieve the Sustainable Development Goals (SDGs), particularly with regards to mitigating climate change, fighting famine and hunger, improving response to disease outbreaks, and monitoring energy usage. To this end, the ITU has published the "United Nations Activities on Artificial Intelligence."[129]

Finally, one of the most relevant social initiatives to define AI principles are the Asilomar principles developed with the 2017 Asilomar conference on beneficial AI.[130] These principles which primarily focus on research, established five enumerated goals:

1) The goal of AI research should be to create not undirected intelligence, but beneficial intelligence;

2) Investments in AI should be accompanied by funding for research on ensuring its beneficial use […];

3) There should be constructive and healthy exchange between AI researchers and policy-makers;

4) A culture of cooperation, trust, and transparency should be fostered among researchers and developers of AI;

5) Teams developing AI systems should actively cooperate to avoid corner-cutting on safety standards.[131]

These five principles are followed by 18 more focusing on ethics and values including safety, transparency, responsibility, human dignity, personal privacy, human control, and recursive self-improvement.

1.2 The algorithm behind data protection laws

Alongside the above political and social initiatives, so far, legislative action relevant to the proliferation of the use of algorithms mostly taken place in the sphere of data protection. The EU leads the way with the introduction of the General Data Protection Regulation (GDPR).[132]

The GDPR entered into force in April of 2018 replacing the EU's 1995 Data Protection Directive. It is said to be groundbreaking for it has established more robust—and perhaps far stricter compared to other jurisdictions—rules for the collection, storage, and use of personal information. [133] Moreover, it has addressed important gaps that existed in the EU's approach to data protection and has given EU citizens more power to lodge complaints regarding the violation of their data protection rights.

Firstly, the GDPR is "stricter" because as a regulation, unlike a directive, it ensures the enforcement of data protection laws. While a directive only sets out the rules to be transferred into national law by the member states as they deem fit, a regulation is directly binding. It requires no enabling legislation to take effect but rather *is* the law of the EU member states from the moment it enters into force.[134] Secondly, the GDPR is far harsher in punishing data protection violations than the Data Protection Directive of 1995. The fines (at least a range of them) are no longer established on a country by country basis, but rather apply EU wide.[135] The maximum fine is 20 million euros or four percent of global revenue (Article 83, Paragraph 5), whichever is *greater.*[136]

Another achievement of the GDPR is that it has addressed the lack of regulation for foreign companies processing personal information of EU citizens. The GDPR establishes that all companies processing the data of EU citizens, regardless of where the data is being processed, are subject to its jurisdiction.[137]

The GDPR includes new rights that give citizens more power to effectively control their personal information. The new right to data portability (Article 20) also allows citizens to obtain their personal data from an internet service provider in a machine-readable, common-use format (active portability), and even have it automatically transferred from one service provider to another of their choice (passive portability).[138]

In addition, the directive introduces two new critical rights specifically related to algorithms. Firstly, Article 21 outlines the right to object to automated individual decision-making, including profiling. Article 22 expresses the right to not be subject to a decision based solely on automated processing, including profiling, which may affect the individual legally on in other ways. According to Article 21 of the GDPR, data subjects have the right to object to the processing of personal data concerning them on grounds relating to their particular situation *at any time* (Article 21.1). In that case the data controller can no longer process their personal data unless they can demonstrate compelling legitimate reasons to do so. Furthermore, data subjects always have the right to object to the processing of their personal data for direct marketing purposes (Article 21.2). The directive also introduces new information duties whereby the data subjects must be specifically informed about the existence of automated decision-making, including profiling (Articles 13.2.f) and 14.2.g)).

Finally, a highly significant new right ought to be mentioned in this guide. Article 80 is the right of representation by a body, organization, or association which is to be added to the wide array of remedies already laid out in the Directive. This paves the way for privacy class actions similar to those possible in countries like the United States.

2. ALGORITHMIC REGULATION PROBLEMS

2.1 Regulations vs. innovation: the intellectual property implications

Another important sphere of legislative action when it comes to the use of algorithms is intellectual property (IP). It refers to intangible works created by human minds. Intellectual property rights—copyright, patents, trademarks, industrial designs—exist to protect the interests of creators over their original creations and to reward and incentivize further creativity and innovation. Copyright, for example, protects authors' rights over their intellectual or artistic work. These rights include moral rights (no one can steal credit from the author) and economic rights (no one can gain financial reward from the use of the work without the author's consent).[139]

Algorithms are also creations of the human mind and as such can be protected under intellectual property rights. Arguably, developers would not be motivated to invest their time, effort, and resources into creating algorithms if they were not sure that they would gain recognition and financial reward for the investment.

Certain manifestations of algorithms are easier to regulate than others. For instance, computer programs are easy to regulate. Many countries, including those in the EU, have already developed copyright laws for computer programs and the World Intellectual Property Organization (WIPO) has included computer programs in its Copyright Treaty of 1996.[140] However it is far more difficult to incorporate AI into intellectual property laws. How can artistic works or inventions generated from AI be protected? After all, copyright, patents, industrial design, and trademarks only protect creations of the *human mind*. Can AI be an author or an inventor in and of itself? Must a link be made between the final product and the data that was initially inputted? WIPO Director General Francis Gurry has stated that "the question is at what stage do we attribute value to the human origin of data? We don't yet have answers to that question."[141]

Furthermore, since data is crucial for the development of AI, there has been much discussion with regard to protecting access to data, as well as its ownership. While some advocate the free flow of data in order to enable faster growth of AI, others insist that data must be protected under IP laws in order to ensure that people are incentivized to invest in AI.[142]

Finally, another challenge with regulating AI under IP laws is the fast development of AI. Since AI is constantly evolving, it is very likely that the IP rights that might be applicable now will no longer be relevant in the future.[143]

Despite the fact that it is very difficult to incorporate AI into the existing IP framework, trust in the current IP system must be reaffirmed, irrespective of the fact that new layers may need to be added to IP law to comprehensively address AI, especially at an international level.[144]

2.2 Other regulatory conflicts: consumer protection, competition, and privacy

The implications for data protection, as discussed above, are even more serious and inevitably linked to our fundamental right to privacy. The right to privacy, or right to be left alone,[145] manifests in many ways: the right to control the collection of our data; the right to demand that our data is not being collected or that it is deleted from third-party databases; and the right to be forgotten (also protected under Article 17 of the GDPR under certain circumstances).[146] When we think of commercial practices for data collection, for example tracking and targeted advertising, one can see the obvious conflict. Market competition drives various actors towards more data collection and (re)usage. Perhaps one of the biggest challenges of our era is how to protect the individual amidst this phenomenon. This is particularly puzzling when we think of the numerous ways and instances in which we voluntarily hand out our data (commonly for free) in exchange for products and services that provide convenience. The most obvious example is our data footprints that are being collected on a daily basis from the various paid or free applications on our phones and other connected devices.

As well as data protection laws, consumer protection laws must also reflect the new needs of the data economy. The aforementioned possibilities for tracking consumer preferences particularly call for regulation to tackle the phenomenon of targeted and personalized pricing. Dynamic pricing, based on the number of personal visits to a webpage, while a customer is looking for airline tickets or hotels, for example, is highly problematic, especially when targeting traditionally vulnerable consumer groups.[147] It is the role of consumer protection laws, in conjunction with the aforementioned data protection guarantees, to address such opaque market practices.

Finally, competition regulation must keep the power of big tech monopolies in check. In the European context both the EU and the national competition authorities and courts apply competition law to ensure that powerful companies such as Amazon, Google, and Apple do not use algorithms to squash potential competitors.[148] Competition law is generally applicable when powerful companies abuse their authority or engage in illegal behaviors within the market, such as price fixing. Ensuring a healthy and competitive market is key both for the protection of consumers and for the protection of the market itself. A healthy market fosters the possibility for new market entrants and innovation that ultimately benefits again the consumer with low prices and high-quality products and services.

3. THE MOST COMMON ETHICAL AND LEGAL AI PRINCIPLES

3.1. Respect for human dignity, personal identity, and human rights

EU constitutions, together with so many others all over the world, enshrine the right to human dignity. For example, the notion of human dignity ("Würde des Menschen") is especially relevant for example in the 1949 German Constitution, which acted as a model for explicit protection of the right to dignity for many other constitutions around Europe. [149]

We have discussed the notion of algocracy and algorithmic control above. However, we should add that algorithmic control is also quite important also in light of the right to dignity, which is protected by various European constitutions. Yet, with the rise of algorithmic control, respect for such rights is slowly deteriorating. In other words, the greater the algorithmic control, the greater the risk to our right to dignity.

Algorithms, when not applied and used properly, have the potential to harm individual rights. This is the case when algorithmic systems harm vulnerable members of society, inadvertently worsening current social injustices, particularly with regards to sexist and racist biases.[150] Indeed, "algorithms learn from historical data and thus also learn from our past... unfairness and injustice in our world is reflected in the data fed into these algorithms."[151] Many terms have been used to discuss this phenomena, mainly the aforementioned notion of algorithmic bias, but also that of data violence. Although the term "data violence" may seem over-dramatic, it seeks to describe the harmful

consequences of flawed data gathering and algorithmic processes. For instance, the body scanners used at airports often identify transgender people and other vulnerable or minority groups as threats,[152] a phenomenon that is extremely challenging not only from a discrimination standpoint but also from an ethical perspective.

Together with dignity and other human rights, the need to protect personal identity is also extremely important. As mentioned in the introduction to this guide, technological advancements can affect not only how we relate with others, but also how we relate to ourselves. In order to retain our human identity in an algorithmic society, we must need to preserve human identity (and humanism) in the algorithmic context.[153]

Nevertheless, it is important to reflect on the fact that algorithmic control is not always negative, or rather, is not always incompatible with our right to dignity. For instance, in the medical field, AI is used to detect DNA mutations in tumors, predict heart attacks, diagnose and detect cancer, keep track of and record a patient's vitals, predict suicide risks, and predict the risk of dying. In these cases, algorithmic control is being used to reinforce fundamental human rights by improving our access to healthcare.[154] Therefore, at least from a medical perspective, the exponential growth of the use of algorithms is also a great advantage. Finally, it is worth noting again that, arguably, algorithmic bias and algorithmic mistakes are easier to solve than human prejudice and long embedded social injustices.[155]

3.2. Fairness and transparency

HUMAN VS. ALGORITHMIC DECISION MAKING: THE CHALLENGE OF EXPLANATION

How do we ensure that decisions made by algorithms are fair and representative of the desired goal? We may start by looking at the difference between an algorithmic decision and a human one.

The main difference between decisions made by an algorithm and a human is that an algorithm does not readily provide an explanation for the decision made. Human decisions might not necessarily carry explanations with them, but it is generally easier to inquire about an explanation for a human decision than an algorithmic one. Through the data inputs and the learning tools they develop, however, algorithms also in a sense "make decisions." In a way, this process reflects what human developers

have designed them for, albeit the explanation of this process is far from straightforward. Without explanation, the process leading to algorithmic decisions is very much like a "black box."

Nevertheless, there is not yet a general standard of transparency for algorithms to base themselves on. While the notion of transparency could be subject to many interpretations, there is a general need for transparency when it comes to the algorithmic process(es): a need to understand what happens in between the input and the output phase—that is, what is inside the "black box."[156]

The EU's GDPR is a good example of legislative progress in this respect. [157] As seen above, the GDPR ensures data subjects certain rights to information, whether personal data is collected directly from the data subject or obtained from third parties (Articles 13 and 14). Such rights, and in particular the right to be informed about the existence of automated decision making, including profiling, have been compared to the nutritional information that consumers can generally find in food packaging.[158] In other words, an individual should know how intelligence is being managed by a particular organization and how this may directly affect them.[159] As also mentioned above, the GDPR outlines clear rights to object to profile tracking and to not being subject of decisions based on automated individual decision making (Articles 21 and 22).

For a whole number of reasons, particularly regarding protection against privacy invading algorithms, GDPR has definitely become the global standard for data protection.

Hence, there is a clear need for algorithmic transparency which would in turn lead to algorithmic accountability.

ALGORITHMIC TRANSPARENCY IS ENSURED BY CLEAR RIGHTS TO EXPLANATION FOR DATA SUBJECTS

3.3 Algorithmic accountability: the right to an explanation

Following the GDPR standards, algorithmic transparency is ensured by clear rights to explanation for data subjects. Algorithms should, for example, provide the general public with a "counterfactual explanation" for the decisions made, including the reasons that led them to make the particular decision.[160] Moreover, there is a stipulation that these explanations provided by the algorithms should prove whether the decision was made on biased assumptions by the algorithm.

On the other hand, these explanations could not be as useful for, for example, providing a "recourse" for consumers to change the outcome of a decision made by an algorithm. But again, this does not necessarily guarantee the fairness of the algorithmic decision.[161]

For AI to come with explanations and ideally unbiased results, an analysis of the source of the algorithms must be considered. Indeed, as explained earlier, it is the input data that fuels those decisions. Algorithms learn through the data fed into them. Thus, the correct questions to pose, also in the case of transparency and accountability are the following: What type of data should be fed into algorithms for them to learn and interpret without (any) incorrect judgement? How do we ensure transparency during the input of data and during the process that leads to output(s)? And, perhaps more importantly, who should be the competent authority or other stakeholder to do so?

Who will authoritatively answer the questions above? Determining the key stakeholders and competent authorities is key when it comes to protecting citizens' individual rights and guaranteeing algorithmic transparency. To execute this delicate task effectively, it would be advisable that all the parties interested and also affected by algorithms participate in a constructive dialogue. Regarding regulation, in order to adhere to the complexity of the issues that arise, government intervention might not be the only reliable source of regulation. Collaboration with civil society and with the private sector are key. Such a combination can be referred to as "multistakeholderism," a notion of governance already known to the very founders of the internet[162] and subsequently used as the predominant model of Internet Governance. This "non-traditional form"[163] of regulation involves, at one end, the private sector and civil society, and at the other, the government. From an institutional perspective, this should also include the different bodies of the government, such as the legislative bodies as well as the judiciary. Finally, institutions such as citizens' ombudsmen may also play a role.[164] Key stakeholders are also the various civil society organizations—from formal non-profit associations to informal citizens' initiatives—who are both independent stakeholders and relevant intermediaries between the government and other private stakeholders. They can be used to monitor the activity of the administration and public authorities[165] and further ensure algorithmic transparency and accountability.[166]

Overall, multistakeholderism brings about many benefits which "unlike traditional policy processes" include openness, transparency, diversity of opinions, inclusivity, and "the broad-based collaboration and equal participation of those affected in decision making on a particular issue." [167] [168] Furthermore, multistakeholderism enhances transparency, which as we have seen, is a top priority. Another valid argument is that government bodies as such may not have the expertise to regulate a field where transparency and various levels of technological experise is critically required. Thus, in addition to working with civil society and with the private sector, collaboration with experts is equally

as crucial. By experts, we mean those who can easily understand and explain (or “translate”) scientific or technical details to less expert but equally as affected groups.

IV. OUR PROPOSAL FOR GOOD ALGORITHMIC PRINCIPLES

Having explored the opportunities and threats that come with the widespread use of algorithms, along with the most common ethical and legal concerns surrounding them and their use of data, we propose the following principles to ensure that algorithms benefit, rather than harm, civil society:

1. ADHERING TO THE GOOD DATA PRINCIPLE
2. RESPECTING PRINCIPLES OF TRANSPARENCY & EXPLAINABILITY
3. RESPECTING INDIVIDUAL PRIVACY AND AUTONOMY

1. ADHERING TO THE GOOD DATA PRINCIPLE

"Good data" refers to the principle of collecting data in an ethical and just manner in an age where governments and private companies gather masses of data about individuals, often using questionable and opaque methods.[169] For instance, Facebook has been scrutinized for selling information collected from its users to third-parties without the consent. A more recent example is the federal lawsuit launched in the US against Amazon after Alexa, its virtual assistant, recorded children without their consent.[170] The idea is to use "good data" to develop a fair and just digital society, which is crucial as societies and economies become increasingly digitized.

1.1 <u>What exactly is "good data"?</u>

To begin with, "good data" is data that is fit for a certain purpose. This means that in order for data to be "good", only data that meets consumer's and data producer's specific needs should be collected, thus abandoning the common policy of collecting as much data as possible. Within this, "good data" should openly outline who funded the collection and who collected the data, the original purpose of the data collection, when the data was collected, and how it was processed, to ensure maximum transparency.[171] Furthermore, "good data" measures uncertainty and acknowledges limitations.

We tend to blindly trust data but this can generate misleading conclusions. Data, just like everything else, has its flaws and limitations. Therefore, "good data" collectors should explain these uncertainties and limitations so that data used for decision making is more accurate and informed.[172]

Moreover, "good data" must be **readable** for everyone, which means that it must be written in open formats, including .txt, .csv, .html and .mp3. It is also important that "good data" meets the fair(er) criteria: **findable, accessible, interoperable, reusable, ethical, and revisable**.[173] For instance, it must be revisable so that older versions of data can be decommissioned once it is no longer useful. In this way, data can be changed over time to maximize its utility and ensure that it is up-to-date.[174]

Another important characteristic of "good data" is that it is reproducible, as data cannot be deemed reliable if, when it is collected a second time, produces completely different results. Additionally, "good data" is timely, which means that it should be published as soon as possible after collection and composition.[175] Such data must also be appropriately licensed to avoid ambiguity surrounding it purpose. Perhaps the most important characteristic of "good data" is that it must respect a variety of rights when collected, including human and in particular privacy rights, as well as property rights.[176] Linked to this, "good data" must also be published openly and when necessary, anonymously, so that the privacy of individuals is maintained.

Since 1995, the EU has taken steps to promote "good data," as presented above, and protect individuals' data. Nowadays, the GDPR gives citizens greater control over their personal data. Its Article 1 contains many principles indeed grounded on the spirit of "good data", such as the fairness, transparency, purpose limitation, minimization, accuracy, and accountability of data processing activities. Thus, as we have seen, the GDPR obliges organizations to provide citizens with clear information regarding how they process data, including: why the data was collected, how long the data will be stored, with whom the data will be shared, their rights with regards to the data concerned, how to retract their consent if it has already been provided, if their data will be transferred outside of the EU, and how to contact the organization processing their data. The GDPR also allows citizens to request organizations to update their data about them, meeting the "revisable" criteria of "good data" or to completely delete it altogether.[177]

1.2 The relationship between "good data" and the expansion of rights and freedoms

As previously explained, "good data" revolves around the ethical and just collection and publication of data, to protect and expand the rights and freedoms of individuals whose data is collected. This means that with the implementation of "good data," citizens will have power over their own data, particularly in relation to the purpose of data collection. With the growing importance of AI and big data, and increasing concerns surrounding corporations' indiscriminate data gathering, "good data" can become a key tool for implementing ethical practices in the world of data collection and

publication, no doubt ensured by its inclusion in critical pieces of legislation such as the GDPR with the subsequent necessary enforcement.

1.3 "Good data" is also sustainable data

Finally, we must also mention sustainability. The more we learn about e-waste and the environmental impact that our digital footprint has on the planet, the more we need to stress that "good data" need also be sustainable data. Excessive energy consumption—for example, in the case of bitcoin mining—is a serious issue to be considered as we evaluate what "good data" is.

While exercising caution when it comes to data and the environment, there are also productive ways to think of the data-sustainability relationship. For example, using big data to promote sustainable development goals.[178]

2. RESPECTING PRINCIPLES OF TRANSPARENCY AND EXPLAINABILITY

As discussed above, clear standards of transparency, together with the right to an explanation, will ensure algorithmic accountability. Citizens, as data subjects, need to not only be informed about the algorithmic uses of their data, but also in control of the processes involved. Principles of transparency and explainability guarantee such control. This will ultimately lead to a greater level of respect toward individual privacy and autonomy.

3. RESPECTING INDIVIDUAL PRIVACY AND AUTONOMY

From a broader perspective, the use of "good data" together with high levels of data protection, ensured by principles of transparency and explainability, are all methods that promote individual privacy. Privacy can be seen as a goal but also as a means to an even greater end: that of individual autonomy. While the notion of privacy is somewhat defensive, autonomy is more forward-looking as it empowers citizens. By extension, civil society must be protected at all costs due to the fact that autonomy leads to initiative and innovation.

4. EDUCATIONAL CHALLENGE

A society whose systems and procedures can reach an increasing degree of artificial intervention, while communicating consistent values, must effectively cultivate new skills to its citizens and promote knowledge and education. It would be necessary to incorporate the fundamental technical and other concepts discuss as well as the good algorithmic principles in the processes of education at earlier and more advanced stages. Accordingly, we can expect that educators must assume new ethical responsibilities in their relationship with younger generations (who are now all digital native generations) developing notions of coexistence with technology

and understanding algorithms' most common applications in daily life and the threats and opportunities that come along.

VII. CONCLUSION

A DECALOGUE OF MAXIMS

We will conclude with a list of critical observations and recommendations, in the form of maxims, to be further assessed by the readers of this guide. In our proposed "decalogue of maxims" we have incorporated the notions promoted by this guide—algo-awareness, transparency and accountability, and the principle of "good data", and the need for high standards for data protection and sustainability. Fair and sustainable use of algorithms and data is key for innovation that benefits humankind.

Relying on machines to complete tasks is undoubtedly convenient but could result in detachment, alienation, and dependence—in other words, in algorithmic control of humans. We also support awareness among civil society actors, participation, and multi-stakeholder dialogue in order to avoid such algorithmic control and, instead, ensure that *humans* remain *in control* of algorithms.

1. **HUMAN DIGNITY:** While embracing the benefits of algorithms and technological progress, human dignity should remain uncompromised.
2. **HUMAN CONTROL OVER ALGORITHMS:** Humans must exercise control over algorithms (and not the other way around). To avoid detachment and ensure human control, reliance on machines should only take place when it is guaranteed to benefit humankind.
3. **ALGO-AWARENESS:** The use of algorithms is widespread and advantageous. Algo-awareness will help us face the risks and threats that come with algorithms (including threats to equity, privacy, security, and physical integrity) while also enjoying the benefits.
4. **ALGORITHMIC TRANSPARENCY:** Algorithmic transparency is the first step toward fighting opacity.
5. **ALGORITHMIC ACCOUNTABILITY:** Transparency should be coupled with algorithmic accountability.
6. **CIVIL SOCIETY:** Multi-stakeholder dialogue and civil society engagement are paramount to ensure human-centric policies that combat algorithmic control.
7. **"GOOD DATA":** We can combat algorithmic biases by adhering to a "good data" principle meeting the fair(er) criteria: findable, accessible, interoperable, reusable, ethical, and revisable.
8. **PRIVACY:** We must maintain high standards of privacy and data protection, following the guidance of protective frameworks and avoiding race-to-the-bottom scenarios.
9. **DATA SUSTAINABILITY:** We must maintain high standards of environmental protection and sustainability.
10. **INNOVATION:** Fair and sustainable use of algorithms and data is key for innovation that serves the needs of humankind.

ENDNOTES

[1] Gabriel Winant, "Life Under the Algorithm: How a relentless speedup is reshaping the working class", *The New Republic,* December 4, 2019, https://newrepublic.com/article/155666/life-algorithm. To present a small recent sample of popular media coverage on algorithms: Sendhil Mullainathan, "Biased Algorithms Are Easier to Fix Than Biased People", *The New York Times,* December 6, 2019, https://www.nytimes.com/2019/12/06/business/algorithm-bias-fix.html; Kirsten Grind, Sam Schechner, Robert McMillan and John West, "How Google Interferes With Its Search Algorithms and Changes Your Results: The internet giant uses blacklists, algorithm tweaks and an army of contractors to shape what you see", *The Wall Street Journal*, November 15, 2019, https://www.wsj.com/articles/how-google-interferes-with-its-search-algorithms-and-changes-your-results-11573823753. References to this Guide are updated to reflect news coverage and scholarship until December 10, 2019.

[2] *Encyclopaedia Britannica*, *Inc.,* s.v. "Al-Khwārizmī," last modified February 17, 2017, www.britannica.com/biography/al-Khwarizmi.

[3] Lee Ranie and Janna Anderson, "Code-Dependent: Pros and Cons of the Algorithm Age," *Pew Research Center*, February 8, 2017, https://www.pewresearch.org/internet/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age/. Market research executive Barry Chudakov thinks companies should include the equivalent of a nutrition label for their algorithms, indicating how an algorithm might make certain decisions, and the implications of those decisions.

[4] Ministerio de Industria, Comercio y Turismo, *La Sociedad en Red*: *Informe Anual* (Madrid: Ministerio de Industria, Comercio y Turismo, 2017), https://www.ontsi.red.es/ontsi/sites/ontsi/files/La%20sociedad%20en%20red.%20Informe%20anual%202017%20%28Edici%C3%B3n%202018%29.pdf.

[5] Ibid.

[6] Amy Cross, "Data Mining vs. Machine Learning: What's the Difference?," *NGDATA,* June 22, 2018, https://www.ngdata.com/data-mining-vs-machine-learning/.

[7] Ministerio de Industria, Comercio y Turismo, *La Sociedad en Red*.

[8] Thus, according to some classifications and without the following list being exhaustive nor necessarily authoritative, there are: (i.) Simple recursive algorithms, which are used for straight-forward problem solving. They operate with simple input values which used to solve specific questions or issues by applying simple operations. (ii.) Backtracking algorithms, which are general algorithms that build solutions incrementally one step at a time. (iii.) Divide-and-conquer algorithms, which divide large and complex computational problems into smaller and simpler problems. (iv.) Dynamic programming algorithms, which, similarly to divide-and-conquer algorithms, are breaking up larger problems into subproblems to make them easier to solve. What makes them different is that dynamic programming uses minuscule parts of large problems which tend to overlap. (v.) Greedy algorithms, on the other hand, are the exact opposite of dynamic and divide-and-conquer algorithms. Instead of dissecting a problem into micro-problems, they make an optimal solution and apply it on a broad scale. They tend to be easier to create and analyze but also less accurate. (vi.) Branch and bound algorithms solve exponential computational problems and therefore they tend to be time consuming. (vii.) Brute force algorithms are based on a programming style in which there are no shortcuts to improve performance. Instead, this algorithm relies on computing power. (viii.) Randomized algorithms use random information as an input to guide the algorithm's behavior with the goal of attaining success in an average case.
Various classifications and definitions are retrieved from various sources including: "Recursive Algorithm," Old Dominion University, https://www.cs.odu.edu/~toida/nerzic/content/recursive_alg/rec_alg.html ;"Backtracking/Introduction," GeeksforGeeks, https://www.geeksforgeeks.org/backtracking-introduction/ ;Brandon Skerritt, "A Gentle Introduction to Divide and Conquer Algorithms," *Brandon's Blog*, March 19, 2019, https://skerritt.blog/divide-and-conquer-algorithms/ ;James Le, "Greedy Algorithm and Dynamic Programming," *Medium*, Octobre 15, 2018, https://medium.com/cracking-the-data-science-interview/greedy-algorithm-and-dynamic-programming-a8c019928405 ;Stanford University, "Branch and Bound Methods," https://web.stanford.edu/class/ee364b/lectures/bb_slides.pdf ;"Brute Force Algorithms," freeCodeCamp, https://guide.freecodecamp.org/algorithms/brute-force-algorithms/ ;"Randomized Algorithms (Introduction and Analysis)," GeeksforGeeks, https://www.geeksforgeeks.org/randomized-algorithms-set-1-introduction-and-analysis/.

[9] Regulation (EU) 2016/679. See Articles 4 and 9 of the EU General Data Protection Regulation.

[10] Latorre Sentís, *Ética para máquinas*.

[11] John McCarthy, "What is artificial intelligence," Stanford University, November 12, 2007, http://www-formal.stanford.edu/jmc/whatisai/.

[12] Kathleen Walch, "Rethinking weak vs. strong AI, " *Forbes*, October 4, 2019; Kathleen Walch and Ronald Schmelzer, hosts, "AI Today Podcast #008: Weak, Strong AI – Do these Terms Matter?" AI Today Podcast, October 25, 2017, https://www.cognilytica.com/2017/10/25/ai-today-podcast-008-weak-strong-ai-terms-matter/.

[13] Ibid.

[14] John McCarthy, Generality in artificial intelligence, *Communications of the ACM* 30, no.12 (1987): 1030-1035. (Postscript of McCarthy's Alan Turing Award Lecture)

[15] Alan M. Turing, "Computing Machinery and Intelligence," *Mind* 49, no. 236 (October 1950): 433 – 460.

[16] Chris Smith, Brian McGuire, Ting Huang and Gary Yang, "The History of Artificial Intelligence," Washington University, December 2006, https://courses.cs.washington.edu/courses/csep590/06au/projects/history-ai.pdf.

[17] Latorre Sentís, *Ética para máquinas*.

[18] Ibid.

[19] Noting that there is no globally accepted standard of ethics, the balancing might differ in separate algorithmic uses.

[20] Ibid.

[21] Ibid.

[22] José Ignacio Latorre Sentís, *Ética para máquinas,* 1st ed. (Barcelona: Ariel, 2019), 124.

[23] Alan M. Turing, "Computing Machinery and Intelligence," *Mind* 49, no. 236 (October 1950): 433 – 460.

[24] Tal Zarsky, "Episode #1 - Tal Zarsky on the Ethics of Big Data and Predictive Analytics", interview by John Danaher, 2016, https://algocracy.wordpress.com/2016/04/21/1-tal-zarsky-on-the-ethics-of-big-data-and-predictive-analytics/.

[25] Daniel Susser , Beate Roessler, and Helen Nissenbaum, "Online Manipulation: Hidden Influences in a Digital World," *Georgetown Law Technology Review* 4, no. 1 (2019) , https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3306006.

[26] Imre Bard and Harry Armstrong, "Mapping global approaches to AI governance: Who is leading the way in AI governance," *Nesta*, January 22, 2019, https://www.nesta.org.uk/blog/mapping-global-approaches-ai-governance/.

[27] Meredith Whittaker et al., *AI Now Report 2018* (New York: AI Now Institute, 2018), 12.

[28] Tom Simonite, "Google and Microsoft Warn That AI May Do Dumb Things," *Wired,* February 11, 2019, https://www.wired.com/story/google-microsoft-warn-ai-may-do-dumb-things/.

[29] Ibid.

[30] Whittaker et al., *AI Now Report 2018*.

[31] Ibid.

[32] Latorre Sentís, *Ética para máquinas,* 229.

[33] Whittaker et al., *AI Now Report 2018,* 14.

[34] Ibid.

[35] Sven Nyholm, "Episode #3: Svem Nyholm on Love Enhancement, Deep Brain Stimulation and the Ethics of Self-Driving Cars," interview by John Danaher, 2016.
Laura Cabrera,"Episode #13 Laura Cabrera on Human Enhancement, Communication and Values," interview by John Danaher, 2016.

[36] See Nick Bostrom, "A history of transhumanist thought," *Journal of Evolution and Technology* 14, no.1 (April 2005) and Nick Bostrom, "Transhumanist values," *Journal of Philosophical Research* 30, supplement (2005): 3-14.

[37] "Is technology re-engineering humanity?: A book excerpt and interview with Brett Frischmann, co-author of *Re-Engineering Humanity"*, *The Economist*, October 24, 2018, https://www.economist.com/open-future/2018/10/24/is-technology-re-engineering-humanity.

[38] Farah Mohammed, "Why Luddites Are Fashionable Again", *JStor Daily*, May 29, 2019, https://daily.jstor.org/why-luddites-are-fashionable-again; Brett Frischmann, "There's Nothing Wrong with Being a Luddite", *Scientific American*, September 20, 2018, https://blogs.scientificamerican.com/observations/theres-nothing-wrong-with-being-a-luddite/. See also: Richard Conniff, "What the Luddites Really Fought Against", *Smisthonian Magazine*, March 2011, https://www.smithsonianmag.com/history/what-the-luddites-really-fought-against-264412/.

[39] Shirley Turkle, "Connected but alone?" February 2012, ted talk, https://www.ted.com/talks/sherry_turkle_alone_together?language=en.

[40] Harry Kreisler & Shirley Turkle, "Identity in a cyber world*",* 25 February, 2019*,* interview, https://conversations.berkeley.edu/turkle_2019.

[41] Shirley Turkle, "Introduction:Identity in the age of the internet," in *Life on the Screen:Identity in the age of the internet* (New York : Simon & Schuster, 1995), https://books.google.es/books?id=auXlqr6b2ZUC&pg=PA9&source=gbs_toc_r&cad=3#v=onepage&q&f=false.

[42] Ibid.

[43] Ministerio de Industria, Comercio y Turismo, *Sociedad Digital y Derecho* (Madrid: Boletín Oficial del Estado, 2018), 109.

[44] Donna Harman, "Ranking algorithms," in *Information retrieval: Data structures & algorithms,* ed. William Frakes (Prentice Hall, 1992), http://dns.uls.cl/~ej/daa_08/Algoritmos/books/book5/chap14.htm.

[45] Ibid.

[46] Mildrid Ljosland, "Evaluation of web search engines and the search for better ranking algorithms" (paper given at the SIGIR99 Workshop on Evaluation of Web Retrieval**,** Norwegien University of Science and Technology, 1999), http://www.aitel.hist.no/~mildrid/dring/paper/SIGIR.html.

[47] Ibid.

[48] Nam P. Nguyen et. al., "Adaptive algorithms for detecting community structure in dynamic social networks," (paper presented as part of the main technical program at IEEE INFOCOM 2011, Department of Computer and Information Science and Engineering, University of Florida, 2011), https://grid.cs.gsu.edu/~myan2/communitydetection/5.pdf.

[49] Steve Gregory, "Finding overlapping communities using disjoint community detection algorithms," in *Complex Networks* by Santo Fortunato et al. (Springer Berlin Heidelberg, 2009), https://link.springer.com/chapter/10.1007/978-3-642-01206-8_5.

[50] Le Chen and Christo Wilson, "Observing algorithmic marketplaces in-the-wild," *ACM SIGecom Exchange* 15 no. 2 (February 2017), https://www.sigecom.org/exchanges/volume_15/2/CHEN.pdf.

[51] Mehryar Mohri, Afshin Rostamizadeh and Ameet Talwalkar, *Foundations of machine learning,* 2nd ed. (Cambridge, Massachusetts: Massachusetts Institute of Technology Press, 2012).

[52] Shane Long, "The Advantages of Machine Learning Algorithms in Mobile Apps," *SevenTablets,* https://seventablets.com/blog/the-advantages-of-machine-learning-algorithms-in-mobile-apps/.

[53] Mark Andrejevic and Mark Burdon, "Defining the Sensor Society," *Television & New Media* 16, no.1 (July 11, 2014):20, doi: 10.1177/152747641454155.

[54] Ibid.

[55] For more details on facial recognition techniques see: Jorge Orts, "Face Recognition Techniques," (paper part of ECE533 – Image Processing Project, Madison, Wisconsin, 2014), 2.

[56] Orts, "Face Recognition Techniques," 14.

[57] Ibid.

[58] Andrejevic and Burdon, "Defining the Sensor Society," 20.

[59]Simone Cirani, Gianluigi Ferrari, Marco Picone, and Luca Veltri, *Internet Of Things: Architectures, Protocols And Standards*, (John Wiley & Sons, 2018).

[60] Traditionally it is a field of sensors and systems which control or automate other systems or objects. *OECD Science, Technology and Innovation Outlook 2016,* (Paris, OECD, 2016), doi:10.1787/sti_in_outlook-2016-en.

[61]Neil M. Richards and William Smart, "*How Should The Law Think About Robots?"* (SSRN Electronic Journal, 2013), doi:10.2139/ssrn.2263363.

[62]Craig Webster and Stanislav Hristov Ivanov, *The Robot As A Consumer: A Research Agenda*, (SSRN, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960824.

[63]*Robocalls CG Docket No. 17-59: Report of the US Consumer and Governmental Affairs Bureau* (Federal Communications Commission, 2019), https://docs.fcc.gov/public/attachments/DOC-356196A1.pdf.

[64] Joon Ian Wong, "Robocallers Are Finally Being Fined Into Oblivion In The UK," *Quartz*, 2019, https://qz.com/981352/robocallers-are-being-fined-into-oblivion-by-the-uks-privacy-regulator/.

[65] Suzie Miles, "Smart Contracts – Is Code Law?" *IT Portal*, 2018, https://www.itproportal.com/features/smart-contracts-is-code-law/

[66] Ibid.

[67] Adrian Todolí-Signes, "Algorithms, artificial intelligence and automated decisions about workers and the risks of discrimination: The necessary collective governance of data protection," *Transfer: European Review of Labour and Research* 25, no.4, (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3316666.

[68] Ibid.

[69] Ibid.

[70] Miriam I. Otero, "What is the "gig economy?" *BBVA*, 2018, https://www.bbva.com/en/what-is-gig-economy/

[71] Jeremias Prassl, *Humans as a Service: The Promise and Perils of Work in the Gig Economy* (UOP Oxford, 2018), doi:10.1093/oso/9780198797012.001.0001.

[72] Ibid.
[73] Ibid.
[74] Ibid.
[75] Sacha Garben, *Protecting Workers in the Online Platform Economy: An overview of regulatory and policy developments in the EU,* (European Agency for Safety and Health at Work, 2017), https://osha.europa.eu/en/tools-and-publications/publications/regulating-occupational-safety-and-health-impact-online-platform/view.
[76] Ibid, p.79.
[77] Ibid.
[78] Ibid.
[79] Valerio De Stefano, *The rise of the 'just-in-time workforce': On-demand work, crowd work and labour protection in the 'gig-economy'*, (Geneva, International Labour Office, 2016), doi: 10.2139/ssrn.2682602.
[80] Alex J. Wood, Mark Graham, Vili Lehdonvirta, and Isis Hjorth, "Good Gig, Bad Gig: Autonomy And Algorithmic Control In The Global Gig Economy,"*Work, Employment And Society* 33, no.1 (2018): 56-75, doi:10.1177/0950017018785616.
[81] De Stefano, *The rise of the 'just-in-time workforce'.*
[82] Pablo García Mexía, *Criptoderecho, La regulación de Blockchain* (Madrid: Wolters Kluwer, 2018) 43.
[83] Ibid.
[84] Ibid, p. 44
[85] Pablo García Mexía and José Morales Barroso, *Cryptoregulation in a Nutshell: The Basics of Blockchain and Blockchain Regulation* (N.p. :Wolters Kluwer, 2020), 26. Publication pending (scheduled 2020).
[86] Ibid.
[87] *Deep Shift – Technology Tipping Points and Societal Impact,* (World Economic Forum, 2015), http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf.
[88] Konstantinos Stylianou and Nic Carter, "Calculating Cryptoasset Market Shares," *Journal of Competition Law and Economics* 15, (March 19, 2019), https://ssrn.com/abstract=3346558; Angela Walch, "Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems," *Crypto Assets: Legal and Monetary Perspectives (OUP, Forthcoming*), (January 30, 2019), https://ssrn.com/abstract=3326244. For more information see among these.
[89] Lucy Bernholz, "EFF and the invention of digital civil society," *Stanford Social Innovation Review*, (2019).
[90] *Statement on algorithmic transparency and accountability* (Association for Computing Machinery US Public Policy Council, 2017), https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf.
[91] Ibid.
[92] Mike Ananny and Kate Crawford, "Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability," *New Media & Society* 20, no.3 (2018): 973–989, doi: 10.1177/1461444816676645.
[93] Ibid.
[94] Ibid.
[95] Ibid.
[96] Ibid.
[97] Torrens, M., Cortés, U, Valogianni, K., Valor J., Ruiz Hontangas, A., Almirall, E., Argandoña, A. & Guerris, M. "Los Retos Eticos de la Inteligencia Artificial" *Harvard Business Review Deusto* 296 (2020) 34-59.
[98]Michael Núñez, "The Google Arts and Culture App Has a Race Problem," *Mashable*, 2018, https://mashable.com/2018/01/16/google-arts-culture-app-race-problem-racist/?europe=true.
[99] Alex Rosenblat, Tamara Kneese, Danah Boyd, *Networked Employment Discrimination*, (Data & Society Research Institute, 2014), https://www.academia.edu/24135171/Networked_Employment_Discrimination.
[100] Savage David, Richard A. Bales, "Video Games in Job Interviews: Using Algorithms to Minimize Discrimination and Unconscious Bias," *ABA Journal of Labor & Employment Law* 32, (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2887757.
[101] Julia Powles, "The Seductive Diversion of 'Solving' Bias in Artificial Intelligence", *Medium,* 2018, https://onezero.medium.com/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53.
[102] Susser, Roessler, and Nissenbaum, "Online Manipulation"; Veronica Barassi, "Datafied Citizens? Social Media Activism, Digital Traces and the Question about Political Profiling," *Communication and the Public* 1, no.4 (2016): 494-499. For more information see among these.

[103] Christoforos Christoforou, Timothy C. Papadopoulos, Fofi Constantinidou and Maria Theodorou, "Your Brain on the Movies: A Computational Approach for Predicting Box-office Performance from Viewer's Brain Responses to Movie Trailers," *Frontiers in Neuroinformatics* 11, no. 72 (December 19, 2017), https://www.frontiersin.org/articles/10.3389/fninf.2017.00072/full.

[104] David Murakami Wood et al. *A report on the surveillance society* (UK: Surveillance Studies Network, 2006), https://ico.org.uk/media/about-the-ico/documents/1042390/surveillance-society-full-report-2006.pdf

[105] Ibid.

[106] "Internet-based rumors and lies are [...] searchable, replicable and accessible to any decision maker with access to the right software or database".
Rosenblat, Kneese and Boyd, *Networked Employment Discrimination*.

[107] Teena Madox, "The dark side of wearables: How they're secretly jeopardizing your security and privacy," *Technology Republic,* 2015, https://www.techrepublic.com/article/the-dark-side-of-wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy/.

[108] Budapest Convention on Cybercrime, opened for signature 23 November 2001, ETS No 185 (entered into force 1 July 2004), Articles 2-6, https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

[109] Ibid, Articles 7-10.

[110] Ahmed, Ghappour., "Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web." *Stan. L. Rev*. 69 (2017): 1075, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2742706

[111] An example of such cooperation is the Budapest Convention on Cybercrime (supra note 114)

[112] Edson Tandoc, Zheng Wei Lim, and Richard Ling. "Defining "fake news" A typology of scholarly definitions." *Digital journalism* 6.2 (2018): 137-153; Robert Chesney, and Danielle Keats Citron. "Deep fakes: a looming challenge for privacy, democracy, and national security." (2018).

[113] "Spyware and Malware," Federal Trade Commission, https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/spyware-and-malware.

[114] "Unfair, Deceptive, or Abusive Acts of Practices Act," *Mortgage Compliance Magazine*, https://www.mortgagecompliancemagazine.com/mortgage-compliance-alphabet-soups/unfair-deceptive-abusive-acts-practices-act-udaap/.

[115] "Spyware and Malware," Federal Trade Commission.

[116] Ge Wang, Humans in the Loop: The Design of Interactive AI Systems, *Human-Centered Artificial Intelligence Stanford University* (October 21, 2019), https://hai.stanford.edu/news/humans-loop-design-interactive-ai-systems

[117] Brett Frischmann, and Evan Selinger, *Re-engineering humanity*, (Cambridge University Press, 2018).

[118] Ibid.

[119] Ibid.

[120] Cecilio M. Villarejo, *The legacy of Commissioner Vestager and a peek into the future*, (European Commission, 2019), https://ec.europa.eu/competition/speeches/text/sp2019_12_en.pdf.

[121] See Carmen Ramírez Perete, and Pablo García Mexía. "La propiedad sobre el dato:¿ Cabe una vertiente patrimonial de la protección de datos?." *Revista de privacidad y derecho digital* 4.15 (2019): 95-125.

[122] Eric A. Posner, and E. Glen Weyl. *Radical markets: Uprooting capitalism and democracy for a just society*. Princeton University Press, 2018. (see in particular their chapter 5 (Data is labor).

[123] European Commission, *Ethics Guidelines for Trustworthy Artificial Intelligence*, (Brussels, 2019).

[124] Ibid.

[125] European Commission, *Artificial Intelligence for Europe,* COM/2018/237 (Brussels, 2018).

[126] Ibid, p.19.

[127] Organisation for Economic Co-operation and Development, *Council Recommendation on Artificial Intelligence* (Paris, 2019).

[128] OECD, *Principles on Artificial Intelligence*, (OECD, 2019), https://www.oecd.org/going-digital/ai/principles/.

[129] The United Nations, *United Nations Activities on Artificial Intelligence* (New York, 2018), https://futureoflife.org/ai-principles/.

[130], "Asilomar AI Principles," *Future of Life Institute*.

[131] Ibid.

[132] Regulation (EU) 2016/679 (General Data Protection Regulation).

[133] Bryce Goodman and Seth Flaxman, "European Union regulations on algorithmic decision-making and a 'right to explanation'", *AI Magazine* 38, no. 3, (2017), https://arxiv.org/abs/1606.08813.
[134] Ibid.
[135] Ibid.
[136] Regulation (EU) 2016/679 (General Data Protection Regulation).
[137] Goodman and Flaxman, "European Union regulations".
[138] Pablo García Mexía, "Derechos digitales. La nueva regulación española," (paper given at XII Congreso Nacional de la Abogacía, Valladolid Spain, May 8-11, 2019).
[139] World Intellectual Property Organization, *Understanding Copyright and Related Rights*, (WIPO, 2016), https://www.wipo.int/edocs/pubdocs/en/wipo_pub_909_2016.pdf.
[140] "Artificial intelligence and intellectual property: an interview with Francis Gurry", *WIPO Magazine*, 2018.
[141] Ibid.
See also WIPO's public consultation on AI and Intellectual Property policy and the publication of more than 250 Submissions Received on AI and IP Policy Public Consultation (Feb. 20, 2020) , https://www.wipo.int/about-ip/en/artificial_intelligence/news/2020/news_0003.html.
[142] Ibid. (Artificial intelligence and intellectual property: an interview with Francis Gurry)
[143] Ibid.
[144] Ibid.
[145] Samuel D. Warren and Louis D. Brandeis, "Right to Privacy," *Harvard Law Review*,4, no.193 (1890).
[146] See how this right evolved in the EU context especially as interpreted by the Court of Justice of the European Union from the *Google Spain v. Agencia Española de Protección de Datos* (C-131/12) case to the *Google v. Commission nationale de l'informatique et des libertés* (C-507/17) case.
[147] Alex Miller and Kartik Hosanagar, "How Targeted Adds and Dynamic Pricing Can Perpetuate Bias," *Harvard Business Review*, 2019.
[148] Villarejo, *The legacy of Commissioner Vestage*.
[149] Article 18(1) of the Spanish Constitution, for example, states that the right to dignity shall be guaranteed, while Article 18(4) proclaims that the law will limit the use of computer science to guarantee the right to personal dignity. Boletín Oficial del Estado, *Constitución Española* (Madrid, 1978).
[150] Anna Hoffmann, "Data Violence and How Bad Engineering Choices Can Damage Society," 2018, https://medium.com/s/story/data-violence-and-how-bad-engineering-choices-can-damage-society-39e44150e1d4.
[151] Sandra Wachter, "The Other Half of the Truth: Staying human in an algorithmic world," 2019, https://www.oecd-forum.org/users/264249-sandra-wachter/posts/49761-the-other-half-of-the-truth-staying-human-in-an-algorithmic-world.
[152] Hoffmann, "Data Violence and How Bad Engineering Choices Can Damage Society".
[153] Ministerio de Economía y Empresa, *Sociedad Digital y Derecho* (Madrid, 2018) 109.
[154] "Top Smart Algorithms In Healthcare," *The Medical Futurist*, 2019, https://medicalfuturist.com/top-ai-algorithms-healthcare/.
[155] This is the argument reflected in the recent article: Sendhil Mullainathan, "Biased Algorithms Are Easier to Fix Than Biased People," *The New York Times*, 2019.
[156] The European Union has already approached this issue with a non-binding provision in the new Regulation on General Protection Data, aimed at giving more control to users on how companies use their personal information.
[157] Goodman and Flaxman, "European Union regulations".
[158] Ranie and Anderson, "Code-Dependent".
[159] Ibid.
[160] Sandra Wachter, Brendt Mittelstadt, and Chris Russell, "Counterfactual explanations without opening the black box: automated decisions and the GDPR," *Harvard Journal of Law & Technology* 31, no.2, (2018).
See also Louis Matsakis, "What Does a Fair Algorithm Actually Look Like?" *Wired*, November 10, 2019.
[161] Ibid.
[162]Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff, "A brief history of the Internet," *ACM SIGCOMM Computer Communication Review* 39, no.5 (2009):22-31, http://doi.acm.org/10.1145/1629607.1629613.
[163] Anri Van der Spuy, *What if we all governed the Internet? Advancing multistakeholder participation in Internet governance*, (UNESCO Series on Internet Freedom, 2017)19, https://unesdoc.unesco.org/ark:/48223/pf0000259717.

[164] In the Spanish context: "High Commissioner of Parliament responsible for defending citizens' fundamental rights and civil liberties". "What is the Defensor del Pueblo?", *Defensor del Pueblo,* https://www.defensordelpueblo.es/en/who-we-are/what-is-the-defensor/.

[165] Ibid.

[166] See also the recent report from UNESCO. Xianhong Hu, Bhanu Neupane, Lucia Flores Echaiz, Prateek Sibal, Macarena Rivera Lam*, Steering AI and advanced ICTs for knowledge societies: a Rights, Openness, Access, and Multi-stakeholder Perspective* (UNESCO, 2019).

[167] Van der Spuy, *What if we all governed the Internet?*

[168] Ibid, p.28.

[169] Angela Daly, Kate Devitt, and Monique Mann, "Good Data," *Institute of Network Cultures* 1, no.29, (2019):37-54*, https://networkcultures.org/wp-content/uploads/2019/01/Good_Data.pdf*.

[170] Jim Sams, "Federal Lawsuit Charges Amazon's Alexa Violate's Children's Privacy," *Claims Journal*, June 17, 2019, https://www.claimsjournal.com/news/national/2019/06/17/291497.htm.

[171] Daly et al. , "Good Data," 37-54.

[172] Ibid.

[173] According to Daly, Devitt and Mann, 'good data' must form "Useful Social Capital", which refers to the collection of resources that allow for social interaction and understanding. In other words, 'good data' behaves as a social asset that is based on trust and co-operation (Daly et al. , "Good Data," 37-54).

[174] Daly et al. , "Good Data," 37-54.

[175] Ibid.

[176] Ibid.

[177] Comisión Europea, *Guía para los ciudadanos sobre la protección de datos en la UE* (Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2019), https://ec.europa.eu/commission/sites/beta-political/files/data-protection-overview-citizens_es.pdf.

[178] See the relevant discussion lead by the UN (resources available at: www.un.org/en/sections/issues-depth/big-data-sustainable-development/index.html).
See also relevant work of the civil society at a global scale: for example, Global Fishing Watch using data to track vessels (https://globalfishigwatch.org/vessel-tracking-data or the Ocean Observatories Initiative operating a data portal to help build data infrastructure assisting oceanographic research communities (https:/oceanobservatories.org/data-portal/).